U.S. Intelligence Law:

A Comprehensive Multimedia Introduction

DAVID ALAN JORDAN

Creative Commons Course Book for Course 3

Statutory Law and Intelligence

Secondary Authority Course Book 3 of 3

IntelligenceLaw.com®

Creative Commons Course Book for

U.S. Intelligence Law:
A Comprehensive Multimedia Introduction

By

David Alan Jordan
Visiting Assistant Professor of Law
Washington and Lee University

Creative Commons Course Book for Course 3
Statutory Law and Intelligence
(June 2010)

IntelligenceLaw.com®

United States of America, 2010

To the American Civil Liberties Union [www.aclu.org]

Preface

This free course book contains useful background reports on topics relevant to the subject matter of *Course II: U.S. Intelligence Law for American Journalists*. Each report was produced originally for members of Congress by legislative attorneys and subject matter experts at the Congressional Research Service (CRS). I compiled some of the most useful background reports into this free course book for use by United States persons completing this home study course or any of the other law school courses available on IntelligenceLaw.com.

IntelligenceLaw.com is an independent, nonpartisan legal publisher unaffiliated with the United States Government. The Congressional Research Service played no role in the compilation of this course book. IntelligenceLaw.com is responsible for any errors or omissions made while formatting the original government documents into this free consolidated course book.

Neither this course book nor the original reports contained herein are copyrighted; therefore, there are no restrictions on your use of these materials. Please feel free to distribute this text to others or use its contents in any way you feel might be beneficial to your personal projects.

DAVID ALAN JORDAN

June, 2010

Summary of Contents

Full Table of Contents

Creative Commons Course Book for

U.S. Intelligence Law:
A Comprehensive Multimedia Introduction

Creative Commons Course Book for Course 3

Statutory Law and Intelligence

(First Edition 2011)

TITLE 5: GOVERNMENT ORGANIZATION AND EMPLOYEES

5 U.S.C. Chapter 5: Administrative Procedure (5 U.S.C. §§ 500-596)

The Freedom of Information Act (5 U.S.C. § 552)

Access to Government Information In the United States, 97-71 (August 31, 2009).

WENDY R. GINSBERG & HAROLD C. RELYEA, CONGRESSIONAL RESEARCH SERV., ACCESS TO GOVERNMENT INFORMATION IN THE UNITED STATES (2009), *available at* http://www.intelligencelaw.com/library/secondary/crs/pdf/97-71_8-31-2009.pdf.

Wendy R. Ginsberg
Analyst in Government Organization and
Management
wginsberg@crs.loc.gov, 7-3933

Acknowledgments
Parts of this report were originally written by Harold C. Relyea, who has since retired from the Congressional Research Service.

August 31, 2009

Congressional Research Service

7-5700
www.crs.gov
97-71

Summary
The U.S. Constitution makes no specific allowance for any one of the three branches of the federal government to have access to information held by the others. No provision in the U.S. Constitution expressly establishes a procedure for public access to government information.

Congress has legislated various public access laws. Among these laws are two records access statutes,

- the Freedom of Information Act (FOI Act or FOIA; 5 U.S.C. § 552), and
- the Privacy Act (5 U.S.C. § 552a),

and two meetings access statutes,

- the Federal Advisory Committee Act (FACA; 5 U.S.C. App.), and
- the Government in the Sunshine Act (5 U.S.C. § 552b).

The American separation of powers model of government may inherently prompt interbranch conflicts over the accessibility of information. These conflicts are neither unexpected nor necessarily destructive. Although there is considerable interbranch cooperation in the sharing of information and records, such conflicts over access may continue on occasion.

This report offers an overview of the four information access laws noted above, and provides citations to additional resources related to these tools.

History and Background

Throughout the first 150 years of the federal government, access to government information does not appear to have been a major issue for the federal branches or the public. There were a few instances during this period when the President, for reasons of maintaining the constitutional independence and equality of his branch, vigorously resisted attempts by Congress and the courts to obtain executive records.[1] Furthermore, during this same era, an active federal public printing program was established and effectively developed, making government documents more accessible.[2]

Following World War II, some information was available from certain federal departments and agencies.[3] The public availability of records held by the

---

[1] The powers of Congress to access executive-branch records dates back to as early as 1790, when the House established a select congressional committee to investigate the actions of former Superintendent of Finance Robert Morris. For more information see 1 Annals of Cong. 1168 (February 8, 1790). See also United States v. Nixon, 418 U.S. 683, 711 (1974). In U.S. v. Nixon, the court said that if the extent of the President's interest in withholding information for the purpose of confidentiality "relates to the effective discharge of a President's powers, it is constitutionally based." See also House Committee on the Judiciary, "House Judiciary Committee Releases Rove and Miers Interview Transcripts and Over 5,400 Pages of Bush White House Documents," at http://judiciary.house.gov/news/090811.html.

[2] Harold C. Relyea, American Federal Government Printing and Publication Reform: A Special Issue of Government Publications, Part A; Research Articles (Oxford, England: Pergamon Press, 1982).

[3] See U.S. Congress, Senate Committee on the Judiciary, Bills to Amend the Administrative Procedure Act, and for Other Purposes, hearing on S. 1160, S. 1336, S. 1758, and S. 1879, May 12-14 and 21, 1965, 89th Cong., 1st sess. (Washington: GPO, 1965). At the hearing, Chairman James O. Eastland stated the following:

executive branch was limited by narrow interpretation of the housekeeping statute of 1789 (5 U.S.C. § 301), which authorized the heads of departments to prescribe regulations regarding the custody, use, and preservation of the records, papers, and property of their entity. Prevailing law tolerated this state of affairs, offering citizens no clear avenue of access to agency information. Moreover, a provision of the Administrative Procedure Act of 1946 (5 U.S.C. § 551) indicated that matters of official record should be available to the public, but added that an agency could restrict access to its documents "for good cause found" or "in the public interest." These discretionary authorities were relied upon to restrict the accessibility of unpublished agency records and documents.

In response, some congressional panels began examining information access issues and seeking responsive legislative solutions. Among these legislative responses was the creation of the four following statutes:

- the Freedom of Information Act (1966),
- the Federal Advisory Committee Act (1972),
- the Privacy Act (1974), and
- the Sunshine in Government Act (1976).

This report offers an overview of each of these statutes, including the boundaries of their authority. This report then provides citations to additional resources, including additional Congressional Research Service reports, on each of the laws.

Public Access Laws

In 1966, Congress enacted the first law requiring public access to executive branch information. Legislative records were not included in the bill because Congress believed it made its deliberations and proceedings adequately subject to public observation, largely published its records, and otherwise was constitutionally authorized to engage in information restriction in certain circumstances.[4] For example, the Constitution explicitly permitted each house of Congress a discretion to keep portions of its journal of proceedings secret and

---

Access to information about the activities of Government is crucial to the citizen's ability to cope with the bigness and complexity of Government today.... There is no validity therefore, to the frequently heard argument that these [access to executive-branch information] proposals impinge on executive privilege for they would not affect the proper exercise of authority of the President and department heads. (p. 4).

[4] By explicit exclusion, Congress and the courts are not subject to FOIA. The committees that developed FOIA—the House Committee on Government Operations and the Senate Committee on the Judiciary—were responding to perceived secrecy problems in the executive branch. Furthermore, these panels had no jurisdiction over legislation concerning congressional operations. Thus, FOIA was created, approved, and implemented with an executive branch focus. For more information on the limitations of FOIA applicability see Harold C. Relyea, "Congress and Freedom of Information: A Retrospective and a Look at the Current Issue," Government Information Quarterly, vol. 26 (2009), pp. 437-440.

disallowed the questioning of Members of Congress "in any other Place" regarding official speech or debate. Legislators also were satisfied with the openness of federal court files and hearing rooms. Thus, the departments and agencies were the principal object of government information access reform laws. Executive branch officials, however, were not supportive of these measures and, initially, did not always promote or pursue their faithful administration. The current major federal laws facilitating public access to government information are briefly described below; the full text of each statute may be consulted by using the United States Code references provided.

Freedom of Information Act (5 U.S.C. § 552)

Initially enacted in 1966 and subsequently amended, the Freedom of Information Act (FOIA) establishes for any person—corporate or individual, regardless of nationality—presumptive access to existing, unpublished agency records on any topic. The law specifies nine categories of information that may be permissibly exempted from the rule of disclosure. Agencies within the federal intelligence community are prohibited from making any record available to a foreign government or a representative of same pursuant to a FOIA request. Disputes over the accessibility of requested records may be settled, according to the provisions of the act, in federal court.[5] Pursuant to the statute, FOIA does not apply to the legislative or executive branches of the federal government or to lower levels of government.

Fees for search, review, or copying of materials may be imposed, while certain types of requesters may be granted fee waivers or reductions.[6] FOIA was amended in 1996 to provide for public access to information in an electronic form or format. These amendments are often referred to as e-FOIA.[7] In 2007, FOIA was further amended to

- redefine qualifications for fee waivers for those seeking records,
- require the National Archives and Records Administration to create an Office of Government Information Services to act as a centralized FOIA oversight office, and

[5] 5 U.S.C. § 552(4)(B). See U.S. Congress, House Committee on Government Reform, A Citizen's Guide on Using the Freedom of Information Act and the Privacy Act of 1974 to Request Government Records, H.Rept. 109-226, 109th Cong., 1st sess. (Washington: GPO, 2005).

[6] 5 U.S.C. § 552(h)(3).

[7] 5 U.S.C. § 552 note.

- require agencies to create tracking systems that allow requesters to determine the status of their information requests, among other modifications.[8]

Federal Advisory Committee Act (5 U.S.C. App.)

A 1972 statute, the Federal Advisory Committee Act (FACA), in part, requires that the meetings of all federal advisory committees serving executive branch entities be open to public observation and that all committee records be accessible to the public. The statute specifies certain categories of records and debate—identical to the record exemptions in FOIA—that could permit a committee to hold meetings that were not accessible to the public or could prohibit the release of certain committee records.[9] Disputes over the proper public notice for a committee meeting or the closing of a session may be pursued in federal court.

Committees that fit certain FACA criteria are governed by FACA's guidelines.[10] FACA was designed to eliminate duplication of committee expertise and make advisory bodies in the executive branch more transparent. Congress may decide, however, to place some or all FACA requirements on a body that it statutorily created.[11]

Privacy Act (5 U.S.C. § 552a)

Legislated in 1974, the Privacy Act, in part, established for individuals who are United States citizens or permanent resident aliens, presumptive access to personally identifiable files on themselves held by most federal agencies—generally, however, not law enforcement and intelligence entities. The statute specifies seven types of information that may permissively be exempted from the rule of access.[12] Where a file subject contends that a record contains inaccurate information about that individual, the act allows correction through a request to the agency that possesses the record. Disputes over the accessibility or accuracy of personally identifiable files may be pursued in federal court.

---

[8] P.L. 110-175. See also CRS Report R40766, Freedom of Information Act (FOIA): Issues for the 111th Congress, by Wendy R. Ginsberg.

[9] FACA cites 5 U.S.C. § 552(b), which is the section of the U.S. Code that states which records are exempted from FOIA.

[10] 41 C.F.R. Appendix to Subpart A of § 102-3.

[11] For more information on FACA, see CRS Report R40520, Federal Advisory Committees: An Overview, by Wendy R. Ginsberg.

[12] 5 U.S.C. § 552a(j) and 5 U.S.C. § 552a(k).

Government in the Sunshine Act (5 U.S.C. § 552b)

Enacted in 1976, the Sunshine Act presumptively opens the policymaking deliberations of collegially headed federal agencies—such as boards, commissions, or councils—to public scrutiny. Pursuant to the statute, agencies are required to publish advance notice of impending meetings and make those meetings publicly accessible.[13] The act includes ten conditions under which agency meetings would be exempted from the act.[14] Disputes over proper public notice of such meetings or the propriety of closing a deliberation may be pursued in federal court.

Interbranch Access

Both Congress and the judiciary have subpoena powers that can be exercised to compel the production of materials by another branch, but even these demands have sometimes been resisted.[15] In 1974, for example, a Special Prosecutor sought certain tape recordings that President Richard Nixon, on a claim of constitutional privilege, initially refused to provide. The Supreme Court, in United States v. Nixon (418 U.S. 683), disallowed the President's claim of privilege, finding it too general and overbroad and the needs of the Special Prosecutor to pursue criminal prosecutions more compelling. These tape recordings would become known as the Watergate Tapes.

Language within FOIA explicitly states that the statute does not permit agencies to withhold information from Congress. In general, interbranch disputes over access to information are often resolved through negotiation—reduction of the quantity of records initially sought, substitution of other information, alternative delivery mechanisms, or limitation of the number of individuals who will examine materials provided by another branch. Congress could use its "power of the purse" and the Senate could use its advice and consent power to leverage its information access demands. Federal courts rely upon a spirit of justice and fair play to sustain their orders for the production of information by another branch. In view of the American separation of powers model of government, such conflicts are neither unexpected nor necessarily destructive. Furthermore, they probably will continue to occur.

---

[13] 5 U.S.C. § 552b(e)(3).

[14] 5 U.S.C. § 552b(c).

[15] For example, on March 31, 2004, Senator Jim Jeffords, the then-Senate Committee on Environment and Public Works minority ranking member, said at a hearing that he was having difficulty acquiring documents from the Environmental Protection Agency even though he and the committee chairman had drafted a letter to the agency requesting that it respond to requests from either member. U.S. Congress, Senate Committee on Environment and Public Works, Nominations of the 108th Congress, 2nd Session, 108th Cong., 2nd sess., March 31, 2004, S.Hrg. 108-500 (Washington: GPO, 2004), pp. 3-4.

Statistics on Usage

FOIA

The Freedom of Information Act requires each federal agency to submit a report on or before February 1 each year to the Attorney General describing the agency's freedom of information workload. Annual reports from all of the departments and agencies are posted on the Internet by the U.S. Department of Justice at http://www.usdoj.gov/04foia/04_6.html.[16] In FY2008, The Department of Veterans Affairs reported that it received 99,333 new FOIA requests and processed 98,455 requests.[17] The Department of Justice reported receiving 59,615 requests in FY2008 and processed 61,272 requests.[18]

FACA

According to the FACA Database, which is hosted by the General Services Administration, 914 federal advisory bodies have been active in FY2009,[19] costing $357,371,463.[20]

Litigation

A certain number of requests for information under the access to information acts result in judicial action. The Administrative Office of the U.S. Courts provides statistical information on the number of FOIA cases filed in U.S. District Courts in its compendium, Judicial Business of the United States Courts, which is available on the Internet at http://www.uscourts.gov/judbus2008/appendices/C02Sep08.pdf. According to that report, 280 cases related to FOIA commenced in U.S. District Courts in 2008. According to the

[16] Data from the individual annual reports, which are posted on the Department of Justice website, are summarized in tables on the website of Public Citizen, a public interest group. Public Citizen's tables for FY2000 through FY2005 can be found at http://www.citizen.org/litigation/free_info/foic_rep/statistics/index.cfm.

[17] See http://www.va.gov/foia/report/FY2006/InitialRequests.html.

[18] U.S. Department of Justice, U.S. Department of Justice, Freedom of Information Act Annual Report, Fiscal Year 2008, Washington, DC, February 6, 2009, p. 2, http://www.usdoj.gov/oip/annual_report/2008/foiapg5.pdf.

[19] U.S. General Services Administration, Federal Advisory Committees Database, Government Statistics, FY2009, at http://fido.gov/facadatabase/rptgovtstats.asp.

[20] U.S. General Services Administration, Federal Advisory Committees Database, FY2009 Government Totals, at http://fido.gov/facadatabase/rptgovttotals.asp.

report on appellate courts,[21] 60 cases related to FOIA commenced between January 1, 2008, and September 30, 2008.

The Freedom of Information Case List, produced by the Department of Justice Office of Information and Privacy, has compiled lists of cases decided pursuant to FOIA, FACA, the Privacy Act, and the Government in the Sunshine Act. Its principal section, an alphabetical list of judicial decisions addressing access issues under FOIA and the Privacy Act, numbers nearly 5,000 entries. It was last updated in May 2002 and is available on the Internet at http://www.usdoj.gov/04foia/cl-tofc.html. Judicial Watch, a public interest group that seeks to promote transparency in government, has posted information about its own lawsuits under "Our Litigation" at http://www.judicialwatch.org/litigation.shtml. Citizens for Responsibility and Ethics in Washington (CREW), a nonprofit organization that seeks to promote government accountability, has a webpage devoted to lawsuits in which it is involved at http://www.citizensforethics.org/actions/lawsuits. EPIC, a public interest nonprofit that focuses on civil liberties and privacy issues, also has a webpage devoted to FOIA-related litigation at http://epic.org/privacy/litigation/.

Guides to Using the Information Acts

Individuals, groups, and organizations all possess a right to access some government information. Both government and private groups publish guides to the information acts in paper and on the Internet as well.

The U.S. House of Representatives Committee on Government Reform published several editions of its report, A Citizen's Guide on Using the Freedom of Information Act and the Privacy Act of 1974 to Request Government Records (H.Rept. 109-226). In addition to the text of the acts, the Citizen's Guide contains descriptions and explanations, sample document request forms, and bibliographies of related congressional and non-congressional material. The report is available at http://www.access.gpo.gov/congress/house/house07cr109.html. The General Services Administration's Federal Citizen Information Center publishes Your Right To Federal Records: Questions and Answers on the Freedom of Information Act and Privacy Act. Like the Citizen's Guide, this publication contains explanations, samples, and texts, although in less detail than found in the Citizen's Guide. Your Right to Federal Records is available on the Internet at http://www.pueblo.gsa.gov/cic_text/fed_prog/foia/foia.pdf.

The Justice Department is the agency responsible for overseeing and coordinating administration of the Freedom of Information Act. Its website at http://www.usdoj.gov/04foia/index.html includes extensive material about the

[21] At http://www.uscourts.gov/judbus2008/appendices/B01ASep08.pdf.

act, statistics on its usage, guidelines for making requests, and freedom of information contacts at other federal agencies.

Among many non-governmental groups that publish information about freedom of information are Public Citizen and National Security Archive. Public Citizen maintains the "Freedom of Information Clearinghouse" on its website at http://www.citizen.org/litigation/free_info/. The National Security Archive website contains a number of FOIA guides, including, "Effective FOIA Requesting for Everyone: A National Security Archive Guide" published in January 2009 at http://www.gwu.edu/~nsarchiv/nsa/foia/foia_guide.html.

Records on each of the active federal advisory bodies is available on the General Services Administration's FACA Database at http://fido.gov/facadatabase/. The website includes each committee's charter, information on the members of each committee and their contact information, and cumulative data on the cost of federal advisory bodes.

Selected CRS Reports

CRS Report R40520, Federal Advisory Committees: An Overview, by Wendy R. Ginsberg

CRS Report R40238, Presidential Records: Issues for the 111th Congress, by Wendy R. Ginsberg, Presidential Records: Issues for the 111th Congress, by Wendy Ginsberg

CRS Report RL33502, Protection of National Security Information, by Jennifer K. Elsea

CRS Report R40766, Freedom of Information Act (FOIA): Issues for the 111th Congress, by Wendy R. Ginsberg

CRS Report RL33670, Protection of Security-Related Information, by Gina Stevens and Todd B. Tatelman

CRS Report RL30240, Congressional Oversight Manual, by Frederick M. Kaiser et al.

Selected Additional Resources

Sam Archibald. "The Early Years of the Freedom of Information Act—1955 to 1974." PS: Political Science and Politics, Vol. 26, no. 4 (1993): 726-731.

Herbert N. Foerstel. Freedom of Information and the Right To Know: The Origins and Applications of the Freedom of Information Act. Westport, CT: Greenwood Press, 1999.

Harry A. Hammitt, Marc Rotenberg, and John A. Verdi, et al., Litigation Under the Federal Open Government Laws 2008: Covering the Freedom of Information Act, the Privacy Act, the Government in the Sunshine Act, and the Federal Advisory Committee Act, 24th ed. (Washington, DC: EPIC Publications, 2008)

Harry A. Hammitt, Access Reports: Freedom of Information, at http://www.accessreports.com/.

Daniel N. Hoffman. Governmental Secrecy and the Founding Fathers: A Study in Constitutional Controls. Westport, CT: Greenwood Press, 1981.

Public Information Provision in the Digital Age: Implementation and Effects of the U.S. Freedom of Information Act. Santa Monica, CA: RAND, 2001.

U.S. Congress. House. Committee on Government Reform. A Citizen's Guide on Using the Freedom of Information Act and the Privacy Act of 1974 to Request Government Records. 109th Congress, first session. H.Rept. 109-226. Washington: GPO, 2005, at http://fas.org/sgp/foia/ citizen.pdf.

U.S. Congress. Senate. Committee on Governmental Affairs. Federal Advisory Committee Act (Public Law 92-463)—Source Book: Legislative History, Texts, and Other Documents. Committee Print. 95th Congress, second session. Washington: GPO, 1978.

U.S. Congress. Senate. Committee on Governmental Affairs. Government in the Sunshine Act: History and Recent Issues. Committee Print. 101st Congress, first session. Washington: GPO, 1989.

U.S. Department of Justice, Department of Justice Guide to the Freedom of Information Act (2009 Edition), Washington, DC, 2009, http://www.usdoj.gov/oip/foia_guide07/introduction.pdf.

U.S. Department of Justice and U.S. General Services Administration. Your Right to Federal Records: Questions and Answers on the Freedom of Information Act and Privacy Act, May 2006. Washington: GSA Federal Citizen Information Center, 2006.

Freedom of Information Act (FOIA): Issues for the 111th Congress, R40766 (August 12, 2009).

WENDY R. GINSBERG & HAROLD C. RELYEA, CONGRESSIONAL RESEARCH SERV., FREEDOM OF INFORMATION ACT (FOIA): ISSUES FOR THE 111TH CONGRESS (2009), *available at* http://www.intelligencelaw.com/library/secondary/crs/pdf/R40766_8-12-2009.pdf.

Wendy R. Ginsberg
Analyst in Government Organization and Management
wginsberg@crs.loc.gov, 7-3933

Acknowledgments
Parts of this report are adapted from CRS Report RL32780, Freedom of Information Act (FOIA) Amendments: 110th Congress, by Harold C. Relyea.

August 12, 2009
Congressional Research Service

7-5700
www.crs.gov
R40766

Summary

Enacted in 1966 after 11 years of investigation and legislative development in the House—and nearly 6 years of such consideration in the Senate—the Freedom of Information Act (FOIA; 5 U.S.C. §552) replaced the public information section of the Administrative Procedure Act. FOIA was designed to enable any person to request, without explanation or justification, access to existing, identifiable, unpublished, executive branch agency records. The statute specified nine categories of information that may be exempted from the rule of disclosure. Pursuant to FOIA, disputes over the accessibility of requested records could be settled ultimately in court.

The statute has become a widely used tool of inquiry and information gathering for various sectors of American society—particularly the press, businesses, scholars, attorneys, consumers, and activists—as well as some foreign interests. The response to a request may ultimately involve a few sheets of paper, several linear feet of records, or information in an electronic format. Assembling responses requires staff time, search and duplication efforts, and other resource commitments. Agency information management professionals are responsible for efficiently and economically responding to FOIA requests, doing so in the sensitized homeland security milieu. Agencies may negotiate with a requester to

narrow a request's scope, or the agency may explain and justify why certain records cannot be supplied. Simultaneously, agency FOIA response costs need to be kept reasonable. The perception that FOIA standards are not properly met may result in proposed new corrective amendments to the statute.

FOIA has been refined with direct amendments in 1974, 1976, 1986, and 1996. In addition, the 110th Congress enacted the OPEN Government Act of 2007 (P.L. 110-175), which modified FOIA and prompted disagreements with the executive branch. Among the statute's modifications was the creation of both a more inclusive definition for a member of the news media and a more inclusive policy on waiving request processing fees. The legislation more clearly defined the time limits for agencies to respond to requests for information and required the creation of an Office of Government Information Services (OGIS) within the National Archives and Records Administration (NARA). After conflict in 2008 with the George W. Bush Administration over whether the OGIS should be placed in NARA or the Department of Justice, President Barack Obama's FY2010 budget requested $1.4 million and six full-time employees for OGIS implementation within NARA.

In his first full day in office, President Obama issued a memorandum to federal departments and agencies encouraging more collaboration, participation, and transparency in the federal government. As a follow-up to the January 21, 2009, memorandum, the Attorney General drafted new guidelines for agency and department heads on use and implementation of FOIA. The Obama Administration also conducted a three-phase online information-gathering effort linked to its OPEN Government Directive. The directive sought public input on ways to make FOIA and other policies and operations of federal government more effective and efficient.

In the 111th Congress, several bills that directly address FOIA have been introduced, including legislation that would exempt photographs of the treatment of detainees held by the Armed Forces from public disclosure pursuant to FOIA, and a bill that would require the archivist to issue more detailed regulations on the classification of government records.

This report will offer a history of FOIA, discuss current implementation of FOIA statutes, and outline pending FOIA legislation. The report will be updated as events warrant.

Introduction

The Freedom of Information Act (FOIA; 5 U.S.C. § 552), often referred to as the embodiment of "the people's right to know" about the activities and operations of government, statutorily established a presumption of public access to information held by federal departments and agencies. Enacted in 1966 to replace the public information section of the Administrative Procedure Act (APA; 5 U.S.C. Subchapter II), FOIA allows any person—individual or corporate,

regardless of citizenship—to request, without explanation or justification, existing, identifiable, unpublished agency records on any topic.[22]

At the time of its enactment, FOIA was regarded as a somewhat revolutionary law. Only two other nations—Sweden and Finland—had comparable laws, and in neither case was the law as sweeping as the new American model. The law's premise reversed the burden of proof that had existed under the public information section of the APA. Under the APA, requesters had to establish a justification or a need for the information being sought. Under FOIA, in contrast, access was presumed. Instead, agencies had to justify denying a requester access to information. FOIA provided clear exceptions to access, protecting certain types of information from disclosure.

FOIA was also revolutionary in another regard. The product of 11 years of investigation, legislative development, and deliberation in the House and nearly 6 years of such consideration in the Senate, the statute was almost exclusively a congressional creation. No executive branch department or agency head had supported the legislation, and President Lyndon B. Johnson was reported to be reluctant to sign the measure.[23] Because the law was not enthusiastically received by the executive branch, supporters maintained that FOIA implementation and use sometimes required close attention from congressional overseers. The statute has been subsequently refined with direct amendments in 1974, 1976, 1986, and 1996. Other substantial modifications were enacted in 2007.

Congress, at times, has encountered executive-branch resistance to its FOIA designs. The George W. Bush Administration, for example, disregarded Congress's statutory provision creating an Office of Government Information Services (OGIS) within the National Archives and Records Administration (NARA). In his FY2009 budget request, former President Bush did not seek funding for the office and suggested it be moved from NARA to the Department of Justice.[24] The 111th Congress responded by including $1 million in the

---

[22] See 5 U.S.C. § 552.

[23] See Samuel J. Archibald, "The Freedom of Information Act Revisited," Public Administration Review, vol. 39, July-August 1979, pp. 311-318. See also "NOW With Bill Moyers – Politics and Economy: Bill Moyers on the Freedom of Information Act," at http://www.pbs.org/now/commentary/moyers4.html. According to Moyers, Johnson "had to be dragged kicking and screaming to the signing ceremony. He hated the very idea of the Freedom of Information Act; hated the thought of journalists rummaging in government closets; hated them challenging the official view of reality." See also Harold C. Relyea, "Federal Freedom of Information Policy: Highlights of Recent Developments," Government Information Quarterly, vol. 26 (January 12, 2009), p. 314.

[24] The proposal appears in a provision (Section 519) in the President's budget submission for the FY2009 appropriations for the Department of Commerce. U.S. Office of Management and Budget, Budget of the United States Government, Fiscal Year 2009, Appendix (Washington:

explanatory statement that accompanies the FY2009 Omnibus Appropriation Act (P.L. 111-8) for the OGIS to be established within NARA.[25] The Barack Obama Administration's FY2010 budget request included $1.4 million and six full-time employees for OGIS implementation within NARA. Both House and Senate appropriators supported the President's request.[26]

The Government Accountability Office (GAO) found in March 2008, that the volume of FOIA requests in the federal government was increasing, but not as rapidly as it had been increasing in previous years.[27] Moreover, the report found that the backlog of FOIA requests continued to grow between 2005 and 2006. Among the agencies in which the FOIA backlog increased was the Department of Homeland Security's (DHS's) Citizenship and Immigration Services, which handled 89% of DHS's total FOIA requests.

Each new presidential administration has applied FOIA's statutes differently. As recent examples, the George W. Bush Administration, supported "full and deliberate consideration of the institutional, commercial, and personal privacy interests" that surround any requests,[28] while the current Administration of Barack Obama encouraged agencies "to adopt a presumption in favor of disclosure."[29]

OMB, 2008), p. 239. See also Elizabeth Williamson, "Is Ombudsman Already in Jeopardy?" Washington Post, February 6, 2008, p. A17, at http://www.washingtonpost.com/wp-dyn/content/ article/2008/02/05/AR2008020502840.html.

[25] U.S. Congress, House Committee on Appropriations, Explanatory Statement to Accompany Omnibus Appropriations Act, 2009, committee print, 111th Cong., 1st sess., p. 988, at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=111_cong_house_committee_prints&docid=f:47494d.pdf.

[26] U.S. Congress, House Committee on Appropriations, Subcommittee on Financial Services and General Government, Financial Services and General Government Appropriation Bill, 2010, report to accompany H.R. 3170, 111th Cong., 1st sess., July 10, 2009, H.Rept. 111-202 (Washington: GPO, 2009); and U.S. Congress, Senate Committee on Appropriations, Subcommittee on Financial Services and General Government, Financial Services and General Government Appropriations Bill, 2010, report to accompany S. 1432, 111th Cong., 1st sess., July 9, 2009, S.Rept. 11143 (Washington: GPO, 2009), p. 102.

[27] U.S. Government Accountability Office, Freedom Of information Act: Agencies are Making Progress in Reducing Backlog, but Additional Guidance is Needed, GAO-08-344, March 2008, http://www.gao.gov/new.items/d08344.pdf. According to the report, from 2002 through 2006, FOIA requests increased 23%. From 2005 to 2006, requests increased between 1% and 2%, depending on the agency.

[28] Memorandum from John Ashcroft, Attorney General, to Heads of All Federal Departments and Agencies, October 12, 2001, http://www.doi.gov/foia/foia.pdf.

[29] Memorandum from President Barack Obama For Heads of Executive Departments and Agencies, January 21, 2009, http://www.whitehouse.gov/the_press_office/FreedomofInformationAct/.

Several bills have been introduced in the 111th Congress that directly address FOIA. On March 3, 2009, Representative Stephen Driehaus introduced the Reducing Information Control Designations Act (H.R. 1323). Although the bill concentrates its efforts on streamlining agency classification standards, it also requires agencies to ensure that their internal classification system does not hinder the disclosure of information. The act passed the House and was referred to the Senate Committee on Homeland Security and Governmental Affairs. On March 17, 2009, Senator Patrick Leahy introduced the OPEN FOIAAct of 2009 (S. 612), which would require agencies to explicitly state which exemption they are claiming when they deny a FOIA request. The bill was referred to the Senate Committee on the Judiciary. In addition, six bills—three in the House and three in the Senate (H.R. 2712; H.R. 2875; H.R. 3015; S. 1100; S. 1260; and S. 1285)—have been introduced that would exempt photographs of the treatment of detainees held by the Armed Forces from public disclosure pursuant to FOIA. Another bill (H.R. 2450) would require private, state, and local incarceration and detention facilities to comply with FOIA requirements. On May 15, 2009, Representative Sheila Jackson-Lee introduced a bill that would require all private, state, and locally run incarceration and detention facilities be subject to FOIA. The bill has been referred to the House Committee on the Judiciary, Subcommittee on Crime, Terrorism, and Homeland Security.

This report includes a brief history of FOIA, discusses subsequent modifications of FOIA, addresses statutory changes to FOIA that have not yet been implemented, examines Obama Administration efforts to modify the act, and outlines possible legislative issues related to the act.

FOIA History[30]

FOIA applies only to the departments and agencies of the federal executive branch. This scope has been shaped by both historical and constitutional factors. During the latter half of the 1950s, when congressional subcommittees began examining government information availability, the practices of the federal departments and agencies were a primary focus. The public, the press, and even some congressional committees and subcommittees were sometimes rebuffed when seeking information from executive branch entities.

Although presidential records might have been of interest to Congress and the public, the exercise of so-called "executive privilege"—the withholding of information based upon his authority as the head of the executive branch—was a matter of some constitutional complexity and uncertainty, and had not resulted

[30] For a more in-depth legislative history of FOIA, see CRS Report RL32780, Freedom of Information Act (FOIA) Amendments: 110th Congress, by Harold C. Relyea.

in widespread public concern.[31] The President's records were, therefore, exempted from the forthcoming FOIA legislation.[32] The accessibility of federal court records was also not an issue. Access to congressional records were not closely scrutinized, since the subcommittees probing the executive branch in this regard lacked jurisdiction over the whole legislative branch.[33] In a 1955 hearing, Representative John E. Moss, chairman of the newly created Special Subcommittee on Government Information, delineated the scope of the investigation, saying,

> *We are not studying the availability of information from Congress, although many comments have been made by the press in that field, but we are taking a long, hard look at the amount of information available from the executive and independent agencies for both the public and its elected representatives.*[34]

Eleven years after that hearing, FOIA was enacted, and was applicable only to federal, executive-branch departments and agencies. Some Members and academics have asserted that, in the case of Congress, the secret journal clause or

---

[31] See U.S. Congress, Senate Committee on the Judiciary, The Power of the President to Withhold Information from Congress, committee print, 85th Cong., 2nd sess. (Washington: GPO, 1958-1959), 2 parts. Legislative-branch agencies, like the Government Accountability Office, the Congressional Research Service, and the Congressional Budget Office are not subject to FOIA.

[32] For more information on presidential records and vice presidential records see CRS Report R40238, Presidential Records: Issues for the 111th Congress, by Wendy R. Ginsberg.

[33] At present, the definition of agency for FOIA (found at 5 U.S.C. § 551) makes the requirements of the statute applicable only to an "agency," which "means each authority of the Government of the United States, whether or not it is within or subject to review by another agency, but does not include
(A) the Congress; or

(B) the courts of the United States[.]" By explicit exclusion, Congress and the courts are not subject to FOIA. The committees that developed FOIA—the House Committee on Government Operations and the Senate Committee on the Judiciary—were responding to perceived secrecy problems in the executive branch. Furthermore, these panels had no jurisdiction over legislation concerning congressional operations. Thus, FOIA was created, approved, and implemented with an executive branch focus. For more information on the limitations of FOIA applicability see Harold C. Relyea, "Congress and Freedom of Information: A Retrospective and a Look at the Current Issue," Government Information Quarterly, vol. 26 (2009), pp. 437-440.

[34] U.S. Congress, House Committee on Government Operations, Availability of Information from Federal Departments and Agencies, hearing, 84th Cong., 1st sess., November 7, 1955 (Washington: GPO, 1956), p. 3.

the speech or debate clause of the Constitution[35] could be impediments to the effective application of FOIA to Congress.[36]

FOIA Exemptions

FOIA exempts nine categories of records from the statute's rule of disclosure. These exceptions detail certain restrictions. The exemptions are as follows:

1. Information properly classified for national defense or foreign policy purposes as secret under criteria established by an executive order
2. Information relating solely to agency internal personnel rules and practices
3. Data specifically excepted from disclosure by a statute which either requires that matters be withheld in a non-discretionary manner or which establishes particular criteria for withholding or refers to particular types of matters to be withheld
4. Trade secrets and commercial or financial information obtained from a person that is privileged or confidential
5. Inter- or intra-agency memoranda or letters that would not be available by law except to an agency in litigation
6. Personnel, medical, or similar files the disclosure of which would constitute an unwarranted invasion of personal privacy
7. Certain kinds of investigatory records compiled for law enforcement purposes
8. Certain information relating to the regulation of financial institutions
9. Geological and geophysical information and data. (5 U.S.C. § 552(b)) Some of these exemptions, such as the one concerning trade secrets and commercial or financial information, have been litigated and undergone considerable judicial interpretation.[37]

---

[35] Art. I, Sec. 5, which directs each house of Congress to keep a journal of its proceedings and publish the same, except such parts as may be judged to require secrecy, has been interpreted to authorize the House and the Senate to keep other records secret. Art. 1, Sec. 6, which specifies that Members of Congress, "for any Speech or Debate in either House ... shall not be questioned in any other Place," might be regarded as a bar to requests to Members for records concerning their floor, committee, subcommittee, or legislative activity.

[36] See U.S. Congress, Senate Committee on Governmental Affairs, To Eliminate Congressional and Federal Double Standards, hearing, 96th Cong., 1st sess., September 20, 1979 (Washington: GPO, 1979); Harold C. Relyea, "Public Access to Congressional Records: Present Policy and Reform Considerations," Government Information Quarterly, vol. 2, 1985, pp. 235-256.

[37] For sources concerning judicial interpretation of FOIA, see Harry A. Hammitt, Marc Rotenberg, and John A. Verdi and Mark S. Zaid, eds., Litigation Under the Federal Open Government Laws: 2008 (Washington: EPIC Publications and The James Madison Project, 2008); James T. O'Reilly, Federal Information Disclosure, third edition (Eagan, MN: West Group, first published in 2000, with supplements); U.S. Department of Justice, Freedom of Information Act Guide, March 2007 ed. (Washington, DC: GPO, 2007).

A person denied access to requested information, in whole or in part, may make an administrative appeal to the head of the agency for reconsideration. After this step, an appeal for further consideration of access to denied information may be made in federal district court.[38] The newly created Office of Government Information Services (OGIS) may also provide "mediation services to resolve disputes between persons making requests under this section and administrative agencies as a non-exclusive alternative to litigation."[39] The OGIS services are advisory only and are non-binding.

Fees for Service

Agencies responding to FOIA requests are permitted by statute to charge fees for certain administrative activities, such as records searching, reviewing, and duplicating. The amount of the fee will depend upon the type of requester, specifically whether the request is made by a commercial user, an educational or noncommercial scientific institution whose purpose is scholarly or scientific research, a news media representative, or the general public. Moreover, certain requestors may be exempted from FOIA-related fees.[40] Requested records may be furnished by an agency without any charge or at a reduced cost, pursuant to FOIA, "if disclosure of the information is in the public interest because it is likely to contribute significantly to public understanding of the operations or activities of the government and is not primarily in the commercial interest of the requester."[41] Requesters seeking a fee exemption must explicitly request it, and the agency then determines whether they qualify.

The George W. Bush Administration

Executive Order 13392, "Improving Agency Disclosure of Information"

On December 19, 2005, George W. Bush issued E.O. 13392 to ensure appropriate agency disclosure of information.[42] Executive Order 13392 directed all federal agencies subject to FOIA to, among other things,

---

[38] 5 U.S.C. § 552(4)(B). See U.S. Congress, House Committee on Government Reform, A Citizen's Guide on Using the Freedom of Information Act and the Privacy Act of 1974 to Request Government Records, H.Rept. 109-226, 109th Cong., 1st sess. (Washington: GPO, 2005).

[39] 5 U.S.C. § 552(h)(3).

[40] Ibid.

[41] 5 U.S.C. § 552(a)(4)(A)(iii). Additional information about the OGIS is provided later in this report.

[42] Executive Order 13392, 70 Fed. Reg. 75,373 (Dec. 14, 2005), http://edocket.access.gpo.gov/2005/pdf/05-24255.pdf.

(1) Designate a senior agency official at each agency (at the Assistant Secretary or equivalent level), to serve as the Chief FOIA Officer of that agency.
(2) Establish one or more FOIA Requester Service Centers (Center) to serve as the first place that FOIA requesters can contact to seek both information concerning the status of their FOIA requests and appropriate information about the agency's FOIA responses. The Center was required to include appropriate staff to receive and respond to inquiries from FOIA requesters.
(3) Designate one or more agency officials as FOIA Public Liaisons. FOIA Public Liaisons were required to serve as supervisory officials to whom a FOIA requester could raise concerns about the service the FOIA requester received from the Center, following an initial response from the Center staff.
(4) Conduct a review of the agency's FOIA operations to determine whether agency practices are consistent with the policies set forth in the Executive Order.
(5) Develop, in consultation as appropriate with the staff of the agency (including FOIA Public Liaisons), the Attorney General, and the OMB Director, an agency-specific plan to ensure that the agency's administration of FOIA is in accordance with applicable law and the policies set forth in the Executive Order.
(6) Submit a report to the Attorney General and the OMB Director that summarized the results of the agency's review and included a copy of the agency's FOIA Improvement Plan under the Executive Order.
(7) Include in the agency's annual FOIA reports for fiscal years 2006 and 2007 a report on the agency's development and implementation of its FOIA Improvement Plan and on the agency's performance in meeting the milestones set forth in that plan, consistent with Department of Justice guidance.

110th Congress Legislative Reform Efforts

Building on legislation from previous Congresses, Members in the 110th Congress introduced several pieces of FOIA-related legislation. One bill, the Freedom of Information Act Amendments of 2007, was enacted.[43] Among other changes, the bill codified the requirement that all agencies have a chief FOIA officer. After the bill's enactment, however, controversy erupted between the legislative and executive branch over implementation of certain requirements in the bill. This section includes the bill's legislative history and describes the implementation controversy that ensued.

OPEN Government Act of 2007

[43] P.L. 110-175.

On March 5, 2007, Representative Lamar Smith introduced the House version of the OPEN Government Act of 2007 (H.R. 1326).[44] The bill was referred to the House Committee on Oversight and Government Reform, Subcommittee on Information Policy, Census, and National Archives. No further action was taken on that version of the OPEN Government Act. Senator Patrick Leahy then introduced Senate version of the act (S. 849) on March 13. A hearing on the Senate bill was held by the Committee on the Judiciary on March 14. The committee ordered the bill to be reported favorably on April 12, and the report was printed on April 30.[45] The bill was not brought to the Senate floor for consideration or a final vote because of concerns arising from Department of Justice objections, which were resolved just before the Senate adjourned for the August recess. The bill came before the Senate by unanimous consent on August 3, was amended, and passed by unanimous consent. Among other changes, the bill sought to do the following:

- redefine "a representative of the news media";[46]
- modify the conditions for when a complainant has substantially prevailed relative to the recovery of attorney fees and litigation costs;[47]
- create new language concerning the time limits for agencies to act on requests;[48]
- modify the requirements for request tracking arrangements;[49]

---

[44] For more information on the origins of the OPEN Government Act of 2007 and a legislative history of its origins, see CRS Report RL32780, Freedom of Information Act (FOIA) Amendments: 110th Congress, by Harold C. Relyea.

[45] Ibid., March 13, 2007, p. S3066; U.S. Congress, Senate Committee on the Judiciary, Open Government Act of 2007, report to accompany S. 849, 110th Cong., 1st sess., S.Rept. 110-59 (Washington: GPO, 2007).

[46] The bill stated that independent journalists are not barred from obtaining fee waivers solely because they lack an institutional affiliation with a recognized news media organization.

[47] This provision responded to the ruling in Buckhannon Board and Care Home, Inc. v. West Virginia Dep't of Health and Human Services, 532 U.S. 598 (2001), in which the Supreme Court eliminated the so-called "catalyst theory" of attorney fee recovery under certain federal civil rights laws, and which prompted concern that the holding could be extended to FOIA cases. The new definition required the government to pay the complainant's attorney fees if the records were required to be released by court or other administrative order as well as if the complainant's lawsuit prompted the agency to change its decision to release the records even without such an order.

[48] If an agency failed to comply with the new 20-day limit, which was defined as beginning when the agency first received the request, the agency would not be permitted to assert an exemption for the record sought (pursuant to 5 U.S.C. § 552(b)) unless such disclosure would endanger national security or disclose personal information protected by The Privacy Act (5 U.S.C. § 552a).

[49] Pursuant to the bill, agencies would have been required to establish tracking systems and assign requests tracking numbers within 10 days of the agency's receipt of the request. Requesters could

- modify the provision amending the third exemption of the act concerning statutory protections of information;[50] and
- recharter of the proposed Office of Government Information Services as an entity within the National Archives and Records Administration.[51]

The bill was received in the House on September 4, 2007, but was held at the desk. No further action was taken on the bill.

Freedom of Information Act Amendments of 2007

On March 5, 2007—four months prior to S. 849's receipt in the House—Representative William Clay introduced a modified House version of the OPEN Act (H.R. 1309), entitled the Freedom of Information Act Amendments of 2007. H.R. 1309 included explicit language stating the "policy of the Federal Government is to release information to the public in response to a request under" FOIA "if such release is required by law; or if such release is allowed by law and the agency concerned does not reasonably foresee that disclosure would be harmful to an interest protected by an applicable exemption."

When H.R. 1309 came under consideration by the Committee on Oversight and Government Reform during a March 8, 2007, markup, an amendment to the bill was approved. The added provision would require agencies to indicate, for each redaction made in a record, which specific FOIA exemption was involved. The amended legislation was then approved for House floor consideration.

Negotiations to resolve differences between H.R. 1309 and S. 849 continued through the fall. One of the more contentious issues concerned who would be entitled to payments if an agency changed its position concerning the release of records after a requester challenged an agency denial in court but prior to any court determination. While the House bill provided that such payments would come from annually appropriated agency funds, the lack of such specificity in the

---

then track the progress of their request via the number. Agencies would have also had to establish a telephone or Internet system to allow requesters to obtain information on the status of their individual requests, including an estimated date on which action on the request will be completed.

[50] The third exemption to the rule of disclosure exempts matters that are "specifically exempted from disclosure by statute [other than the Privacy Act], provided that such statute (A) requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld." 5 U.S.C. § 552(b)(3). The amendment would have affected any FOIA exemption that was adopted by Congress after enactment of S. 849. This provision was later offered in separate legislation as well as in future congressional sessions, including the 111th Congress.

[51] The OGIS would review agency policies and procedures, audit agency performance, recommend policy changes, and mediate disputes between FOIA requesters and agencies with a view to alleviate the need for litigation, while not limiting the ability of requester to litigate FOIA claims.

Senate bill posed the strong possibility that it would trigger "pay-as-you-go" objections in the House.[52] On December 6, Senator Leahy, with Senator Cornyn as a cosponsor, introduced S. 2427, a revised version of S. 849 that contained the language of the House bill concerning the source of attorney fees payments.[53] On December 14, a slightly revised version of this bill, addressing other House concerns, was introduced by Senator Leahy, with 17 bipartisan cosponsors, as S. 2488. That same day, the Senate considered the bill, and approved it without amendment by unanimous consent.[54] As adopted by the Senate, the bill amended FOIA as follows:

- redefined "representative of the news media" and "news" for purposes of request processing fees, and specified a freelance journalist as working for a news media entity if the journalist can demonstrate a solid basis for expecting publication through that entity;
- provided that, for purposes of awarding attorney fees and litigation costs, a FOIA complainant has substantially prevailed in a legal proceeding to compel disclosure if such complainant obtained relief through either (1) a judicial order or an enforceable written agreement or consent decree, or (2) a voluntary or unilateral change in position by the agency if the complainant's claim is not substantial;
- prohibited the Treasury Claims and Judgment Fund from being used to pay reasonable attorney fees in cases where the complainant has substantially prevailed, and required fees to be paid only from funds annually appropriated for authorized purposes for the federal agency against which a claim or judgment has been rendered;
- directed the Attorney General to (1) notify the Special Counsel of civil actions taken for arbitrary and capricious rejections of requests for agency records, and (2) submit annual reports to Congress on such civil actions, while also directing the Special Counsel to submit an annual report on investigations of agency rejections of FOIA requests;
- required the 20-day period during which an agency must determine whether to comply with a FOIA request to begin on the date the request is received by the appropriate component of the agency, but no later than 10 days after the request is received by any component that is designated to receive FOIA requests in the agency's FOIA regulations; and prohibited the agency from halting the count of the 20-day period by the agency, except (1) that the agency may make one request to the requester for clarifying information and halt the 20-day period while awaiting such information, or (2) if necessary to clarify with the requester issues

[52] For more information on Pay-As-You-Go procedures, see CRS Report RL32835, PAYGO Rules for Budget Enforcement in the House and Senate, by Robert Keith and Bill Heniff Jr.

[53] Congressional Record, daily edition, vol. 153, Dec. 6, 2007, pp. S14853-S14855.

[54] Ibid., Dec. 14, 2007, pp. S15701-S15704.

regarding fee assessment, the agency may halt the 20-day period while negotiating the fee.

- prohibited an agency from assessing search or duplication fees if it failed to comply with time limits, provided that no unusual or exceptional circumstances apply to the processing of the request, and requires each agency to make available its FOIA Public Liaison (see below), who shall assist in the resolution of any disputes between the agency and the requester;
- required agencies to establish (1) a system to assign an individualized tracking number for each FOIA request received that will take longer than 10 days to process, and (2) a telephone line or Internet service that provides information on the status of a request;
- revised annual reporting requirements on agency compliance with FOIA to require information on (1) FOIA denials based upon particular statutory provisions, (2) response times, and (3) compliance by the agency and by each principal component thereof; and requires agencies to make the raw statistical data used in reports electronically available to the public upon request;
- redefined "record" under FOIA to include any information maintained by an agency contractor;
- required establishment within the National Archives and Records Administration an Office of Government Information Services (OGIS) to (1) review compliance with FOIA policies, (2) recommend policy changes to Congress and the President, and (3) offer mediation services between FOIA requesters and agencies as a non-exclusive alternative to litigation; and authorizes the OGIS to issue advisory opinions if mediation fails to resolve a dispute;
- required each agency to designate a chief FOIA officer, who shall (1) have responsibility for FOIA compliance, (2) monitor FOIA implementation, (3) recommend to the agency head adjustments to agency practices, policies, personnel, and funding to improve implementation of FOIA, and (4) facilitate public understanding of the purposes of FOIA's statutory exemptions; and requires agencies to designate at least one FOIA public liaison, who shall be appointed by the chief FOIA officer to (1) serve as an official to whom a FOIA requester can raise concerns about service from the FOIA Requester Center, and (2) be responsible for assisting in reducing delays, increasing transparency and understanding of the status of requests, and assisting in the resolution of disputes;
- required the Office of Personnel Management to report to Congress on personnel policies related to FOIA; and
- required the identification of the FOIA exemption(s) relied upon to redact information from records provided in response to a FOIA request.

The Senate-approved bill was received in the House on December 17, and it was referred to the Committee on Oversight and Government Reform. The following day, the measure was considered by the House under a suspension of the rules,

agreed to by voice vote, and cleared for the President.[55] The legislation was signed into law by then-President George W. Bush on December 31, 2007.[56]

FOIA Amendment Implementation

Less than a month after passage of the Freedom of Information Act Amendments of 2007, Senator Patrick Leahy, the principal Senate proponent of the FOIA-reform legislation, noted to his colleagues that OMB officials had indicated that they intended to place in the Department of Justice budget for FY2009 all of the funding Congress had authorized by the new law for the OGIS within NARA. Some Members and open government organizations were concerned that OMB's desired arrangement could give DOJ control over the OGIS, perhaps to the point of eradicating it. DOJ, could, for example, allocate OGIS funds to its own Office of Information and Privacy, which oversees FOIA compliance by federal agencies.[57] In creating the OGIS, legislators had consciously placed it outside of the Department of Justice, which represents agencies sued by FOIA requesters.

Calling the OMB's attempt to place the OGIS within DOJ "not only contrary to the express intent of the Congress, but ... also contrary to the very purpose of this legislation," Senator Leahy expressed hope "that the administration will reconsider this unsound decision and enforce this law as the Congress intended."[58] OMB declined to comment on the matter prior to the formal presentation of the President's budget to Congress on February 4, 2008.

President George W. Bush requested the following as part of Title V, General Provisions, of the Commerce, Justice, Science, and Related Agencies Appropriations legislation for FY2009:

> *Sec. 519. The Department of Justice shall carry out the responsibilities of the office established in 5 U.S.C. 552(h), from amounts made available in the Department of Justice appropriation for "General Administration Salaries and*

---

[55] Ibid., Dec. 18, 2007, pp. H16788-H16792.

[56] P.L. 110-175.

[57] See U.S. Senator Patrick Leahy, "Leahy: FOIA Ombudsman Belongs At Archives, Not DOJ," press release, February 14, 2008, http://leahy.senate.gov/press/200802/021408a.html; and Citizen Media Law Project, "Bush Refuses to Fund New FOIA Ombudsman, Takes the Heart Out of Open Government Reform Law," weblog, February 7, 2008, at http://www.citmedialaw.org/blog/2008/bush-refuses-fund-new-foia-ombudsman-takes-heart-out-open-governmentreform-law.

[58] Congressional Record, daily edition, vol. 154, Jan. 23, 2008, pp. S201-S202; Dan Friedman, "Senators Say White House Plans to Eliminate Special FOIA Office," CongressDaily, Jan. 25, 2008, available at http://www.govexec.com/ story_page_pf.cfm?articleid=39120&dcn=e_gvet.

> *Expenses." In addition, subsection (h) of section 552 of title 5, United States Code, is hereby repealed, and subsections (i) through (l) are redesignated as (h) through (k).*[59]

The office established in 5 U.S.C. §552(h) is the OGIS. The Department of Justice, which would have been vested with carrying out the responsibilities of that office, would have been authorized to utilize funds from its general administration appropriation to do so. House appropriators subsequently rejected this language. Both House and Senate appropriators recommended $1 million go to OGIS. The Omnibus Appropriations Act, 2009 (P.L. 111-8) did not explicitly mention OGIS.[60] President Barack Obama's FY2010 budget requested $1.4 million and six full-time employees for OGIS implementation within NARA. In the report to accompany the FY2010 Financial Services and General Government appropriations bill, the Senate Committee on Appropriations recommended $1.4 million for OGIS.[61] The House report does not explicitly mention OGIS, but it does recommend funding NARA at the same levels requested by the President.

The Obama Administration

On January 21, 2009, President Barack Obama issued a "Memorandum for the Heads of Executive Departments and Agencies" on FOIA. In the memorandum, Obama stated that FOIA "should be administered with a clear presumption: In the face of doubt, openness prevails."[62] The memorandum stated that under the new administration:

> *All agencies should adopt a presumption in favor of disclosure, in order to renew their commitment to the principles embodied in FOIA, and to usher in a new era of open Government. The presumption of disclosure should be applied to all decisions involving FOIA.*[63]

---

[59] U.S. Office of Management and Budget, Budget of the United States Government, Fiscal Year 2009—Appendix (Washington: GPO, 2008), p. 239.

[60] U.S. Congress, House Committee on Appropriations, Financial Services and General Government Appropriations Bill, 2009, committee print, 110th Cong., 2nd sess. (Washington: GPO, 2008), pp. 80-81.

[61] U.S. Congress, Senate Committee on Appropriations, Subcommittee on Financial Services and General Government, Financial Services and General Government Appropriations Bill, 2010, report to accompany S. 1432, 111th Cong., 1st sess., July 9, 2009, S.Rept. 111-43 (Washington: GPO, 2009), p. 102.

[62] Barack Obama, U.S. President, Memorandum for the Heads of Executive Departments and Agencies, January 21, 2009, at http://www.whitehouse.gov/the_press_office/FreedomofInformationAct/.

[63] Ibid.

The memorandum then directed the attorney general to "issue new guidelines governing the FOIA to the heads of executive departments and agencies, reaffirming the commitment to accountability and transparency, and to publish such guidelines in the Federal Register."[64]

On March 19, 2009, Attorney General Eric Holder issued the memorandum in which he required "A Presumption of Openness." The memorandum explicitly rescinded former Attorney General John Ashcroft's October 12, 2001, memorandum.[65] Holder's memorandum read as follows:

> *First, an agency should not withhold information simply because it may do so legally.... An agency should not withhold records merely because it can demonstrate, as a technical matter, that the records fall within the scope of a FOIA exemption.*
>
> *Second, whenever an agency determines that it cannot make full disclosure of a requested record, it must consider whether it can make partial disclosure. Agencies should always be mindful that the FOIA requires them to take reasonable steps to segregate and release nonexempt information. Even if some parts of a record must be withheld, other parts either may not be covered by a statutory exemption, or may be covered only in a technical sense unrelated to the actual impact of disclosure.*
>
> *At the same time, the disclosure obligation under the FOIA is not absolute....*
>
> *[T]he Department of Justice will defend a denial of a FOIA request only if (1) the agency reasonably foresees that disclosure would harm an interest protected by one of the statutory exemptions, or (2) disclosure is prohibited by law.*[66]

Some newspapers and open government advocates argued that the Obama and Holder memorandums on FOIA marked a significant break with the policies of

---

[64] Ibid. The memorandum does not include a deadline by which such guidelines must be published.

[65] This memorandum is described in more detail below.

[66] Attorney General Eric Holder, Memorandum For the Heads of Executive Departments and Agencies, U.S. Department of Justice, Washington, DC, March 19, 2009, pp. 1-2, http://www.usdoj.gov/ag/foia-memo-march2009.pdf.

the previous administration.[67] In a memorandum written by former Attorney General John Ashcroft shortly after the 9/11 terrorist attacks, the Bush Administration required agency and department heads to release documents "only after full and deliberate consideration of the institutional, commercial, and personal privacy interests that could be implicated by disclosure of the information."[68] The memorandum continued:

> *When you carefully consider FOIA requests and decide to withhold records, in whole or in part, you can be assured that the Department of Justice will defend your decisions unless they lack a sound legal basis or present an unwarranted risk of adverse impact on the ability of other agencies to protect other important records.*[69]

The Obama Administration also sought to solicit information and ideas from the public on how to make FOIA a more useful tool. In May, the administration announced a three-phase Open Government Initiative aimed at collecting ideas from the public on how to make government more collaborative, transparent, and participatory. From May 21 through June 3, 2009, the Obama Administration's Office of Science & Technology Policy (OSTP) entered the first phase of the directive by tapping the National Academy of Public Administration (NAPA) to host an online "brainstorming session,"[70] seeking public comment on "innovative approaches to policy, specific project suggestions, government-wide or agency-specific instructions, and any relevant examples and stories relating to law, policy, technology, culture, or practice."[71] The brainstorming session garnered 4,205 suggestions and comments, some of which addressed FOIA. One suggestion, for example, said that agencies should be required to post documents online that are released in relation to a FOIA request. The suggestion stated that

---

[67] In an editorial, the Los Angeles Times called President Obama's new policy "a transformation of incalculable significance." "Obama Gives New Life to the FOIA," The Los Angeles Times, January 23, 2009, at http://www.latimes.com/news/printedition/opinion/la-ed-foia23-2009jan23,0,4722159.story. The Sunshine in Government Initiative said the memorandum demonstrated that transparency was a "wonderful" priority for the Obama Administration. The Sunshine in Government Initiative," January 21, 2009, press release, at http://www.sunshineingovernment.org/index.php?cat=31.

[68] John Ashcroft, U.S. Attorney General, Memorandum for the Heads of all Federal Departments and Agencies, October 12, 2001, http://www.doi.gov/foia/foia.pdf.

[69] Ibid.

[70] National Academy of Public Administration (NAPA), Open Government Dialogue, May 21, 2009, http://opengov.ideascale.com/akira/panel.do?id=4049. When the dialogue began, users could offer ideas without signing up for a log-on identity. On May 23, NAPA changed that policy and required all participants to log into the website before their comments could be posted.

[71] Ibid.

such action could reduce the number of duplicative requests to which agencies and departments must respond.

From June 3 through June 26, 2009, OSTP began the second phase of its Open Government Initiative, which focused in greater depth on some of the ideas that emerged in the brainstorming session forums. On June 10, 2009, Michael Fitzpatrick, associate administrator for the Office of Information and Regulatory Affairs, posted a question on OSTP's blog asking for "recommendations … for agencies to pro-actively post information on their websites to avoid a FOIA request from even occurring" and "recommendations to make FOIA reading rooms more useful and information more easily searchable, as they are meant to be a mechanism for information dissemination to the public."[72] The request prompted 58 responses, including one response that suggested documents released as part of a FOIA request not only be published online, but also be text searchable.[73]

From June 22 through July 6, 2009, OSTP conducted the third phase of the initiative: drafting. Using an online program, members of the public created online documents that included policy recommendations. Participants critiqued, endorsed, and rated the policy recommendations.[74] OSTP said that the "recommendations will inform the drafting of an 'Open Government Directive' to Executive branch agencies."[75] Among the policy recommendations posted was a suggestion to "rebuild technical capacity for information dissemination in the agencies (and government-wide)" so historical agency information can be stored electronically and accessed more efficiently when it is requested by the public.[76]

FOIA and the 111th Congress

The administration's new guidelines on how agencies are to apply FOIA could prompt Congress to reevaluate certain FOIA practices and policies. An issue potentially subject to reevaluation is whether Secret Service records should be considered "presidential records," administered according to the Presidential

---

[72] Michael Fitzpatrick, associate administrator for OIRA, Transparency: Access to Information, Executive Office of the President, Office of Science & Technology Policy, June 10, 2009, http://blog.ostp.gov/2009/06/10/transparencyaccess-to-information/.

[73] Transparency: Access to Information, Executive Office of the President, Office of Science & Technology Policy, June 10, 2009, http://blog.ostp.gov/2009/06/10/transparency-access-to-information/.

[74] For more information on MixedInk, see http://www.vimeo.com/2674991.

[75] U.S. Office of Science and Technology Policy, Executive Office of the President, Open Government Directive, Phase 3: Drafting, 2009.

[76] MixedInk, Institutionalizing Transparency in Government, at http://mixedink.com/OpenGov/InstitutionalizingTransparency.

Records Act of 1978 (PRA). Making Secret Service records subject to PRA could protect certain records from disclosure for up to 20 years more than protections afforded under FOIA. In addition, several pieces of legislation have been introduced in the 111th Congress that directly or tangentially address FOIA.

Secret Service or Presidential Records

Debate and litigation surrounding the Secret Service records began in 2006, when Citizens for Responsibility and Ethics in Washington (CREW) filed a FOIA request with the Secret Service seeking access to sign-in logs maintained at the White House and the Vice Presidential Residence. The logs track who attends meetings at the two locations. CREW filed suit in federal district court in 2007, after the Secret Service failed to respond to the FOIA request. The suit also challenged the service's policy of deleting certain White House visitor records, claiming such action violated the Federal Records Act[77] and the Administrative Procedure Act.[78]

The district court found that the sign-in logs at the White House and the Vice Presidential Residence are created and controlled by the Secret Service, and, therefore, are "agency records."[79] The court also rejected the Secret Service's claim that disclosure of the records would prompt separation of powers concerns because they could "impede the ability of the President and Vice President to receive full and frank submissions of facts and opinions and to seek confidential information from many sources, both inside and outside the government."[80] The opinion of the district court is currently on appeal to the D.C. Circuit.

Congress may opt to enact legislation that would explicitly state whether the Secret Service logs should be treated as "presidential records."[81] If the records were designated as "presidential records" the logs would be afforded additional protections that could delay their release by up to 20 years.[82] If the records were

[77] 44 U.S. C. § 3101 et seq. (2006).

[78] 5 U.S.C. § 551 et seq. (2006).

[79] CREW, 527 F.Supp.2d at 98 (citing Tax Analysts, 492 U.S. at 147).

[80] Ibid. at 98 (citing Def. Mot. S.J. at 30). The court's opinion questioned whether releasing the log books would "impede the President's ability to perform his constitutional duty," saying the threat is not "great enough to justify curtailing the public disclosure aims of FOIA."

[81] If Congress opted to create such legislation, it could do so by amending FOIA (5 U.S.C. § 552), PRA (44 U.S.C. § 2201), or the Secret Service Statute (18 U.S.C. § 3056) to explicitly state the status of the Secret Service logs.

[82] Pursuant to the PRA, an outgoing President can restrict access to certain records for up to 12 years (44 U.S.C. § 2204(a). After 12 years, the President's records are then subject to release pursuant to FOIA's provisions. The 20-year protection assumes a record was created in January

determined not to be "presidential records," they would be subject to public release unless a FOIA exemption applied. Congress may also consider whether the legislation should be applied retroactively to the records of the Bush Administration or if the policy should apply only to current and future Secret Service logs. Congress could opt to take no action and wait for a determination of the records' status by the D.C. Circuit Court of Appeals. If the court does not overturn the district court's findings, the logs would be subject to FOIA, and would not receive any additional protections.

On May 19, 2009, the U.S. Court of Appeals decided that the Office of Administration (OA) within the Executive Office of the President (EOP) was not subject to FOIA.[83] CREW was again the appellant in the case, and sought information related to e-mails that went missing from the OA. The court stated the test to determine if an EOP entity was subject to FOIA was to ask whether the entity "wielded substantial authority independently of the President."[84] Finding that the OA was "directly related to the operational and administrative support of the work of the President and his EOP staff,"[85] the court decided that OA did not qualify as an executive branch agency.

FOIA Legislation in the 111th Congress

H.R. 1323

Introduced by Representative Steve Driehaus on March 5, 2009, the Reducing Information Control Designs Act would require federal agencies to streamline their internal classification designations. The bill would not affect classification standards that are codified or established by executive order. Pursuant to the legislation, the archivist of the United States would promulgate regulations aiming to standardize agencies' classification designations to "maximize public access to information," among making other reforms. Any modifications of classification designations "should have no relationship to determinations of public disclosure pursuant to the Freedom of Information Act (FOIA)."[86] The House agreed to the bill by voice vote on March 17, 2009. The next day, the

---

of a two-term (8-year) President's first term. The 12-year restriction to record access begins at the end of a President's tenure. For more information on the PRA see CRS Report R40238, Presidential Records: Issues for the 111th Congress, by Wendy R. Ginsberg.

[83] Citizens for Responsibility and Ethics in Washington v. Office of Administration, 566 F.3d 219 (D.C. Cir. 2009).

[84] Id., at 222.

[85] Id., at 224.

[86] U.S. Congress, House Committee on Oversight and Government Reform, Reducing Information Control Designations Act, report to accompany H.R. 1323, 111th Cong., 1st sess., March 16, 2009, H.Rept. 111-38 (Washington: GPO, 2009), pp. 3-4.

Senate received the bill and referred it to the Senate Committee on Homeland Security and Governmental Affairs.

H.R. 2450

Introduced by Representative Sheila Jackson-Lee on May 15, 2009, the Private Prison Information Act of 2009 would require all private, state, and locally run incarceration and detention facilities to comply with FOIA. Pursuant to the act, non-federal prisons and correctional facilities would be required "to release information about the operation of the non-Federal prison or correctional facility" unless the information was exempted from release by one of FOIA's nine exemptions.

H.R. 2712 (Representative Conaway); H.R. 2875 (Representative Conaway); H.R. 3015 (Representative Conaway); S. 1100 (Senator Joseph Lieberman); S. 1260 (Senator Joseph Lieberman); and S. 1285 (Senator Joseph Lieberman)

These six bills address the public release of photographs of the treatment of individuals engaged, captured, or detained by the U.S. Armed Forces from September 11, 2001 through January 22, 2009. Pursuant to the bills, these photographs would exempted from disclosure under FOIA. S. 1285 was introduced on March 17, 2009 and passed by unanimous consent that same day. On March 18, the bill was sent to the House, where it was referred both the House Committee on Oversight and Government Reform and the House Committee on Armed Services. The House bills have all been concurrently reported to the House Committee on Oversight and Government Reform and the House Committee on Armed Services. The Senate bills (other than S. 1285) have been referred to the Senate Committee on the Judiciary.

S. 612

Introduced by Senator Patrick J. Leahy on March 17, 2009, the OPEN FOIAAct of 2009 would require Congress to be detailed and explicit when creating any future statutory exemptions to the public release of records within FOIA. Any exemptions made subsequent to the enactment of S. 612 pursuant to the third exemption of FOIA, must cite directly to the third exemption. This bill is similar to legislation introduced in both the 109th and 110th Congresses. On March 17, the bill was referred to the Senate Committee on the Judiciary. The language of this bill was placed in S. 1285, which—as noted earlier—has passed the Senate and has been referred to two committees in the House.

The Privacy Act of 1974 (5 U.S.C. § 552a)

The Privacy Act: Emerging Issues and Related Legislation, RL30824 (February 26, 2002).

HAROLD C. RELYEA, CONGRESSIONAL RESEARCH SERV., THE PRIVACY ACT: EMERGING ISSUES AND RELATED LEGISLATION (2002), *available at* http://www.intelligencelaw.com/library/secondary/crs/pdf/RL30824_2-26-2002.pdf.

Order Code RL30824

Updated February 26, 2002

Harold C. Relyea
Specialist in American National Government
Government and Finance Division

Summary

The Privacy Act of 1974 represents an attempt by Congress to legislate several aspects of personal privacy protection as it relates to federal agency operations and practices. First, it sustains some traditional major privacy principles. Second, it provides an individual who is a citizen of the United States, or an alien lawfully admitted for permanent residence, with access and emendation arrangements for records maintained on him or her by most, but not all, federal agencies. Third, the statute embodies a number of principles of fair information practice: it sets certain conditions concerning the disclosure of personally identifiable information; prescribes requirements for the accounting of certain disclosures of such information; requires agencies to collect information, to the greatest extent practicable, directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under federal programs; requires agencies to specify their authority and purposes for collecting personally identifiable information from an individual; requires agencies to maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination; and provides civil and criminal enforcement arrangements.

Since its enactment, the Privacy Act has been amended on six occasions; actions in 1988 and 1990 establishing new procedures and data protection boards for computer matching are generally seen as being the most significant. Of late, new issues have arisen concerning these matters and some long-prevailing concerns. This report reviews the background and development of the statute, its current provisions, and emerging issues pertaining to it. As legislative and other relevant developments occur, this report will be updated.

Introduction

The Privacy Act of 1974 represents an attempt by Congress to legislate several aspects of personal privacy protection as it relates to federal agency operations and practices.[87] Its eclectic provisions can be traced to several contemporaneous events prompting congressional interest in securing personal privacy.

Since the years of the late 19th century, various developments—not the least of which have been new, intrusive technologies—have contributed to more disparate understandings of the concept of privacy and infringements upon it.[88] Congress made an initial effort at legislating a new kind of privacy protection in 1970 when enacting the Fair Credit Reporting Act regulating the collection and dissemination of personal information by consumer reporting entities.[89]

With the Crime Control Act of 1973, Congress prohibited federal personnel and state agencies receiving law enforcement assistance funds pursuant to the statute from making unauthorized disclosures of personally identifiable criminal history research or statistical information. It also permitted "an individual who believes that criminal history information concerning him contained in an automated system is inaccurate, incomplete, or maintained in violation of this [law] ... to review such information and to obtain a copy of it for the purpose of challenge or correction."[90]

That same year, the Advisory Committee on Automated Personal Data Systems, established by Secretary of Health, Education, and Welfare Elliot L. Richardson in early 1972, offered an important proposal. The panel's July 1973 final report recommended "the enactment of legislation establishing a Code of Fair Information Practice for all automated personal data systems." Such a code would: punish unfair information practice with civil and criminal penalties; provide injunctive relief to prevent violations of safeguard requirements; empower individuals to bring suits for unfair information practices to recover actual, liquidated, and punitive damages, in individual or class actions; and allow

---

[87] For the text of the Privacy Act, see 5 U.S.C. 552a.

[88] See CRS Report RL30671, Personal Privacy Protection: The Legislative Response, by Harold C. Relyea.

[89] 84 Stat. 1128; 15 U.S.C. 1681 et seq.

[90] 87 Stat. 197, at 215-216; 42 U.S.C. 3789g.

the recovery of reasonable attorneys' fees and other costs of litigation incurred by individuals who bring successful suits.[91]

Congressional efforts to legislate notice, access, and emendation arrangements for individuals concerning personally identifiable records maintained on them by federal departments and agencies began in the House in June 1972, but did not extend beyond the subcommittee hearing stage during the 92nd Congress. However, a few days before these inaugural House hearings on legislation that would evolve into the Privacy Act, a burglary occurred at Democratic National Committee headquarters. It was the beginning of the Watergate incident, which would significantly affect attitudes toward privacy protection legislation and the leadership for such legislation.

Legislation leading to the enactment of the Privacy Act began in the House largely as an effort to create a procedure whereby individuals could learn if federal agencies maintained files on them, could review the contents of the records in those files, could correct inaccuracies they contained, and could know how this information was being used and by whom. In the Senate, a privacy protection bill sponsored by Senator Sam Ervin, Jr., initially sought largely to establish a Federal Privacy Board and to create standards and management systems for handling personally identifiable information in federal agencies, state and local governments, and other organizations. Other aspects of privacy policy were added to these bills as they moved through their respective houses of Congress, and then were reconciled in a somewhat unusual manner to create an amalgamated bill acceptable to the House, the Senate, and the President.

House hearings began in mid-February 1974 under Representative William S. Moorhead, chairman of the Subcommittee on Foreign Operations and Government Information of the Committee on Government Operations (now Government Reform), and a principal manager of the legislation. The subcommittee held markup discussions in May, June, and July. These deliberations resulted in a clean bill (H.R. 16373), which was introduced by Representative Moorhead with 13 bipartisan cosponsors in mid-August and favorably reported by the Subcommittee without a dissenting vote. The Committee on Government Operations considered the legislation in mid-September, substituted revised text for the original language, and favorably reported it. President Gerald Ford, who had recently succeeded to the Oval Office after President Richard Nixon's early August resignation, endorsed the House bill

---

[91] U.S. Department of Health, Education, and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, Records, Computers, and the Rights of Citizens (Washington: GPO, 1973), pp. xxiii, 50.

in an October 9 statement.[92] The measure was considered by the House on November 20 and 21, and approved, with amendments, on a 353-1 yea-and-nay vote.[93]

A somewhat different counterpart privacy proposal emerged in the Senate. Senator Ervin introduced his bill (S. 3418) on May 1, 1974, with bipartisan cosponsorship. Hearings on this and related legislation occurred in June. During June, July, and August, staff of the Senate Committee on Government Operations, its Ad Hoc Subcommittee on Privacy and Information Systems, and the Subcommittee on Constitutional Rights of the Committee on the Judiciary—all panels chaired by Senator Ervin—further refined the language of the bill. In a mid-August committee mark-up, a staff-developed version of the measure was amended and favorably reported to the Senate.

The new text of the bill would have established the Privacy Protection Commission, composed of five members appointed by the President from private life and subject to Senate approval. It would have been responsible for compiling and publishing an annual directory of information systems subject to the provisions of the bill, enforcing the legislation, and developing model guidelines for its implementation, including the conduct of research in this regard. The bill also would have established federal agency standards and management systems for handling information relating to individuals. These included fair information practice principles, disclosure standards, mailing list restrictions, and civil and criminal penalties.

On November 21, 1974, the Senate considered the Ervin legislation; amendments developed by committee staff and the Office of Management and Budget (OMB) were adopted, and the resulting version of the legislation was approved.[94] The following day, the Senate took up the House counterpart bill, struck its language and substituted in lieu there of the language of the Ervin bill, and approved the amended version of the House bill.[95]

With only a few weeks remaining before the 93rd Congress would adjourn sine die, House and Senate managers found they had very little time to reconcile the two differing bills. There was, however, strong desire for the passage of such

---

[92] U.S. General Services Administration, National Archives and Records Service, Office of the Federal Register, Public Papers of the Presidents of the United States: Gerald R. Ford, 1974 (Washington: GPO, 1976), pp. 243-244.

[93] Congressional Record, vol. 120, Nov. 20, 1974, pp. 36643-36660; Ibid., Nov. 21, 1974, pp. 36955-36977.

[94] Congressional Record, vol. 120, Nov. 21, 1974, pp. 36882-36921.

[95] Ibid., Nov. 22, 1974, pp. 37064-37069.

legislation, not only as a so-called Watergate reform, but also as a tribute and memorial to Senator Ervin, who was retiring from congressional service. Consequently, Representative Moorhead and Senator Ervin, with the concurrence of their respective committees, agreed to the rare arrangement of having their committee staffs negotiate a mutually agreeable legislative measure. After this effort reduced 108 substantive differences to eight, the leaders of the respective House and Senate committees brought those to resolution.[96] In lieu of a conference committee report, a staff analysis of the compromise legislation was produced.[97] The major concession was the relegation of the enforcement commission to the status of a temporary national study commission. Its oversight responsibilities were vested in OMB, but without enforcement authority.

On December 11, the House adopted the Senate bill as amended with the language of its own bill.[98] The Senate concurred with the House amendment by passing its own amendment on a 77-8 vote on December 17, clearing the measure for further House action.[99] The following day, the House agreed to the Senate amendments with an amendment of its own,[100] and the Senate concurred with the House amendments the same day, clearing the measure for the President's signature.[101] The Privacy Act was signed into law by President Ford on December 31, 1974.[102] In his signing statement, the President said the new law "signified an historic beginning by codifying fundamental principles to safeguard personal privacy in the collection and handling of recorded personal information by federal agencies."[103]

Major Provisions

The Privacy Act provides privacy protection in several ways. First, it sustains some traditional major privacy principles. For example, an agency shall "maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual

---

[96] Ibid., Dec. 17, 1974, p. 40400.

[97] See ibid., pp. 40405-40408.

[98] Ibid., Dec. 11, 1974, pp. 39200-39204.

[99] Ibid., Dec. 17, 1974, pp. 40397-40413.

[100] Ibid., Dec. 18, 1974, pp. 40879-40886.

[101] Ibid., pp. 40730-40731.

[102] 88 Stat. 1896; 5 U.S.C. 552a.

[103] U.S. General Services Administration, National Archives and Records Service, Office of the Federal Register, Public Papers of the Presidents of the United States: Gerald R. Ford, 1975 (Washington: GPO, 1977), pp. 1-2.

about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity."[104]

Second, similar to the Fair Credit Reporting Act, the Privacy Act provides an individual who is a citizen of the United States, or an alien lawfully admitted for permanent residence, with access and emendation arrangements for records maintained on him or her by most, but not all, federal agencies. General exemptions in this regard are provided for systems of records maintained by the Central Intelligence Agency and federal criminal law enforcement agencies.

Third, the statute embodies a number of principles of fair information practice. For example, it sets certain conditions concerning the disclosure of personally identifiable information; prescribes requirements for the accounting of certain disclosures of such information; requires agencies to "collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs"; requires agencies to specify their authority and purposes for collecting personally identifiable information from an individual; requires agencies to "maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination"; and provides civil and criminal enforcement arrangements.

Since its enactment, the Privacy Act has been amended on six occasions. In 1982, the Debt Collection Act added a new exception to the disclosure prohibition for disclosures made to consumer credit reporting agencies.[105] That same year, the Congressional Reports Elimination Act changed the annual report requirement of the Privacy Act and modified the provision for publication of agency systems of records.[106] In 1984, the Central Intelligence Agency Information Act resolved a long-standing controversy by specifying that the Privacy Act is not authority "to withhold from an individual any record which is otherwise accessible to the individual under the provisions of" the Freedom of Information Act.[107] Amendments in 1988[108] and 1990[109] established new procedures and data

---

[104] 5 U.S.C. 552(e)(7).

[105] 96 Stat. 1749, adding 5 U.S.C. 552a(b)(12).

[106] 96 Stat. 1819, at 1821-1822, modifying 5 U.S.C. 552a(e)(4) and (p).

[107] 96 Stat. 2209, at 2211-2212, adding 5 U.S.C. 552a(q)(2).

[108] 102 Stat. 2507, adding 5 U.S.C. 552a(o),(p),(q), and (u), and amending 5 U.S.C. 552a(a), (e), and (v).

[109] 104 Stat. 1388-334, modifying 5 U.S.C. 552a(p).

protection boards to ensure privacy, integrity, and verification of data disclosed for computer matching. Recently, the Federal Reports Elimination and Sunset Act of 1995, as amended by the Miscellaneous Appropriations Act for FY 2000, repealed the requirement for a biennial Privacy Act report to Congress.[110]

Emerging Issues

Better Enforcement or Overhaul. Several issues are before the 107th Congress regarding the Privacy Act. A September 2000 General Accounting Office (GAO) report on a survey of online privacy protections at federal Web sites found that 23 of 70 agencies had disclosed personal information gathered from their Web sites to third parties, mostly other agencies. However, at least four agencies were discovered to be sharing such information with private entities—trade organizations, bilateral development banks, product manufacturers, distributors, and retailers. The offending agencies were not identified by GAO. Responding to these findings, some privacy advocates called for updating the Privacy Act to specify privacy protections for Internet visitors to agency Web sites, while others urged better oversight and enforcement of the statute.[111]

Managing "Cookies"

Federal agencies obtained personal information about visitors to their Web sites through the use of computer software known as "cookies." In June 2000, press disclosures revealed that the National Drug Control Policy Office, an agency within the Executive Office of the President, was secretly tracking visitors to its Web site through the use of "cookies."[112] In response, OMB issued a June 22, 2000, memorandum to the heads of all executive departments and agencies indicating that "'cookies' should not be used at Federal web sites, or by contractors when operating web sites on behalf of agencies, unless, in addition to clear and conspicuous notice, [certain specified] ... conditions are met."[113]

In October 2000, press disclosures revealed that a GAO followup study contended that 13 federal agencies had ignored the OMB June 22 memorandum prohibiting the tracking of visitors to government Web sites. An appended letter

---

[110] 109 Stat. 707, as amended by section 236 of H.R. 3425, as incorporated, at 113 Stat. 1537-296, repealing 5 U.S.C. 552a(s).

[111] Lance Gay, "GAO Finds Agencies Sharing Data of On-line Visitors," Washington Times, Sept. 8, 2000, p. A3; U.S. General Accounting Office, Internet Privacy: Agencies' Efforts to Implement OMB's Privacy Policy, GAO Report GAO/GGD-00-191, Sept. 2000.

[112] See John F. Harris and John Schwartz, "Anti-Drug Web Site Tracks Visitors," Washington Post, June 22, 2000, p. A23; Lance Gay, "White House Uses Drug-Message Site to Track Inquiries," Washington Times, June 21, 2000, p. A3.

[113] The memorandum is available from the OMB Web site at: [http://www.whitehouse.gov/omb/memoranda/m00-13.html].

from the OMB deputy director for management defended agency use of so-called "session cookies," which, the letter said, facilitated transactions at the website and were not banned by OMB. Session cookies last only as long as one is visiting the website. Clearly prohibited are "persistent cookies," which may track web habits for long periods of time, and the dissemination of a person's information to a private company. GAO found seven agencies engaging in one or both of these activities.[114]

In mid-April 2001, Senator Fred Thompson, chairman of the Senate Committee on Governmental Affairs, released the preliminary findings of agency Inspectors General who were required by a provision of the Treasury-Postal title of the Consolidated Appropriations Act of 2001 to report on how their agencies collect and review personal information on their Web sites.[115] Reports on 16 agencies found 64 Web sites making use of "persistent cookies."[116] Shortly thereafter, a GAO senior attorney criticized OMB's contradictory guidelines about federal agency use of "cookies." OMB, it was observed, had encouraged agencies to comply with the fair information practice principles of the Federal Trade Commission, which are not statutorily mandated, and also adhere to the requirements of the Privacy Act.[117] The Privacy Act might be amended to eliminate any such contradiction, to prescribe conditions when "sessions cookies" may be used, and to outlaw the use of "persistent cookies."

Oversight and Enforcement Responsibility

Another issue concerns continued vestment of Privacy Act oversight and enforcement in the director of OMB or, alternatively, in another entity. Options for consideration in this regard include a small privacy agency having no regulatory authority over the private sector[118] or a Chief Information Officer of the United States (CIOUS). Such an official had been proposed in 1995 Senate legislation underlying the Clinger-Cohen Act governing information technology

---

[114] Associated Press, "U.S. Agencies Ignore Ban, Track Visitors to Web Sites," Washington Times, Oct. 22, 2000, p. C3; D. Ian Hopper, "Agencies Track Online Visitors Despite Rules," Washington Post, Oct. 22, 2000, p. A13; D. Ian Hopper, "Renewed Ban on U.S. Web 'Cookies'," Washington Post, Oct. 24, 2000, p. A25; U.S. General Accounting Office, Internet Privacy: Federal Agency Use of Cookies, GAO Letter GAO-01-147R, Oct. 20, 2000.

[115] P.L. 106-554, sec. 646.

[116] Associated Press, "Federal Web Sites Can Track Visitors," Washington Times, Apr. 17, 2001, p. A8; Senator Thompson's release of the preliminary findings may be found at [http:www.senate.gov/~gov_affairs/041601a_press.htm].

[117] Drew Clark, "Conflicting Guidelines on Web 'Cookies' Spur Confusion," GovExec.com Daily Briefing, Apr. 24, 2001, available at [http://www.govexec.com/].

[118] See Robert Gellman, "Taming the Privacy Monster: A Proposal for a Non-Regulatory Privacy Agency," Government Information Quarterly, vol. 17, no. 3, 2000, pp. 235-241.

acquisition and management. A Progressive Policy Institute report recommended such a position in March 2000,[119] and legislation in support of the concept was offered in the House during the 106th Congress.[120] Texas Governor George W. Bush, the anticipated Republican presidential nominee, endorsed the CIOUS idea in a June 9, 2000, government reform speech in Philadelphia. During a September 2000 House subcommittee hearing on the proffered CIOUS bills[121] and in related published views, proponents of the new position contended that many aspects of information technology (IT) management would benefit from having a IT expert in charge of this area, that such an official would better facilitate OMB oversight of IT applications and use, and that efficiencies and economies could well result if this official could prevent federal agencies from purchasing computer systems that did not work or otherwise performed poorly in, or failed, security tests. Critics maintained that the CIOUS would unnecessarily perform a subset of duties currently vested in the OMB deputy director for management, would seemingly have few immediate enforcement powers, and, in some versions, might be controlling funds outside the traditional appropriations process. Members of the CIO Council reportedly are at odds over the need for the CIOUS.[122] In the early weeks of the new administration, President Bush vacated his earlier endorsement of a CIOUS.

Broader Application

A third issue concerns inclusion of the White House Office and the Office of the Vice President within the scope of the Privacy Act, and to what extent, if any, the legislative branch should be subject to the statute or parallel requirements set by rule or standing order. Disclosures of personally identifiable information by the White House during the Clinton Administration has fueled this issue. Similarly, although Congress and the legislative support agencies are not currently subject to the Privacy Act, the issue of legislatively requiring their inclusion is fueled by

---

[119] See Robert D. Atkinson and Jacob Ulevich, Digital Government: The Next Step to Reengineering the Federal Government (Washington: Progressive Policy Institute, March 2000), p. 13.

[120] H.R. 4670 was introduced on June 15 by Rep. Jim Turner, and H.R. 5024 was introduced on July 27 by Rep. Tom Davis; both bills were referred to the Committee on Government Reform.

[121] U.S. Congress, House Committee on Government Reform, Subcommittee on Government Management, Information, and Technology, Establishing a Federal CIO: Information Technology Management and Assurance Within the Federal Government, hearing, 106th Cong., 2nd sess., Sept. 12, 2000 (Washington: transcript awaiting publication).

[122] See Christopher J. Dorobek, "Experts Debate Need for Federal IT Czar," Government Computer News, vol. 19, Mar. 6, 2000, p. 58; Christopher J. Dorobek, "CIO Council on Track, Members Say," Government Computer News, vol. 19, May 8, 2000, p. 65; Christopher J. Dorobek, "What Would Governmentwide CIO Do?," Government Computer News, vol. 19, July 10, 2000, p. 74; Joseph J. Petrillo, "David Bill Would Give IT Czar Carrots, but No Stick," Government Computer News, vol. 19, Sept. 11, 2000, p. 24.

considerations of executive and legislative branch parity in this regard, as well as by the perceived need for more explicit privacy protections within the legislative branch.[123]

Military Exclusion

A fourth issue arises from a September 2000 federal district court ruling that the Feres doctrine, which prohibits military personnel from suing the government for injuries,[124] applies equally to lawsuits brought under the Privacy Act, resulting in a prohibition on suing not only for damages, but also even for the correction of records.[125] In this case, a U.S. Navy fighter pilot sought damages for the leaking of her confidential flight evaluation to Robert L. Gandt, an author researching a book on navy fighter pilots. The evaluation's recommendation that Cummings be stripped of her flight status was rejected by the commander of the Naval Air Force for the Atlantic Fleet. Gandt's 1997 book, Bogey's and Bandits: The Making of a Fighter Pilot, quoted from the evaluation, but assigned Cummings a pseudonym. A 1988 graduate of the U.S. Naval Academy, Cummings left the navy in 1999 and is currently an assistant professor of engineering at Virginia Polytechnic Institute and Statute University.[126]

On August 2, 2001, Representative Rick Boucher, with bipartisan cosponsorship, introduced H.R. 2738 to amend Title 5, United States Code, to clarify that all of the protections of the Freedom of Information Act and the Privacy Act apply to members of the armed forces to the same extent and in the same manner as to any other individual. The bill was referred to the Committee on Government Reform.

On February 15, 2002, the U.S. Court of Appeals for the District of Columbia reversed the trial court in the navy fighter pilot case seeking Privacy Act relief. The 2-1 ruling said that members of the military can sue the government for invading their privacy, indicating that the Feres doctrine does not take

---

[123] See U.S. Congress, House Committee on Government Reform, Subcommittee on Criminal Justice, Drug Policy, and Human Resources, The Privacy Act and the Presidency, hearing, 106th Cong., 2nd sess., Sept. 8, 2000 (Washington: transcript awaiting publication).

[124] Feres v. U.S., 340 U.S. 135 (1950). The Feres case involved a liability claim under the Federal Tort Claims Act by the executor of a soldier who had died in a barracks fire. The Supreme Court, while continuing to uphold the doctrine, has stressed that it "cannot be reduced to a few bright-line rules," but rather "each case must be examined in light of the [Tort Claims Act] as it has been construed in Feres and subsequent cases." U.S. v. Shearer, 473 U.S. 52, 105 (1985). The Privacy Act affords liability damages apart from the Tort Claims Act.

[125] Mary Louise Cummings v. Department of the Navy, Civil Action No. 98-1183 (D.C. D.C., Sept. 6, 2000).

[126] Steve Vogel, "Navy Pilot Fights Privacy Ruling," Washington Post, Oct 3, 2000, pp. B1, B7.

precedence over the Privacy Act.[127] Because the decision is binding only on the courts of the circuit, a legislative clarification may still be sought.

Routine Use Reconsidered

Still another issue concerns the possible modification of the "routine use" clause of the Privacy Act to improve citizen awareness of the routine uses that agencies have indicated they will make of personally identifiable information and to limit the discretion of agency officials to share personally identifiable information with other agencies. The Privacy Act requires each agency in possession of systems of records to publish for each system the routine uses to which the information might be put. Such notices are published in the Federal Register. Most citizens are unaware of these notices and their implications, with the result that they have little understanding of how information supplied by or about them to government agencies might be used. Furthermore, in the view of one policy analyst examining the situation, "agency officials have interpreted the routine use clause broadly and have created almost unlimited ability to move data among Federal agencies."[128]

However, from another perspective, the routine use clause may not be quite as broadly interpreted as has been asserted. A May 1998 report, prepared by a benefit eligibility verification study committee of the President's Council on Integrity and Efficiency, for example, considered it doubtful that, given prevailing judicial interpretation, "disclosure of information collected by one agency for a specific program, to another agency for eligibility verification in an unrelated program, would be considered a routine use."[129]

Matching and Sharing

Finally, an issue has arisen regarding the circumstances, if any, when computer matching of personally identifiable information in systems of records across government programs and agencies should be permitted. Agency officials responsible for combating waste, fraud, and abuse in federal benefits programs urge a reconsideration of the Privacy Act's strict matching requirements, while privacy advocates would retain the status quo.[130] The case for reconsideration began to emerge a few years ago, the May 1998 benefit eligibility verification

---

[127] Mary Louise Cummings v. Department of the Navy, 2002 WL 226134 (D.C. Cir. No. 005348).

[128] Gloria Cox, "Implementation of the Routine Use Clause of the Privacy Act," Policy Studies Review, vol. 10, Winter 1991-1992, p. 43.

[129] President's Council on Integrity and Efficiency, Ad Hoc Committee on Benefit Eligibility Verification, Eligibility Verification Needed to Deter and Detect Fraud in Federal Government Benefit and Credit Programs, May 1998, p. 3.

[130] See U.S. General Accounting Office, The Challenge of Data Sharing: Results of a GAO-Sponsored Symposium on Benefit and Loan Programs, GAO Report GAO-01-67, Oct. 2000.

study report of the President's Council on Integrity and Efficiency being exemplary. Describing the demanding and cumbersome requirements for producing and executing a computer matching agreement, the report reiterated earlier OMB findings "that the procedures for renegotiating agreements for recurring matches, such as would be required for program eligibility verification, require the expenditure of enormous personnel resources with little substantive benefit, and that "verifying eligibility before payments are initiated ... would avoid overpayments and allow agencies to ' ... move from a pay and chase mode to one that is far more proactive and efficient'."[131]

[131] President's Council on Integrity and Efficiency, Ad Hoc Committee on Benefit Eligibility Verification, Eligibility Verification Needed to Deter and Detect Fraud in Federal Government Benefit and Credit Programs, p. 4.

Sharing Law Enforcement and Intelligence Information: The Congressional Role, RL33873 (February 13, 2007).

RICHARD A. BEST, JR., CONGRESSIONAL RESEARCH SERV., SHARING LAW ENFORCEMENT AND INTELLIGENCE INFORMATION: THE CONGRESSIONAL ROLE (2007), *available at* http://www.intelligencelaw.com/library/secondary/crs/pdf/RL33873_2-13-2007.pdf.

Order Code RL33873
February 13, 2007

Richard A. Best Jr.
Specialist in National Defense
Foreign Affairs, Defense, and Trade Division

Summary

Almost all assessments of the attacks of September 11, 2001, have concluded that U.S. intelligence and law enforcement agencies had failed to share information that might have provided advance warning of the plot. This realization led Congress to approve provisions in the USA PATRIOT Act (P.L. 107-56) and subsequent legislation that removed barriers to information sharing between intelligence and law enforcement agencies, and mandated exchanges of information relating to terrorist threats. Most experts agreed that statutory changes, albeit difficult to enact, were essential to change the approaches taken by executive branch agencies.

The barriers that existed prior to September 2001 had a long history based on a determination to prevent government spying on U.S. persons. This had led to the establishment of high statutory barriers to the sharing of law enforcement and intelligence information. The statutes laid the foundation of the so-called "wall" between intelligence and law enforcement that was buttressed by regulations, Justice Department policies, and guidance from the judicial branch.

Despite the widespread acceptance of a barrier between law enforcement and intelligence, by the early 1990s it had become apparent to some that the two communities could mutually support efforts to combat international criminal activities including narcotics smuggling. Later in the decade dangerous threats to the U.S. posed by international terrorists came into sharper focus. Nevertheless, efforts to adjust laws, regulations, and practices did not succeed, drawing strong opposition from civil libertarians. Only the tragedy of the 9/11 attacks overcame earlier concerns and led Congress and the executive branch to remove most statutory barriers to information sharing.

Laws and regulations have changed significantly since September 2001 and an Information Sharing Executive (ISE) has been established within the Office of the Director of National Intelligence to design and implement information sharing procedures. It is clear, however, that sustaining the exchange of law enforcement and intelligence information remains a challenge. In particular, there is continued concern about sharing of information that might in some way jeopardize the rights of free speech or association of U.S. persons. This opposition has contributed to the difficulty Congress has had in addressing legislation in this area and can be expected to continue. Some argue that, given the extent of legislation enacted in recent years, extensive oversight of information sharing efforts may be an appropriate way to ensure that the balance between ensuring domestic security and protecting civil liberties can be maintained.

This report will be updated as additional information becomes available.

Introduction

The failure of the U.S. Intelligence Community to provide better warning of the September 11, 2001, attacks has been widely attributed to the existence of "walls" between intelligence and law enforcement agencies. The walls arguably kept analysts from talking to each other and from sharing pieces of information that, if they had been viewed in close relationship, might have yielded a coherent picture of the emerging plot. This theory cannot of course be fully proven — the overall plot might not have been discerned even if the best analysts had had access to all available information in every agency. Nevertheless, the fact that available data had not in fact been shared focused public and congressional attention on the real or perceived walls that inhibited the exchange of information among agencies.

A consensus emerged that the walls should be torn down. In December 2002, the Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001, established by the two congressional intelligence committees, made a factual finding that the "important point is that the Intelligence Community, for a variety of reasons, did not bring together and fully appreciate a range of information that could have greatly enhanced its chances of uncovering and preventing Usama Bin Ladin's plan to attack the United States on September 11, 2001."[132] The Inquiry also made a systemic finding that:

---

[132] U.S. Congress, 107th Congress, Senate, Select Committee on Intelligence, and House of Representatives, Permanent Select Committee on Intelligence, Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001, Report, S.Rept. 107-351, H.Rept. 107-792 [Hereafter: Joint Inquiry Report], December 2002, p. 33.

> *Within the Intelligence Community, agencies did not adequately share relevant counterterrorism information, prior to September 11. This breakdown in communications was the result of a number of factors, including differences in the agencies' missions, legal authorities and cultures. Information was not sufficiently shared, not only between different Intelligence Community agencies, but also within individual agencies, and between the intelligence and law enforcement agencies.*[133]

Similar conclusions were reached in July2004 by the 9/11 Commission (the National Commission on Terrorist Attacks Upon the United States) carefully documented the failures of pre-9/11 information sharing among agencies and within different offices of the Justice Department and recommended a number of initiatives to encourage unity of effort in sharing information.[134]

The Legacy of FISA

The failure to share information prior to 9/11 had not occurred by happenstance. Law enforcement and intelligence information was not routinely shared and collectors and analysts were walled off from one another through a complex arrangement of constitutional principles, statutes, policies, and practices. These regulations had their origin in longstanding divisions of labor that reached back far into pre-World War II practices and in the provision of the National Security Act of 1947 requiring that the Central Intelligence Agency (CIA) "have no police, subpoena, or law enforcement powers or internal security functions."[135] The regulations were significantly strengthened in the 1970s when, in reaction to domestic intelligence gathering activities during the Vietnam War era, Congress undertook extensive investigations of intelligence activities and enacted legislation regulating domestic surveillance activities. Ultimately, in response to recommendations derived from this investigation, in 1978 Congress passed and President Jimmy Carter signed the Foreign Intelligence Surveillance Act (FISA),

---

[133] Ibid., p. xvii. Intelligence agencies focus on concerns outside U.S. territory (and are sometimes known as "foreign intelligence" agencies). They include the Central Intelligence Agency (CIA), the National Security Agency (NSA), the Defense Intelligence Agency (DIA), the National Reconnaissance Office (NRO), the National Geospatial-Intelligence Agency (NGA), the Bureau of Intelligence and Research of the State Department, the intelligence components of the military services and the Department of Homeland Security. Law enforcement agencies include the Federal Bureau of Investigation (FBI), the Drug Enforcement Administration, the Secret Service, and the Customs Service. The FBI is considered both a foreign intelligence agency and a law enforcement agency; this is also the case with the Coast Guard.

[134] U.S., National Commission on Terrorist Attacks upon the United States, The 9/11 Commission Report (Washington: Government Printing Office, 2004); see pp. 416-419.

[135] 50 U.S.C. 403-3(d)(1); on FISA generally, see CRS Report RL30465, The Foreign Intelligence Surveillance Act: An Overview of the Statutory Framework and Recent Judicial Decisions, by Elizabeth B. Bazan.

P.L. 95-511.[136] FISA provides a statutory framework for electronic surveillance in foreign intelligence investigations while electronic surveillance in criminal investigations continues to be governed by Title III of the Omnibus Crime Control Act of 1968 (usually referred to as Title III).[137] The implementation of FISA came to have an important influence on the relationship between law enforcement and intelligence.

FISA required that "the purpose" of domestic electronic surveillance (or a physical search) had to be the gathering of foreign intelligence information.[138] FISA permitted the dissemination to the law enforcement community of information relating to criminal activity incidentally acquired during a FISA electronic surveillance or physical search. When such dissemination was challenged by defense attorneys as running afoul of the Fourth Amendment,[139] a number of federal courts of appeals had upheld the government's contention in several cases that the "primary purpose" of an electronic surveillance or physical search had been the collection of foreign intelligence information. Thus, this use of FISA was held to be not inconsistent with Fourth Amendment requirements for criminal cases.[140]

Before 9/11 a considerable body of government practice and Justice Department policy increasingly reflected an understanding that adhering to the primary purpose standard effectively precluded Fourth Amendment challenges. The concern was to avoid letting aggressive criminal investigators obtain FISA court

---

[136] In 1994 FISA was modified to include physical searches (section 807 of the Intelligence Authorization Act for FY1995, P.L. 103-359).

[137] Title III prohibits all interception of wire or electronic communications unless that interception falls within one of the exceptions to Title III; electronic surveillance under FISA is one of the exceptions (18 U.S.C. 2511(2)(f). It is to be noted that "foreign intelligence" may not involve actual or potential violations of U.S. laws, e.g. intelligence could be acquired, in the U.S., regarding a plot involving parties outside the U.S. that would not involve activities prohibited by U.S. law. Such intelligence could be of great interest to national policymakers but there would be no justification for relying on Title III surveillance authorities in trying to obtain it. As will be noted below, there is, however, a significant potential for overlap when intelligence provides evidence of activities that are illegal under U.S. law.

[138] 50 U.S.C. 1804(a)(7)(B), 50 U.S.C. 1823(a)(7)(B). Sec. 218 of the USA PATRIOT Act (P.L. 107-56) had amended these sections to replace "the purpose" with "a significant purpose."

[139] The Fourth Amendment to the Constitution states: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

[140] A detailed assessment of the various judicial views and rulings on this question lies beyond the scope of this Report; see, however, David S. Kris, "The Rise and Fall of the FISA Wall," Stanford Law and Policy Review, Spring 2006, pp. 487-529.

orders when they were interested in obtaining evidence of criminal activities. There was a pervasive concern within the Justice Department that a court in a criminal trial would suppress information obtained through a FISA investigation on the grounds that it was primarily being used, not to collect foreign intelligence, but to gather criminal evidence or even that FISA itself would be overturned. In practice, information collected by intelligence agencies (including the parts of the Federal Bureau of Investigation (FBI) dealing with counterterrorism and counterintelligence) was kept apart from information collected for the use of prosecutors.

Recognizing the Need to Share Information

FISA's requirements appear not to have posed major problems until the mid1990s,[141] but law enforcement and intelligence agencies tended to function in separate worlds. Concern about these divisions did exist and there had been major initiatives largely as a result of concerns about the development of barriers between law enforcement and intelligence agencies in the aftermath of the controversy surrounding the illegal activities of the Banca Nazionale del Lavoro (BNL) and the Bank of Credit and Commerce International (BCCI) in the early 1990s. The controversy involved complex banking fraud and other criminal activities undertaken by the two foreign banks. Congressional investigators developed information that the CIA had obtained information indicating suspicious activities by the two banks that had not been passed to prosecutors in large measure because channels of communications had not been established between intelligence and law enforcement agencies. The Senate Intelligence Committee investigators concluded that:

> *The fundamental policy governing the relationship between law enforcement and intelligence needs to be addressed by the Attorney General and the DCI [Director of Central Intelligence], in conjunction with the congressional oversight committees. Confusion is apparent on both sides as to what the proper role (and authority) of intelligence agencies is in circumstances like those presented in the BNL case.*[142]

The reaction to the BNL/BCCI affairs reflected a shift away from emphasis on a strict separation of law enforcement and intelligence efforts to an appreciation by Congress of the need for closer cooperation. As a result of congressional concerns, the DCI and the Attorney General directed that a review of the

---

[141] See Diane Carraway Piette and Jesselyn Radack, "Piercing the 'Historical Mists': the People and Events Behind the Passage of FISA and the Creation of the 'Wall,'" Stanford Law and Policy Review, Spring 2006, p. 461.

[142] U.S. Congress, 103d Congress, 1st session, Senate, Select Committee on Intelligence, The Intelligence Community's Involvement in the Banca Nazionale del Lavoro (BNL) Affair, S. Prt. 103-12, February 1993, p. 27.

intelligence-law enforcement relationship be conducted. The review, undertaken by a group of senior executive branch officials known as the Joint Task Force on Intelligence and Law Enforcement, submitted a report in August 1994. The Task Force described the failure by intelligence and law enforcement agencies to make use of all available information on the activities of the two foreign banks. It called for a number of bureaucratic mechanisms to ensure greater information exchanges in the future, but argued that no statutory changes were called for:

> *What is required is not new legislation radically altering the relationship [between intelligence and law enforcement agencies], but rather a different approach to the existing relationship — one that is more interactive on a number of fronts, yet maintains the important distinctions between these two communities based on law, culture, and mission.*[143]

The Joint Task Force Report led to the establishment of a series of interagency coordinative mechanisms — the Intelligence-Law Enforcement Policy Board, the Joint Intelligence-Law Enforcement Working Group (JICLE) — at various levels to encourage information exchanges and resolve difficulties.[144] Although the Task Force provided a perceptive analysis of the difficulties that then existed and officials assigned to the resultant interagency bodies worked diligently at overcoming obstacles, progress was limited.[145]

By the 1990s, the threat of new forms of international terrorism was becoming apparent. Middle Eastern terrorists were operating against U.S. forces overseas

---

[143] U.S., Joint Task Force on Intelligence and Law Enforcement, Report to the Attorney General and Director of Central Intelligence, August, 1994, p. 4. The absence of a need for legislation was also the position of the then-DCI James Woolsey: "Rather, we can accomplish our goal of enhanced cooperation through a series of initiatives — such as joint training of law enforcement and intelligence officers." Address by R. James Woolsey, Director of Central Intelligence, before the American Bar Association, Washington, DC, April 29, 1994. In 2001, however, Woolsey would write in regard to the 1993 World Trade Center bombing, "No one other than the prosecutors, the Clinton Justice Department, and the FBI had access to the materials surrounding the case until they were presented in court, because they were virtually all obtained by a federal grand jury and hence kept not only from the public but from the rest of the government under the extreme secrecy requirements of Rule 6(e) of the Federal Rules of Criminal Procedure." R. James Woolsey, "Blood Baath: the Iraq Connection," New Republic, September 24, 2001, p. 21. Rule 6(e) established requirements for the secrecy of grand jury proceedings.

[144] See CRS Report RL30252, Intelligence and Law Enforcement: Countering Transnational Threats to the U.S., by Richard A. Best Jr.

[145] A key factor appears to have been the potential that litigation over important espionage cases could jeopardize existing practices; see, for instance, the testimony of John Gannon, former head of the National Intelligence Council and other senior government positions, to the Senate Judiciary Committee, May 2, 2006; Gannon claimed that the "early post-war determination to share information and push the 'wall' on information sharing between intelligence and law enforcement was set back by the sensational Ames, Nicholson, and Hanson espionage cases."

and, occasionally, within the U.S. (as in the 1993 World Trade Center attacks). Observers believed that both intelligence and law enforcement agencies were collecting relevant information on international terrorism. Members of Congress began to seek administrative and statutory changes that could facilitate information sharing in this area.

Pursuant to P.L. 105-277, a supplemental appropriations act passed in 1998, the National Commission on Terrorism, headed by former Ambassador L. Paul Bremer, was established to review the laws, regulations, directives, policies and practices for preventing and punishing international terrorism. The Bremer Commission's June 2000 report highlighted concerns about the inadequate sharing of terrorism-related information. It recommended the elimination of barriers to the aggressive collection of information on terrorists and suggested that the FBI suffered from bureaucratic and cultural obstacles to gathering terrorism information. It found that the "Department of Justice applies the statute governing electronic surveillance and physical searches of international terrorists in a cumbersome and overly cautious manner."[146] Although it noted that the FISA application process had been recently streamlined, it recommended that the Justice Department's Office of Intelligence Policy Review (OIPR) should not require the inclusion of information in excess of that which was actually mandated by FISA. It also recommended that OIPR be substantially expanded and that it be directed to cooperate with the FBI.[147]

The Commission further concluded:

> *Law enforcement agencies are traditionally reluctant to share information outside of their circles so as not to jeopardize any potential prosecution. The FBI does promptly share information warning about specific terrorist threats with the CIA and other agencies. But the FBI is far less likely to disseminate terrorist information that may not relate to an immediate threat even though this could be of immense long-term or cumulative value to the intelligence community. . . . Moreover, certain laws limit the sharing of law enforcement information, such as grand jury or criminal wiretap information, with the intelligence community. These laws are subject to different interpretations, so that in some cases it is unclear whether the restrictions apply."*[148]

---

[146] U.S., National Commission on Terrorism, Countering the Changing Threat of International Terrorism, June 2000, p. 10.

[147] Ibid., p. 12.

[148] Ibid., pp. 15-16.

The Commission did not indicate a need for immediate statutory changes, but recommended that the "Attorney General should clarify what information can be shared and direct maximum dissemination of terrorist-related information to policymakers and intelligence analysts consistent with the law."[149]

Initial Efforts to Legislate

Members of Congress did propose various approaches to address the lack of information sharing. S. 2089 as introduced in February 2000 by Senator Specter, would have required that the Attorney General prescribe in regulations the circumstances under which information acquired pursuant to FISA "shall be disclosed for law enforcement purposes." The bill would also have required two reports addressing issues of information sharing. First, it would have tasked the Director of the FBI to submit a report on "the feasibility of establishing within the Bureau a comprehensive intelligence reporting function having the responsibility for disseminating among the elements of the intelligence community information collected and assembled by the Bureau on international terrorism and other national security matters." Secondly, the bill would have required the President to submit a report on the legal authorities that govern the sharing of criminal wiretap information with intelligence agencies and with recommendations to improve the capability of the Justice Department to share "foreign intelligence information or counterintelligence information with elements of the United States intelligence community on matters such as counterterrorism."

In its report on the bill, the Senate Intelligence Committee argued:

> *For the intelligence mission of the United States to be successful, there must be a cooperative and concerted effort among intelligence agencies. Any information collected by one agency under foreign intelligence authorities that could assist another agency in executing its lawful mission should be shared fully and promptly....*
>
> *The Committee has been briefed on the recent efforts by the Federal Bureau of Investigation and the Central Intelligence Agency to enhance their ability to share valuable information collected under FISA orders. The Committee commends these efforts and expects them to continue and to be broadened to include all areas of the foreign intelligence mission.*[150]

---

[149] Ibid, p.16.

[150] U.S. Congress, 106th Congress, 2d session, Senate, Select Committee on Intelligence, The Counterintelligence Reform Act of 2000, S.Rept. 106-352, July 20, 2000, p. 6.

As reported to the Senate in July 2000, S. 2089 was modified to include only a request for reports from the Attorney General on mechanisms for determinations of disclosure of FISA-derived information for law enforcement purposes and on actions taken by the Department of Justice (DOJ) to coordinate the dissemination of intelligence information within DOJ.

Congressional concern about the growing threat of terrorism was also demonstrated in S. 3205, introduced in October 2000 and known as the Kyl-Feinstein Counterterrorism Act of 2000, which was based directly on recommendations of the Bremer Commission that had been released in August. The bill took notice of the attack on the U.S.S. Cole, which had occurred on October 12, 2000, and aimed to discourage financial support of terrorist organizations. This bill also addressed information sharing issues; section 9 would have required a report on the feasibility of assigning the FBI responsibility for disseminating among the elements of the Intelligence Community information collected and assembled by the FBI on international terrorism and other national security matters. Section 10 of the bill would have required a report on the legal authorities that govern the sharing of criminal wiretap information with various law enforcement agencies and intelligence agencies and "recommendations, if any," for legislative language that would improve the Justice Department's capabilities to share information on matters such as counterterrorism with intelligence agencies "with elements of the United States intelligence community on matters such as counterterrorism."

Consideration of the legislation reflected many of the same privacy and civil liberties concerns that had influenced existing procedures in the Justice Department. Criticisms of the approach taken by the legislation were voiced by some civil libertarians. One group opposed the sharing of information obtained by electronic surveillance conducted under Title III authorities with intelligence agencies. Such an effort, it was argued, "breaches the well-established and constitutionally vital line between law enforcement and intelligence activities."[151] Concern was also expressed about the potential use of such information by the CIA and other intelligence agencies: "The secretive data gathering, storage and retention practices of the intelligence agencies are appropriate only when conducted overseas for national defense and foreign policy purposes and only when directed against people who are not U.S. citizens or permanent residents."[152] Further concern was directed at the potential use of information gathered under counterintelligence authorities (presumably FISA) in criminal proceedings:

---

[151] Letter from Laura W. Murphy, Director, American Civil Liberties Union, Washington National Office, James X. Dempsey, Senior Staff Counsel, Center for Democracy and Technology, and Kate Martin, Executive Director, Center for National Security Studies, reprinted in Congressional Record, October 26, 2000, p. S11118.

[152] Ibid.

> *Since the period of ... the Church committee, it has been recognized that the rights of Americans are better protected (and the FBI may be more effective) when international terrorism and national security investigations are conducted under the rules for criminal investigations.*[153]

Such views reflected a continuing distrust of intelligence agencies and a fear that past practices might be revived. In floor debate, Senator Leahy noted that initial drafts of S. 3205 had posed "serious constitutional problems and risks to important civil liberties we hold dear." After modifications, however, "no longer does the bill require a change in the wiretap statute allowing the permissive disclosure of information obtained in a Title III wiretap to the intelligence agencies."[154]

The Clinton Administration Justice Department took a different approach, arguing that then-current statutes and regulations provided law enforcement agencies with "authority under current law to share Title III information regarding terrorism with intelligence agencies when the information is of over-riding importance to the national security." Any change "must accommodate legal constraints such as Criminal Rule 6(e) and the need to protect equities relating to ongoing criminal investigations."[155] Accordingly, the Justice Department specifically opposed the provision in the bill that would permit the sharing of foreign intelligence or counterintelligence information collected under Title III by investigative or law enforcement officer with intelligence agencies.[156]

The Kyl-Feinstein bill would not have changed statutory language, but only asked for reports on the issue of information. Even so, according to Senator Leahy, the initial proposal to mandate such changes "prompted a firestorm of controversy

---

[153] Ibid., p. S11119.

[154] Congressional Record, November 14, 2000, p. S11540. Almost a year later during consideration of the USA PATRIOT Act, Senator Leahy would note that the Justice Department had opposed the original Kyl legislation because it might have opened sensitive materials to the discovery process and it raised issues about sharing information about U.S. persons. Congressional Record, October 25, 2001, p. S 11001.

[155] Letter from Robert Raben, Assistant Attorney General, Department of Justice, reprinted in Congressional Record, October 26, 2000, pp. S11119. The letter did not elaborate on how Rule 6(e) and the need to protect equities could be balanced against the need to share information. Apparently, precise details of a planned assassination plot would meet the "overriding importance" standard, but Raben gave no recognition that intelligence agencies should have access to ambiguous data that might yield evidence of a plot only when combined with other information; in other words, dots that are innocuous in themselves but which, when connected to other information, reveal a dangerous threat.

[156] Ibid., p. S11119.

from civil liberties and human rights organizations, as well as the Department of Justice."[157] Even though the House took no action on this bill, passage of the legislation by the Senate reflected concerns at the end of 2000 regarding the possible need to adjust information sharing mechanisms, coupled with a determination to move cautiously before implementing changes that could affect civil liberties. Ultimately, the legislation was adopted by the Senate on November 14, 2000, but it was not sent to the House before the adjournment of the 106th Congress.

The FY2001 Intelligence Authorization Act, P.L. 106-567, signed on December 27, 2000, reflected the concerns that had inspired both S. 2089 and S. 3205. It included a requirement for a report from the Attorney General on "the authorities and procedures utilized by the Department of Justice for determining whether or not to disclose information acquired under the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) for law enforcement purposes."[158] This Act also formalized procedures for authorizing FISA surveillance, expanded grounds for establishing probable cause, established new procedures for physical searches within FISA, and specified mechanisms to facilitate the use of intelligence in counterintelligence investigations. It provided increased funding for OIPR subsequent to the submission of a report indicating efforts taken to streamline and improve the FISA application process. It included a provision (in section 606) derived from S. 2089 requiring a report from the Attorney General on actions taken to "coordinate the dissemination of intelligence information within the appropriate components of the [Justice] Department and the formulation of policy on national security issues." It did not, however, address the question of making information from law enforcement sources available to the Intelligence Community.

Clearly, the problems created by the existence of the "wall" had not been unrecognized prior to 9/11. The Justice Department's opposition in 2000 to legislative proposals to remove barriers has been noted. On the other hand, some argue that the primary factor in preventing statutory changes was, as one observer has claimed, that "in most instances both the Department of Justice and The White House turned down the requests because it was firmly believed by senior members of the Executive Branch that the United States Congress would

---

[157] Congressional Record, November 14, 2000, p. S11540; Leahy himself, however, had earlier that year indicated support for legislation that would promote information sharing and consultation between intelligence agencies in regard to counterintelligence. "In an area of such national importance, it is critical that our law enforcement and intelligence agencies work together as efficiently and cooperatively as possible." Prepared Statement of Hon. Patrick Leahy printed in U.S. Congress, 106th Congress, 2d session, Senate, Committee on the Judiciary, Subcommittee on Administrative Oversight and the Courts, Counterintelligence Reform Act of 2000, S.Hrg. 106-993, March 7, 2000, p. 12.

[158] Section 604(b), P.L. 106-567.

not allow the IC [Intelligence Community] to have broader surveillance powers."[159] This view would be expressed by former Attorney General William Barr in testimony to the 9/11 Commission:

> *For three decades leading up to 9/11, Congress was at the fore of a steady campaign to curtail the Bureau's domestic intelligence activities and impose on all its activities the standards and process of the criminal justice system. These concerns made it extremely difficult for the Bureau to pursue domestic security matters outside the strictures of the criminal justice process. Prohibitions on sharing grand jury information with intelligence agencies and with using intelligence information in criminal investigations created a 'wall of separation.'*[160]

It is clear in retrospect that there were those in both the Executive Branch and Congress who realized the need to lower barriers to sharing law enforcement and intelligence information, but their views did not, prior to 9/11, reflect a consensus in either branch. Those opposed to greater information sharing did so in large measure because of their awareness of the past history of domestic surveillance and a distrust of intelligence organizations. The result was a number of very tentative steps that, in the event, proved wholly inadequate to task of gathering information about al Qaeda's plot. The FY2001 Intelligence Authorization Act included some minimalist provisions, but the wall was left in place. Neither the Clinton Administration or the Bush Administration, in the first eight months of 2001, sought to amend the relevant laws.[161] The problem was recognized but proposed solutions faced strong opposition.

After 9/11, Congress Tears Down the Wall

The attacks of September 11, 2001, destroyed the World Trade Center and a portion of the Pentagon; they also demolished the wall between U.S. law enforcement and intelligence. After 9/11, it was almost immediately accepted that

---

[159] Robert M. Blitzer (a former FBI official), "Domestic Intelligence Challenges in the 21st Century," (Arlington, VA: Lexington Institute, 2002), p. 10; available at [http://www.lexingtoninstitute.org/docs/497.pdf].

[160] Statement of William P. Barr to the 9/11 Commission, December 8, 2003; available at [http://www.9-11commission.gov/hearings/hearing6/witness_barr.htm].

[161] The incoming Bush Administration was reviewing procedures relating to the wall, but as late as August 2001, Larry D. Thompson, the Deputy Attorney General, reiterated that departmental guidelines regarding the wall were still in effect; Larry D. Thompson Memorandum to Criminal Division, Office of Intelligence Policy and Review, and FBI, August 6, 2001 available at [http://www.cnss.org/9.11commissionintelligence.htm]; see also, John Ashcroft, Never Again: Securing America and Restoring Justice (New York: Center Street, 2006), p. 147; Thomas H. Kean and Lee H. Hamilton, Without Precedent: the Inside Story of the 9/11 Commission (New York: Knopf, 2006), p. 195.

counterterrorism would have to involve all parts of the U.S. Government, including law enforcement agencies and the Intelligence Community. It was agreed that the counterterrorism effort must be based on sharing information from whatever source. The problem for both Congress and the executive branch was to establish appropriate mechanisms for information sharing with adequate safeguards for using the information in future criminal trials.

Congress immediately set about to consider the most appropriate legislative response that could be quickly enacted. Former Attorney General John Ashcroft writes, "The 9/11 attacks occurred on a Tuesday. By Saturday, we had a full-blown legislative proposal. Part of the reasons we were able to move so quickly was that a number of the provisions had been proposed to Congress in 1996, and Congress had rejected them."[162] Attention focused on various proposals and recommendations of commissions that had looked at international terrorism and related issues and to earlier legislative proposals that had not been adopted.[163] A wide number of proposals came together as the USA PATRIOT Act (P.L. 107-56) that would be debated in the final weeks of September and early October 2001.[164] The USA PATRIOT Act changed the requirement that "the purpose" of a FISA surveillance be to collect foreign intelligence information, to require that collecting such information be "a significant purpose" of FISA electronic surveillance or physical search. This provided latitude to use FISA authority for electronic surveillance or physical searches where the primary purpose was criminal investigation, as long as a significant foreign intelligence purpose was also present.

The USA PATRIOT Act also addressed concerns about sharing intelligence and law enforcement information. Although a discussion of all the complex provisions that were included in the USA PATRIOT Act lies beyond the scope of this Report,[165] several provisions address the sharing of law enforcement and intelligence information. Section 203 of the Act removed some of the restrictions on federal government attorneys sharing grand jury information. Subsection

---

[162] Ashcroft, Never Again, p. 154.

[163] One skeptical observer noted that the "great majority of the new surveillance provisions had been discussed within the executive branch or Congress in previous years and had not been adopted. After the September 11 attacks, professional staff in the agencies simply went into their files and pulled out provisions they had been advocating previously. In the super-charged climate of the fall of 2001 many of these provisions received remarkablylittle scrutiny or debate." Peter P. Swire, "The System of Foreign Intelligence Surveillance Law," George Washington Law Review, August 2004, p. 1349.

[164] Unitingand Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001 (P.L. 107-56; signed October 26, 2001). The legislation was adopted by a 357-66 vote in the House and a 98-1 vote in the Senate.

[165] See CRS Report RL31377, The USA PATRIOT Act: A Legal Analysis, by Charles Doyle.

203(a) authorized federal government attorneys to share matters occurring before the grand jury involving foreign intelligence, counterintelligence, or foreign intelligence information with a federal law enforcement, intelligence, protective, immigration, national defense, or national security official to assist that official in the performance of his or her duties. Subsection (a) authorized the sharing of grand jury information "when the matters involve foreign intelligence or counterintelligence."[166]

Subsection 203(b) permitted investigative and law enforcement officers and Government attorneys to share information acquired under or derived from the interception of a wire, oral, or electronic communication under Title III with any other federal law enforcement, intelligence, protective, immigration, national defense or national security official for use in his or her official duties to the extent that the contents of that communication include foreign intelligence or counterintelligence information.

Subsection (c) provides authority for the Attorney General to establish implementing procedures.

Subsection 203(d) permitted the disclosure of foreign intelligence, counterintelligence, or foreign intelligence information obtained as part of a federal criminal investigation, notwithstanding any other provision of law, to any federal law enforcement, intelligence, protective, immigrations, national defense, or national security official in order to assist that official in carrying out his or her official duties, subject to any limitations on the unauthorized disclosure of that information.

Section 504 permitted federal officers conducting electronic surveillance or physical searches under FISA to consult with federal law enforcement officers or state or local law enforcement personnel to coordinate against actual or potential attacks or other grave hostile acts of a foreign power or its agent; sabotage or international terrorism by a foreign power or its agent, or clandestine intelligence activities by an intelligence service or network of a foreign power or its agent.

Section 905 requires the Attorney General or heads of other Federal agencies with law enforcement responsibilities to disclose expeditiously to the DCI (later replaced by the Director of National Intelligence (DNI)), under relevant guidelines, foreign intelligence acquired in the course of a criminal investigation. Exceptions could be made where the disclosure of such foreign intelligence would jeopardize an ongoing law enforcement investigation or impair other significant

---

[166] Section 203(a)(1) provides that any Federal official to whom such information is made available may use it only in the conduct of that person's official duties. Further: "Within a reasonable time after such disclosure, an attorney for the government shall file under seal a notice with the court stating the fact that such information was disclosed and the departments, agencies, or entities to which the disclosure was made."

law enforcement interests. In addition, Section 905 required the Attorney General, in consultation with the DCI (now the DNI), to develop procedures to give the Director timely notice of the Attorney General's decision to begin or decline to begin a criminal investigation based on information from an element of the intelligence community regarding possible criminal activity of a foreign intelligence source or potential source.[167]

The provisions included in the USA PATRIOT Act and DOJ's effort to implement them were far-reaching and to some extent were not welcomed by the FISA Court. In particular, the FISA Court in In re all Matters Submitted to the Foreign Intelligence Court found that proposed 2002 procedures issued by the Attorney General "eliminate[d] the bright line in the 1995 procedures prohibiting direction and control by prosecutors on which the Court has relied to moderate the broad acquisition[,] retention, and dissemination of FISA information in overlapping intelligence and criminal investigations."[168] The FISA Court thus attempted to "reinstate the bright line used in the 1995 procedures, on which the Court has relied."[169]

Concerned that its proposed procedures were rejected, the Justice Department appealed the Foreign Intelligence Surveillance Court's granting of a request modified in accordance with its earlier ruling in In re All Matters Submitted to the Foreign Intelligence Surveillance Court. The appeal went to the Foreign Intelligence Surveillance Court of Review and was the first appeal to that court. In a sweeping decision, the Court of Review overruled the limitations imposed by the FISA Court, along with a considerable amount of customary FISA practice. The Court of Review expressed concern that the FISA Court had overstepped its role by prescribing the internal procedures for handling surveillances within the Justice Department. The Court of Review maintained that the FISA Court "determined an investigation became primarily criminal when the Criminal Division played a lead role. This approach has led, over time, to the quite

---

[167] The Act provided that some, but not all, of its provisions would expire (or "sunset") at the end of 2005, giving Congress the opportunity to assess their effects in the intervening months. Subsections 203(b) and 203(d) (but not (a) and (c)) were among those that were scheduled to sunset; section 905 was not scheduled to sunset. As noted by Charles Doyle, CRS Report RL32186, USA PATRIOT Act Sunset Provisions That Were to Expire on December 31, 2005, these provisions are similar to and may duplicate other statutory provisions in the USA PATRIOT Act and other legislation that were not scheduled to sunset; the legal issue regarding the extent to which these provisions are in fact duplicative lies beyond the scope of this Report. In any event, P.L.109-177, signed on March 9, 2006, made subsections 203(b), 203(d) and 905 permanent. See also CRS Report RL33332, USA PATRIOT Improvement and Reauthorization Act of 2005: A Legal Analysis, by Brian T. Yeh and Charles Doyle.

[168] In re all matters submitted to the Foreign Intelligence Surveillance Court, 218 F. Supp.2d, pp. 621-622 (May 17, 2002).

[169] Ibid., p. 625.

intrusive organizational and personnel tasking the FISA [C]ourt adopted. Putting aside the impropriety of an Article III court imposing such organizational strictures ... [the wall] was unstable because it generates dangerous confusion and creates perverse organizational incentives."[170] The Court of Review thereby gave the final blow to the legal structure supporting the wall between law enforcement and intelligence information.

Implementation of the information-sharing provisions of the USA PATRIOT Act and other legislation is underway. The Homeland Security Act of 2002 (P.L. 107-296) and the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458) required that procedures be established under which federal agencies can share intelligence and law enforcement information about international terrorism. The Intelligence Reform Act mandated the creation of an Information Sharing Environment (ISE) that combines policies, procedures, and technologies to link information collections and users. In November 2006 the Administration released a lengthy implementation plan for the ISE. The plan sets forth procedures for sharing information among agencies at federal, state, and local levels and seeks to promote a culture of information sharing. It also provides procedures for protecting information privacy and civil liberties.[171] Congress may choose to review the implementation of the ISE during coming months.

Conclusion

A fundamental issue that faces both Congress and the U.S. public remains the need to balance the advantages to be gained by sharing information from all sources with the possibility that the availability of data accumulations could be used to undermine lawful political or religious activities. An unstable balance between these two separate goals — often portrayed as competing — greatly complicated the counterterrorism and counterintelligence effort prior to 9/11. The fact that public opinion appeared deeply ambivalent made procedural changes difficult and contributed to the luxuriant growth of complex regulations adopted by DOJ and endorsed by the FISA Court. After 9/11, public opinion shifted dramatically, resulting in the rapid passage of the USA PATRIOT Act and other legislation. The need to encourage the sharing of information and the connection of dots is now unquestioned, but there are lingering concerns about the risks that widespread information sharing may jeopardize civil liberties. Congress will undoubtedly seek to determine whether the new statutes,

---

[170] In re Sealed Case, 310 F.3d, p. 743 (November 18, 2002).

[171] The implementation plan is available at [http://www.ise.gov/docs/ISE-impplan200611.pdf]. For additional background see U.S. Government Accountability Office, Information Sharing: the Federal Government Needs to Establish Policies and Processes for Sharing Terrorism-Related and Sensitive but Unclassified Information, GAO-06-385, March 17, 2006. Many of the initiatives in regard to the ISE have been widely criticized; see Ellen Nakashima, "Civil Libertarians Protest Privacy Policy; New Guidelines Do Little to Protect Established Rights, White House Board Told," Washington Post, Dec. 6, 2006, p. A11.

regulations, and procedures that have been adopted will prove both effective and sensitive to individual rights.

The importance of sharing intelligence and law enforcement information is not limited to issues relating to international terrorism but extends to banking fraud, narcotics smuggling, and a variety of international concerns. Narcotics smuggling, for instance, can be addressed by encouraging other countries to halt the cultivation of opium poppies or coca, as well as by law enforcement in the U.S. Terrorism, of course, is uniquely threatening and in combating terrorists more vigorous non-law enforcement approaches are considered more legitimate than is the case with drug smugglers or embezzlers. What is advantageous in all cases is assembling the full range of information about the activity and subjecting it to rigorous analysis.

There is, however, the possibility that the current consensus may unravel. The political controversy surrounding NSA's electronic surveillance efforts and other data mining programs may come to focus on the sharing of information that some argue was not lawfully obtained, and this concern could lead to efforts to restrict information sharing across the boards. There is also a possibility that the use of information obtained by surveillance in accordance with FISA might ultimately not be allowed in court cases out of concern that the Fourth Amendment has been bypassed.[172] Despite the widespread acceptance of the need for information sharing, concerns that sharing information could lead to governmental abuses persists across the political spectrum. These concerns are tenaciously held, and have in the past made legislating very controversial. There is no reason to believe that they will not resurface should the threat from international terrorism seem less menacing.

The potential threat to civil liberties does not, of course, represent the full extent of the issues raised by increased information sharing. Sharing sensitive information inevitably raises the danger that intelligence sources and methods may be compromised either accidentally or purposefully. For intelligence professionals, in particular, the danger to valuable sources that may have taken years to develop is a fundamental concern. Moreover, when a human source is compromised there is not only a danger to a particular individual, but also a potential loss of confidence in U.S. intelligence agencies by other actual or potential sources.

---

[172] This possibility was even alluded to by the November 2002 Foreign Intelligence Court of Review that maintained that "…a FISA order may not be a 'warrant' contemplated by the Fourth Amendment. The government does not actually claim that it is, instead noting only that there is authority for the proposition that a FISA order is a warrant in the constitutional sense." The Court of Review added: "We do not decide the issue but note that to the extent a FISA order comes close to meeting Title III, that certainly bears on its reasonableness under the Fourth Amendment." In re: Sealed Case, 310 F.3d, p. 742.

The role of Congress in dealing with information sharing issues is especially important. There are delicate questions of liberty and security involved and a sensitive balance is crucial. Air Force General Michael V. Hayden, who now serves as CIA Director, in the past argued that Members of Congress are in close touch with their constituents and "What I really need you to do is talk to your constituents and find out where the American people want that line between security and liberty to be."[173] Congress also can provide the ongoing oversight to ensure that the sorts of abuses that occurred in the 1960s and 1970s do not recur. Ultimately, an information sharing policy that is largely consistent with public opinion and is held to account by rigorous oversight should enhance the chances that the dots can be connected without jeopardizing the rights of Americans. Observers see a danger, however, that gridlock in both the Executive and Legislative Branches might inhibit the government's ability to find effective and sensible ways to acquire and analyze information on new threats to the national security.

[173] Testimony of Lt. Gen. Michael V. Hayden, USAF, U.S. Congress, 107th Congress, Senate, Select Committee on Intelligence, and House of Representatives, Permanent Select Committee on Intelligence, Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001, Hearings, Vol. II, October 1, 3, 8 and 17, 2002, S.Hrg. 107-1086, pp.801-802.

Privacy: Total Information Awareness Programs and Related Information Access, Collection, and Protection Laws, RL31730 (March 21, 2003).

GINA MARIE STEVENS, CONGRESSIONAL RESEARCH SERV., PRIVACY: TOTAL INFORMATION AWARENESS PROGRAMS AND RELATED INFORMATION ACCESS, COLLECTION, AND PROTECTION LAWS (2003), *available at* http://www.intelligencelaw.com/library/secondary/crs/pdf/RL31730_3-21-2003.pdf.

Order Code RL31730
Updated March 21, 2003

Gina Marie Stevens
Legislative Attorney
American Law Division

The author wishes to thank Attorneys Maureen Murphy and Charles Doyle of the American Law Division for their substantial contributions to this report.

Summary

This report describes the Total Information Awareness (TIA) programs in the Defense Research Projects Agency (DARPA) of the Department of Defense, and related information access, collection, and protection laws. TIA is a new technology under development that plans to use data mining technologies to sift through personal transactions in electronic data to find patterns and associations connected to terrorist threats and activities. Data mining technologies are currently used by federal agencies for various purposes. DARPA has underway a five year research project to develop and integrate information technologies into prototype systems to identify foreign terrorists for use by the intelligence, counterintelligence, law enforcement, and homeland security communities. Recent increased awareness about the existence of the TIA project provoked expressions of concern about the potential for the invasion of privacy of law-abiding citizens by the Government, and about the direction of the project by John Poindexter, a central figure in the Iran-Contra affair. While the law enforcement and intelligence communities argue that more sophisticated information gathering techniques are essential to combat today's sophisticated terrorists, civil libertarians worry that the Government's increased capability to assemble information will result in increased and unchecked government power, and the erosion of individual privacy. A coalition of public interest groups has asked Congress to intervene.

Significant policy and legal issues are raised by the government's TIA plans. Chief among them are privacy issues involving questions of access to, and use and disclosure of personal information by the federal government. This report

describes current laws and safeguards to protect the privacy of personal information, the required legal process for officials who seek access to information, and the provisions currently in place that permit access and dissemination of information for law enforcement, intelligence, and terrorism purposes. Federal laws currently protect government, credit, communications, education, bank, cable, video, motor vehicle, health, telecommunications, children's, and financial information; generally carve out exceptions for disclosure of personal information; and authorize use of warrants, subpoenas, and court orders to obtain information.

Some Members of Congress seek additional Congressional oversight of TIA programs. Legislation has been introduced in the 108th Congress regulating TIA programs. On January 23, 2003, the Senate passed amendment S.Amdt. 59 to H.J.Res. 2, the Omnibus Appropriations Act for Fiscal Year 2003, imposing limitations on the unfolding Total Information Awareness programs, and requiring a detailed report to Congress. On February 13, 2003, both the House and Senate approved the Fiscal Year 2003 omnibus spending bill (P.L. 108-7) including, with slight modifications, the language from S.Amdt. 59. For more information, see CRS Report RL31786, Total Information Awareness Programs: Funding, Oversight and Composition Issues by Amy Belasco; and CRS Report RL31798, Data Mining: An Overview, by Jeffrey Seifert. This report will be updated as warranted.

Total Information Awareness Programs

The September 11th terrorist attacks increased government awareness of the inadequacies of its information gathering techniques, its information technology, and its information holdings. To remedy this situation various federal agencies are addressing issues that may possibly have a direct bearing on the balance between the government's need for information and an individual's expectation of privacy in their information. This report describes the Total Information Awareness (TIA) programs underway in the Department of Defense (DOD) which may develop prototype research and development technologies for information gathering and analysis capabilities that could be used by DOD and other agencies. It will then discuss current laws and safeguards to protect the privacy of personal information, the provisions currently in place that permit access and dissemination of information for law enforcement, intelligence, and terrorism purposes, and the required legal process for officials who seek access to information.

The TIA program is being developed by the Defense Advanced Research Projects Agency (DARPA) of the Department of Defense in the Information Awareness Office (IAO)[174] as an experimental prototype system that integrates three types of

[174] The Total Information Awareness program will integrate some or all of the R&D efforts that are managed by the Information Awareness Office, including Project Genoa, Project Genoa II,

technologies — machine translation of languages; data search and pattern recognition; and advanced collaborative and decision support.[175] DARPA "aspires to create the tools that would permit analysts to data-mine an indefinitely expandable universe of databases" "to analyze, detect, classify and identify foreign terrorists – and decipher their plans – and thereby enable the U.S. to take timely action to successfully preempt and defeat terrorist acts."[176] The TIA system is designed to be a tool in the war against terrorism that "would, among other things, help analysts search randomly for indications of travel to risky areas, suspicious emails, odd fund transfers and improbable medical activity, such as the treatments of anthrax sores."[177] The goal of the TIA program is "to create a counter-terrorism information system that: (i) increases the information coverage . . . ; (ii) provides focused warnings within an hour after a triggering event occurs or an evidence threshold is passed; [and] (iii) can automatically cue analysts based on partial pattern matches and analytical reasoning, and information sharing . . . ."[178] DARPA's five year research project to develop and integrate information technologies into a prototype system for use by the intelligence, counterintelligence and law enforcement communities intends to exploit R&D efforts that have been underway for several years in DARPA and elsewhere, as well as private sector data mining technology.[179]

DARPA envisions a database "of an unprecedented scale, [that] will most likely be distributed, must be capable of being continuously updated, and must support both autonomous and semi-automated analysis."[180] Extensive existing databases from both private and public sector information holdings will be used to obtain transactional and biometric data.[181] Transactional data for the TIA database could include financial (e.g., banks, credit cards, and money transmitters, casinos and brokerage firms), educational, travel (e.g., airlines, rail, rental car), medical,

---

Genisys, Evidence Extraction and Link Discovery, Wargaming the Asymmetric Environment, Translingual Information Detection, Extraction and Summarization, Human Identification at a Distance, Bio-Surveillance, Communicator, and Babylon, as well as possibly other R&D developed by DARPA, DOD, other federal agencies, and the private sector. See CRS Report RL31786, Total Information Awareness Programs: Funding, Oversight and Composition Issues, by Amy Belasco.

[175] See Defense Advanced Research Projects Agency's Information Awareness Office and Total Information Awareness Project at [http://www.darpa.mil/iao/programs.htm].

[176] [http://www.darpa.mil/iao/TIASystems.htm].

[177] Robert O'Harrow, U.S. Hopes to Check Computers Globally; System Would Be Used to Hunt Terrorists, Washington Post A4 (Nov. 12, 2002).

[178] [http://www.darpa.mil/body/NewsItems/pdf/DARPAfactfile.pdf].

[179] [http://www.darpa.mil/iao/BAA02-08.pdf].

[180] [http://www.darpa.mil/iao/TIASystems.htm].

[181] [http://www.darpa.mil/iao/solicitations.htm].

veterinary, country entry, place/event entry, transportation, housing, critical resources, government, and communications (e.g., cell, landline, Internet) data. Biometric data for the database could include face, finger prints, gait, and iris data.[182] The TIA system could seek access to databases to discover connections between "passports; visas; work permits; driver's license; credit card; airline tickets; rental cars; gun purchases; chemical purchases – and events – such as arrest or suspicious activities and so forth."[183]

Data Mining

A key component of the TIA program is the deployment of data mining technologies to sift through data and transactions to find patterns and associations to discover and track terrorists.[184] The idea is that "if terrorist organizations are going to plan and execute attacks against the United States, their people must engage in transactions and they will leave signatures in this information space. . . ."[185] TIA plans to mine transaction data for terrorism-related indicators to uncover terrorists plans or attacks. Data mining is the search for significant patterns and trends in large databases using sophisticated statistical techniques and software.[186] The widespread use of computers, and the large amount of information maintained in databases means that there exists a vast repository of information useful for antiterrorism purposes. Today, "it is a rare person in the modern world who can avoid being listed in numerous databases."[187] Data mining technologies facilitate the use of information.

Data mining technologies are currently used by federal agencies for various purposes, and plans exist for considerable expansion of this technology. For example, the Department of Justice is engaged in data mining projects that utilize computer technology to analyze information to reveal patterns of behavior consistent with terrorist activities. Utilizing law enforcement and intelligence information as well as public source data, the Foreign Terrorist Tracking Task Force employs risk modeling algorithms, link analysis, historic review of past patterns of behavior, and other factors to distinguish persons who may pose a

---

[182] See John Woodward, Jr., Rand Corporation, Superbowl Surveillance: Facing Up to Biometrics (2001) available at [http://www.rand.org/publications/IP/IP209/IP209.pdf].

[183] Solicitations, supra note 8.

[184] See CRS Report RL31798, Data Mining: An Overview, by Jeffrey Seifert.

[185] [http://www.darpa.mil/DARPATech2002/presentations/iao_pdf/speeches/POINDEXT.pdf].

[186] Carol Pickering, They're Watching You: Data-Mining Firms Are Watching Your Every Move – and Predicting the Next One, Business 2.0 (Feb. 2000) at [http://www.business2.com].

[187] Whitfield Diffie and Susan Landau Diffie, Privacy on the line: the Politics of Wiretapping and Encryption at119 (1998).

risk of terrorism from those who do not.[188] The Transportation Security Administration's Computer- Assisted Passenger Profiling System is widely employed by the airlines.[189] The National Strategy for Homeland Security includes several initiatives to integrate terrorist-related information from the databases of all government agencies responsible for homeland security. Under this initiative, the Department of Homeland Security, Department of Justice, FBI, and numerous state and local law enforcement agencies would have access to information analysis, using advanced data-mining techniques to reveal patterns of criminal behavior and detain suspected terrorists before they act.[190] Additionally, on January 28, 2003 President Bush proposed to establish a new Terrorism Threat and Integration Center to merge and analyze terrorist-related information collected domestically and abroad.[191]

DOD recently announced plans to form an internal TIA oversight board to establish policies and procedures for use of TIA within and outside of DoD, and to establish an external federal advisory committee to advise the secretary of Defense on policy and legal issues raised by TIA technologies.[192]

Legal Issues

Government access to and mining of information on individuals held in a multiplicity of databases, public and private, raises a plethora of issues – both legal and policy. To what extent should the government be able to gather and mine information about individuals to aid the war against terrorism?[193] Should unrestricted access to personal information be permitted? Should limitations, if any, be imposed on the government's access to information? In resolving these issues, the current state of the law in this area may be consulted. The rest of this report describes current laws and safeguards to protect the privacy of personal

---

[188] The White House Office of Homeland Security, The National Strategy for Homeland Security at 39 (July 2002) at [http://www.whitehouse.gov/homeland/book/index.html].

[189] Section 307 of the Federal Aviation Reauthorization Act of 1996 (P.L. 104-264, 110 Stat. 3253) directed FAA to assist airlines in developing a computer-assisted passenger profiling system in conjunction with other security measures and technologies. See [http://www.house.gov/transportation/aviation/02-27-02/02-27-02memo.html].

[190] Supra note 14.

[191] [http://www.whitehouse.gov/news/releases/2003/01/20030128-12.html].

[192] Available at [http://www.defenselink.mil/news/Feb2003/t02072003_t0207atl.html].

[193] The Markle Foundation Task Force on National Security in the Information Age recently proposed guidelines to allow the effective use of information (including the use of data mining technologies) in the war against terrorism while respecting individuals' interests in the use of private information. The Markle Foundation Task Force on National Security in the Information, Protecting America's Freedom in the Information Age at 32 - 34 (October 2002) at [http://www.markle.org/news/NSTF_Part_1.pdf].

information, the required legal process for officials who seek access to information, and the provisions currently in place that permit access and dissemination of information for law enforcement and intelligence gathering purposes. Following is a description of selected information access, collection, and disclosure laws and regulations.

Federal Laws Governing Federal Government Access to Information

Generally there are no blanket prohibitions on federal government access to publicly available information (e.g., real property records, liens, mortgages, etc.). Occasionally a statute will specifically authorize access to such data. The USA PATRIOT Act, for example, in transforming the Treasury Department's Financial Crimes Enforcement Network (FinCEN) from an administratively established bureau to one established by statute, specified that it was to provide government-wide access to information collected under the anti-money laundering laws, records maintained by other government offices, as well as privately and publicly held information. Other government agencies have also availed themselves of computer software products that provide access to a range of personal information. The FBI reportedly purchases personal information from ChoicePoint Inc, a provider of identification and credential verification services, for data analysis.[194]

As previously discussed the federal government seeks access to publicly and privately held databases in order to build a centralized database to detect and deter against terrorist threats and attacks. This section of the report describes existing legal safeguards for the protection of personal information. It covers applicable federal laws; a discussion of state laws is beyond its scope. In the United States there is no omnibus statute or constitutional provision that provides comprehensive legal protection for the privacy of personal information, but rather an assortment of laws regulate information deemed to be of sufficient importance to be afforded some level of protection. The U.S. Constitution, federal statutes and regulations, and state law combine to govern the collection, use, and disclosure of information. The Constitution provides certain privacy protections, but does not explicitly protect information privacy.[195] Its protections extend only to the protection of the individual against government intrusions, and its guarantees are not applicable unless "state action" has taken place. In other words its guarantees extend to government intrusions rather than private sector abuses. The Fourth Amendment search-andseizure provision protects a right of

---

[194] Glenn R. Simpson, "Big Brother-in-Law: If the FBI Hopes to Get The Goods on You, It May Ask ChoicePoint — U.S. Agencies' Growing Use Of Outside Data Suppliers Raises Privacy Concerns" Wall Street Journal, April 13, 2001 (The company "specialize[s] in doing what the law discourages the government from doing on its own– culling, sorting and packaging data on individuals from scores of sources, including credit bureaus, marketers and regulatory agencies.").

[195] Whalen v. Roe, 429 U.S. 589 (1977).

privacy by requiring warrants before government may invade one's internal space or by requiring that warrantless invasions be reasonable.[196] That amendment protects individual privacy against certain kinds of governmental intrusion. The Supreme Court has interpreted this language as imposing a warrant requirement on all searches and seizures predicated upon governmental authority, and has ruled that violations of this standard will result in the suppression in any criminal proceeding of any material or information derived therefrom. The Court has also recognized exceptions to the warrant requirement. Finally, an individual has no Fourth Amendment rights with respect to information held by third parties.[197]

There is no comprehensive federal statute that protects the privacy of personal information held by the public sector and the private sector. Instead federal law tends to employ a sectoral approach to the regulation of personal information. Historically, the individual's privacy interests have been balanced with the government's information needs.[198] Examples of this balancing of personal and governmental interests can be found in the numerous privacy-related enactments of the past twenty-five years. Federal laws protect government, credit, communications, education, bank, cable, video, motor vehicle, health, telecommunications, children's, and financial information. These laws generally carve out exceptions for the disclosure of personally identifiable information to law enforcement officials, and authorize access to personal information through use of search warrants, subpoenas, and court orders. Notice requirements vary according to statute.

Federal Government Information

The Privacy Act

The Privacy Act of 1974, 5 U.S.C. § 552a, was implemented to protect the privacy of individuals identified in information systems maintained by federal executive branch agencies, and to control the collection, use, and sharing of information. The Act restricts disclosure of personally identifiable records maintained by agencies; grants individuals increased rights of access to agency records maintained on themselves; grants individuals the right to seek amendment of agency records maintained on themselves upon a showing that the records are not accurate, relevant, timely or complete; and establishes a code of "fair information practices" which requires agencies to comply with statutory norms for collection, maintenance, and dissemination of records.

---

[196] "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. Amend. IV.

[197] United States v. Miller, 425 U.S. 435 (1976).

[198] Privacy Protection Study Commission, Personal Privacy in an Information Society (1977).

The general exemptions of the Privacy Act, which are agency and function-oriented, permit the Central Intelligence Agency[199] and federal criminal law enforcement agencies to exempt certain systems of records from some of the Act's requirements.[200] The general exemption for the CIA covers all of its files. The general exemption for federal criminal law enforcement agencies covers identification information, criminal investigative materials, and reports compiled between the stages of arrest and release from criminal agency supervision. An agency which has law enforcement, prosecution, or probation activities can use this general exemption. In addition specific exemptions permit an agency to exempt a system of records from specified Privacy Act requirements if the system of records is: national security information which would be protected from mandatory disclosure by FOIA;[201] law enforcement material which falls outside the criminal law enforcement general exemption; Secret Service files; Census material and other matter required by law to be kept only as a statistical record; confidential sources of government background investigation information; test materials of the civil service selection and promotion process; and confidential evaluations of military and naval personnel.[202]

The general disclosure rule under the Privacy Act is that unless a statutory exception applies, no federal executive branch agency shall disclose any record which is contained in a system of records to any person or to another agency except pursuant to a written request by, or with prior written consent of the individual to whom the record pertains.[203] Disclosure includes dissemination within the executive branch from one agency to another or from one large segment of an agency to another segment.[204] This rule would appear to prohibit the sharing of personal information collected by one agency with other agencies for purposes other than for which it was originally collected. In reality, though, the Act's many exemptions and exceptions ease this prohibition. Many of the

---

[199] 32 CFR Part 109.

[200] 5 U.S.C. § 552a(j).

[201] 5 U.S.C. § 552(b)(1). Exemption 1 of the FOIA protects from disclosure national security information concerning the national defense or foreign policy, provided that it has been properly classified in accordance with the requirements of an executive order.

[202] 5 U.S.C. § 552a(k).

[203] 5 U.S.C. § 552a(b).

[204] Office of Management and Budget, Guidelines for Implementing Section 552a of Title 5, at 6 (1975).

exceptions – as well as specific laws authorizing sharing of records – permit an agency to disclose or share personal information with other agencies.[205]

Several of the statutory exemptions are relevant to the information collection and sharing activities of the Total Information Awareness system, and would appear to authorize the disclosure of personal information in federal records systems without the individual's consent.[206] The routine use exemption allows an agency to share, without consent, an individual's personal information with other agencies if that sharing is listed as a routine use for that agency in the Federal Register and is compatible with the purpose of the initial information gathering.[207] The January 2003 publication by the Transportation Security Administration of a notice to amend the "Aviation Security Screening Records" system of records illustrates how broadly records can be disclosed pursuant to the routine use exemption, without the consent of the subject of the record, for agency purposes.[208] The exemption for civil and criminal law enforcement

---

[205] 5 U.S.C. § 552a(b).

[206] See Sean Fogarty and Daniel R. Ortiz, "Limitations Upon Interagency Information Sharing: The Privacy Act of 1974" in The Markle Foundation Task Force Report, National Security in the Information Age at 127 - 132 (October 2002).

[207] 5 U.S.C. § 552a(b)(3). The OMB guidelines state that the "compatibility" concept encompasses functionality equivalent uses, and other uses that are necessary and proper.

[208] Records in the system include passenger name records (PNRs) and associated data; reservation and manifest information of passenger carriers and, in the case of individuals who are deemed to pose a possible risk to transportation security, record categories may include: risk assessment reports; financial and transactional data; public source information; proprietary data; and information from law enforcement and intelligence sources. Data are retrievable by the name or other identifying information of the individual, such as flight information. Information may be disclosed from this system as follows (routine uses of records): (1) to appropriate Federal, State, territorial, tribal, local, international, or foreign agencies responsible for investigating or prosecuting the violations of, or for enforcing or implementing, a statute, rule, regulation, order, or license, ... (2) to contractors, grantees, experts, consultants, agents and other non-Federal employees performing or working on a contract, service, grant, cooperative agreement, or other assignment from the Federal government for the purpose of providing consulting, data processing, clerical, or other functions to assist TSA . . . . (3) to Federal, State, territorial, tribal, and local law enforcement and regulatory agencies–foreign, international, and domestic–in response to queries regarding persons who may pose a risk to transportation or national security; a risk of air piracy or terrorism or a threat to airline or passenger safety; or a threat to aviation safety, civil aviation, or national security. (4) to individuals and organizations, in the course of enforcement efforts, to the extent necessary to elicit information pertinent to the investigation, prosecution, or enforcement of civil or criminal statutes, rules, regulations or orders regarding persons who may pose a risk to transportation or national security; a risk of air piracy or terrorism or a threat to airline or passenger safety; or a threat to aviation safety, civil aviation, or national security. (5) to a Federal, State, or local agency, where such agency has requested information relevant or necessary for the hiring or retention of an individual, or issuance of a security clearance, license, contract, grant, or other benefit. (6) to the news media . . . . (7) to the Department of State, or other Federal agencies concerned with visas and immigration, and to

activities permits the disclosure of personal information for legally authorized activities.[209] This exemption would allow the disclosure of information to an intelligence agency for the prevention of terrorist acts. The exemption for foreign counterintelligence in the Computer Matching and Privacy Protection Act of 1988,[210] which amended the Privacy Act, legitimizes information sharing through data matching among agencies for national security purposes.[211]

Agencies are required to make reasonable efforts to serve notice on an individual when any record on such individual is made available to any person under compulsory legal process when such process becomes a matter of public record.

Education Information

The Family Educational Rights and Privacy Act of 1974

FERPA governs access to and disclosure of personally identifiable information in educational records held by federally funded educational institutions and agencies.[212] Disclosure requires prior consent of the student's parents unless done pursuant to federal grand jury subpoena, administrative subpoena, or court order for law enforcement purposes. Upon good cause shown, the court shall order that the existence or contents of a subpoena or the information furnished not be disclosed. The USA PATRIOT Act of 2001 amended FERPA to authorize the Justice Department to obtain a court order to collect education records relevant to a terrorism-related offense or an act of domestic or international terrorism.[213] The order can only be issued if a court finds that the records are relevant to a terrorism investigation. The amendment also protects educational institutions from liability for complying with such order.

---

agencies in the Intelligence Community, to further those agencies' efforts with respect to persons who may pose a risk to transportation or national security; a risk of air piracy or terrorism or a threat to airline or passenger safety; or a threat to aviation safety, civil aviation, or national security. (8) to international and foreign governmental authorities in accordance with law and . . international agreements. (9) in proceedings before any court, administrative, adjudicative, or tribunal body before which TSA appears, . . . provided, however, that in each case, TSA determines that disclosure of the records in the proceeding is a use of the information contained in the records that is compatible with the purpose for which the records were collected. (10) to airports and aircraft operators . . .. (11) to the National Archives and Records Administration . . . . 68 Fed. Reg. 2101 (Jan. 15, 2003).

[209] 5 U.S.C. § 552a(b)(7).

[210] P.L. 100-503, 5 U.S.C. § 552a note.

[211] 5 U.S.C. 552a(a)(8)(B)(vi).

[212] 20 U.S.C. § 1232g. See CRS Report RL31482, The Family Educational Rights and Privacy Act of 1974: Recent Developments in the Law.

[213] P.L. 107-56, 20 U.S.C. § 1232g(j). See CRS Report RL31377: The USA PATRIOT Act: A Legal Analysis.

The Cable Communications Policy Act of 1984

Limits the disclosure of cable television subscriber names, addresses, and utilization information.[214] Cable companies are prohibited from disclosing personally identifiable information concerning a cable subscriber to the government except pursuant to a court order. The order can only be issued if a court finds clear and convincing evidence that the customer was suspected of engaging in a crime and that the information sought was material evidence in the case; and the subject was afforded the opportunity to appear and contest the government's claim. The USA PATRIOT Act of 2001 amended the Cable Act's privacy provision to clarify that it applies only to information about a customer's cable TV service, but not to information about a customer who receives Internet or telephone service from a cable provider. When the government is requesting information about a customer receiving Internet or telephone service from a cable provider, the federal electronic surveillance statutes apply.

The Video Privacy Protection Act of 1988

Regulates the treatment of personally identifiable information collected in connection with video sales and rentals.[215] The Act prohibits videotape service providers from disclosing their customers' names, addresses, and specific videotapes rented or purchased except pursuant to customer consent, or pursuant to a federal or state search warrant, grand jury subpoena, or court order issued to a law enforcement agency. The order can only be issued if a court finds that there is probable cause to believe that the records or other information sought are relevant to a legitimate law enforcement inquiry. Issuance of court orders requires prior notice to the customer. A court may quash or modify such order if the information or records requested are unreasonably voluminous or if compliance would cause an unreasonable burden on the provider.

Telecommunications Act of 1996

Limits the use and disclosure of customer proprietary network information (CPNI) by telecommunications service providers.[216] The statute does not include specific provisions for the disclosure of CPNI to law enforcement or government officials. Except as required by law or with customer consent, a telecommunications carrier must only use, disclose, or permit access to

---

[214] 47 U.S.C. § 551.

[215] 18 U.S.C. § 2710.

[216] 47 U.S.C. § 222. See CRS Report RL30671, Personal Privacy Protection: The Legislative Response.

individually identifiable customer proprietary network information in providing the telecommunications service. Upon customer request, a telecommunications carrier may disclose that customer's proprietary network information to any person designated by the customer. Customer proprietary network information is information that relates to the quantity, technical configuration, type, destination, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship, and includes information contained in the bills pertaining to telephone exchange service or telephone toll service, but does not include subscriber list information.

Health Information

The Health Insurance Portability and Accountability Act of 1996

HIPAA required publication of a medical privacy rule by the Department of Health and Human Services (HHS) in the absence of a congressional enactment.[217] The final privacy rule, "Standards for the Privacy of Individually Identifiable Health Information," was published in December 2000 and modified in August 2002.[218] Enforcement of the rule goes into effect for the majority of covered entities April 2003. The rule establishes privacy protections for individually identifiable health information held by health care providers, health care plans, and health care clearinghouses. It establishes a series of regulatory permissions for uses and disclosures of individually identifiable health information.[219] Individually identifiable health information is health information created or received by a covered entity (health care provider, health plan, or health care clearinghouse) that relates to past, present, or future physical or mental health or a condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and identifies the individual or there is a reasonable basis to believe that the information can be used to identify the individual. The rule excludes education records covered by FERPA, and employment records held by a covered entity in its role as employer.

The medical privacy rule establishes new procedures and safeguards to restrict the circumstances under which a covered entity may give such information to law enforcement officers. For example, the rule limits the type of information that covered entities may disclose to law enforcement, absent a warrant or other prior process, when law enforcement is seeking to identify or locate a suspect. It specifically prohibits disclosure of DNA information for this purpose, absent

---

[217] P.L. 104-191 § 264, 42 U.S.C. 1320d note.

[218] Standards for the Privacy of Individually Identifiable Health Inforamtion,45 CFR Parts 160 and 164 at [http://www.hhs.gov/ocr/combinedregtext.pdf].

[219] See CRS Report RS20934, A Brief Summary of the Medical Privacy Rule.

some other legal requirements such as a warrant. Where state law imposes additional restrictions on disclosure of health information to law enforcement, those state laws continue to apply. This rule sets a national floor of legal protections. In those circumstances when disclosure to law enforcement is permitted by the rule, the privacy rule does not require covered entities to disclose any information. In the event that some other federal or state law requires a disclosure, the privacy rule does not interfere with the operation of those other laws. However, unless the disclosure is required by some other law, covered entities are to use their professional judgment to decide whether to disclose information.

For law enforcement purposes the rule permits disclosure without consent or authorization pursuant to process, and as otherwise required by law.[220] A covered entity may disclose protected health information as required by law;[221] or in compliance with the requirements of (i) a court order or court-ordered warrant, a judicial subpoena or summons, (ii) a grand jury subpoena, or (iii) an administrative request, including an administrative subpoena or summons, a civil or authorized investigative demand, or similar process authorized under law, provided that the information sought is relevant and material to a legitimate law enforcement inquiry; the request is specific and limited in scope; and de-identified information could not reasonably be used. Covered entities are also permitted to disclose protected health information in the course of judicial and administrative proceedings, and limited information for identification purposes. They are also permitted to disclose information to a law enforcement official about an individual who has died if there is reason to believe the death may have resulted form criminal conduct. A covered entity may disclose protected health information to authorized federal officials for the conduct of lawful intelligence, counter-intelligence, and other national security activities authorized by the National Security Act and implementing authority.[222]

Motor Vehicle Information

Driver's Privacy Protection Act of 1994

Regulates the use and disclosure of personal information from state motor vehicle records.[223] Personal information is defined as information that identifies an individual, including an individual's photograph, Social Security number, driver identification number, name, address, telephone number, and medical or

---

[220] 45 CFR § 164.512(f).

[221] Required by law means a mandate contained in law that compels a covered entity to make a use or disclosure or protected health information an that is enforceable in a court of law.

[222] 45 CFR § 164.512(k).

[223] 18 U.S.C. § 2721.

disability information, but does not include information on vehicular accidents, driving violations, and driver's status. Personal information contained in a motor vehicle record may be disclosed for use by any government agency, including any court or law enforcement agency, in carrying out its functions, or to any private person or entity acting on behalf of a Federal, State, or local agency; and for use in connection with any civil, criminal, administrative, or arbitral proceeding in any Federal, State, or local court or agency or before any self-regulatory body, or pursuant to a Federal, State, or local court order.

Communications and Communications Records

Title III of the Omnibus Crime Control and Safe Streets Act of 1968

The federal wiretapping and electronic eavesdropping statute permits federal and state law enforcement officers to use wiretapping and electronic eavesdropping under strict limitations.[224] 18 U.S.C. 2510 et seq. The federal and state courts may issue interception orders upon applications approved by senior Justice Department or state prosecutors. The applications must demonstrate probable cause to believe that the proposed interceptions will result in the capture of evidence of one or more of statutorily designated crimes. The orders are crafted to minimize the capture of innocent conversations. Officers may share information secured under the orders with other law enforcement or with intelligence officials in connection with the performance of their official duties. Senior Justice Department and state prosecutors may authorize emergency interceptions for 48 hours while an application for a court order is being prepared and presented. Unless postponed by the court for cause, the targets and anyone whose conversations have been captured are entitled to notification within 90 days of the expiration of the order. There are criminal, civil, and administrative sanctions for illegal interception, and evidence secured through an unlawful interception may be declared inadmissible in subsequent judicial or administrative proceedings. See table on "Laws Relating to Federal Government Access to Information Pursuant to the Fourth Amendment, the Federal Wiretap Statute, and the Foreign Intelligence Surveillance Act."

The Foreign Intelligence Surveillance Act of 1978

FISA governs the use of wiretapping to collect "foreign intelligence" which is defined as "information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities."[225] 50 U.S.C. §§ 1861 et seq. The eleven judges of a special court, whose members are assigned from the federal

[224] See CRS Report 98-326, Privacy: An Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping.

[225] See CRS Report RL30465, The Foreign Intelligence Surveillance Act: An Overview of the Statutory Framework.

bench, may authorize surveillance upon applications approved by the Attorney General asserting probable cause to belief that the effort will yield foreign intelligence. FISA court surveillance orders are crafted to minimize the capture of conversations not related to foreign intelligence. Officers may share the results with law enforcement officials for the performance of their duties. The Attorney General may authorize emergency surveillance for 72 hours while a FISA order is being secured. The President may authorize surveillance without a court order during time of war or for communications between or among foreign powers. If the government intends to use the results as evidence in judicial proceedings it must inform the parties to the intercepted conversations. Challenges to the legality of the surveillance may be considered ex parte upon petition of the Attorney General. Unlawful surveillance is subject to criminal, civil, and administrative sanctions, and evidence illegally secured may be suppressed.

FISA also empowered judges of the FISA court to issue physical search orders under limitations similar to FISA surveillance orders. In foreign intelligence cases, FISA likewise tracks the procedure used in criminal cases for the installation and use of pen register and trap and trace devices under court order. Finally, it called for FISA orders for the production of tangible items in foreign intelligence and international terrorism investigations. See table on "Laws Relating to Federal Government Access to Information Pursuant to the Fourth Amendment, the Federal Wiretap Statute, and the Foreign Intelligence Surveillance Act."

The Electronic Communications Privacy Act of 1986

ECPA amended and augmented Title III. It regulates government access to ongoing and stored wire and electronic communications (such as voice mail or electronic mail), transactional records access, and the use of pen registers, and trap and trace devices.[226] After its modifications the surreptitious capture of e-mails and other electronic communications in transit enjoy the coverage of Title III and may be accomplished under a Title III court order. When voice mail, e-mails and other electronic communications have been in storage for less than 180 days, they can be seized under a search warrant based on probable cause. Those in storage for 180 days or more can be secured under a court order upon a showing of relevancy and materiality, under a subpoena, or under a search warrant.

ECPA also authorized court orders for the installation and use of pen registers as well as trap and trace devices, which identify source and address of communications, but not the contents of the conversation. These orders may be issued on the basis of relevancy to a criminal investigation and their results need

[226] 18 U.S.C. §§ 2510 et seq. See CRS Report 98-326, Privacy: An Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping.

not be disclosed to the individuals whose communications are their targets. Perhaps because in the case of Internet communications header information is more revealing than the mere identification of source and addressee telephone numbers, results of such orders must be reported to the issuing court under seal.

Finally, ECPA established a procedure for government access to the customer records of telephone company or other communications service providers. Here too, access may be had by search warrant, subpoena, or court order (on a showing of relevancy). See "Laws Relating to Federal Government Access to Information Pursuant to the Fourth Amendment, the Federal Wiretap Statute, and the Foreign Intelligence Surveillance Act."

The USA PATRIOT Act of 2001

The Act substantively amended Title III of the Omnibus Crime Control and Safe Streets Act, the Electronic Communications Privacy Act, and the Foreign Intelligence Surveillance Act of 1978.[227] The USA PATRIOT Act authorized the disclosure of wiretap and grand jury information to "any federal, law enforcement, intelligence, protective, immigration, national defense, or national security official" for the performance of his duties.[228] It permitted use of FISA surveillance orders when foreign intelligence gathering is "a significant" reason for the order rather than "the" reason. It brought e-mail and other forms of electronic communications within the pen register and trap and trace procedures under both ECPA and FISA. Finally, it authorized FISA orders for access to any tangible item rather than only business records held by lodging, car rental, and locker rental businesses. See table on "Laws Relating to Federal Government Access to Information Pursuant to the Fourth Amendment, the Federal Wiretap Statute, and the Foreign Intelligence Surveillance Act."

The Homeland Security Act of 2002

The Act amended Title III of the Omnibus Crime Control and Safe Streets Act, the Electronic Communications Privacy Act, and the Foreign Intelligence Surveillance Act of 1978[229] to authorize sharing the results of the federal government's information gathering efforts under those statutes with relevant foreign, state and local officials. See table on "Laws Relating to Federal Government Access to Information Pursuant to the Fourth Amendment, the Federal Wiretap Statute, and the Foreign Intelligence Surveillance Act."

---

[227] P.L. 107-56. See CRS Report 98-326, Privacy: An Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping.

[228] P.L. 107-56, § 202.

[229] P.L. 107-296. See CRS Electronic Briefing Book, Terrorism – Wiretapping Authority.

Financial Information

This section provides a description of the Fair Credit Reporting Act, the Right to Financial Privacy Act, and the Gramm-Leach-Bliley Act. The table appended to this report on "Laws Relating to Federal Government Access to Personal Financial Information" also includes the Bank Secrecy Act of 1970, the U.S.A. Patriot Act provisions related to the Financial Crimes Enforcement Network (FinCEN), and relevant provisions of the Tax Reform Act of 1976.

The Fair Credit Reporting Act of 1970

FCRA sets forth rights for individuals and responsibilities for consumer "credit reporting agencies" in connection with the preparation and dissemination of personal information in a consumer report. Under the FCRA, consumer reporting agencies are prohibited from disclosing consumer reports to anyone who does not have a permissible purpose.[230] FCRA covers information gathered by consumer reporting agencies on consumers to evaluate qualifications for credit, employment, insurance, and other transactions; covered information may include identifying (name, address, employer and former address and employer), credit (transactions, etc.), and public record information as well as information on entities seeking credit reports on the consumer. A limited amount of identifying information from a credit bureau's file on a consumer (i.e., "header information" – name, address, employment and previous address) may be disclosed upon request. No notice is required. Consumer reports and any other information in a consumer's file can be disclosed pursuant to a court order or grand jury subpoena; or in connection with the application for a license or for determining eligibility for a government benefit or license. The FBI, for foreign counterintelligence investigative purposes, may obtain names and addresses of financial institutions at which consumers maintain or have maintained accounts, provided the request is signed by an appropriate official who has certified that the investigation is not conducted solely on the basis of activity protected under the First Amendment. The USA PATRIOT Act amended the FCRA to authorize the disclosure of consumer reports and any other information in a consumer's file upon request in writing from any government agency authorized to conduct international terrorism investigations, or intelligence or counterintelligence activities related thereto, stating that such information is necessary for the agency's conduct of that activity and signed by an appropriate supervisor. No notice is required. See table on "Laws Relating to Federal Government Access to Personal Financial Information."

The Right to Financial Privacy Act of 1978

---

[230] 15 U.S.C. § 1681 et seq. See CRS Report RL31666, Fair Credit Reporting Act: Rights and Responsibilities.

The RFPA was enacted in response to the 1976 decision of the Supreme Court in United States v. Miller,[231] which ruled that individuals have no Fourth Amendment "expectation of privacy" in records maintained by their banks. The RFPA sets forth procedures for the federal government's access to financial institution customer records.[232] RFPA covers the records of individuals who are customers of banks, thrifts, credit unions, credit card issuers, and consumer finance companies. The Act requires the government to present administrative subpoenas or summons based upon reason to believe the information is relevant to a legitimate law enforcement inquiry. In criminal investigations, judicial search warrants based on probable cause must be obtained. Notice to the customer is required except upon issuance of a court order finding the existence of certain exigent circumstances. However, these restrictions do not apply to foreign intelligence activities and investigations related to international terrorism.[233] See "Laws Relating to Federal Government Access to Personal Financial Information."

The Gramm-Leach-Bliley Act of 1999

Requires financial institutions to disclose their privacy policies to their customers.[234] Title V of the Act regulates nonpublically available personally identifiable customer (or applicant) information held by "financial institutions," a term that is broadly defined to include anyone in the business of providing services that are financial in nature, including banking, securities, insurance, accounting, tax preparation, asset management, real estate leasing and settlement services. GLBA provides exceptions for law enforcement to the law's general prohibition against "financial institution" sharing of personally identifiable customer information with non-affiliated third parties. Exceptions permit sharing of such information in response to judicial process; as permitted or required under other provisions of law, and in accordance with the Right to Financial Privacy Act; and to provide information to law enforcement agencies, or for an investigation on a matter of public safety. No notice of disclosure to the customer is necessary, except as required pursuant to other law. See table on "Laws Relating to Federal Government Access to Personal Financial Information."

---

[231] 425 U.S. 435 (1976).

[232] 12 U.S.C. § 3401 et seq. See CRS Report RS20185, Privacy Protection for Customer Financial Information.

[233] 12 U.S.C. § 3414.

[234] P.L. 106-202, 113 Stat. 1338. See CRS Report RS20185, Privacy Protection for Customer Financial Information.

Other Information

Children's Online Privacy Protection Act of 1998

Requires website operators and online service providers to obtain parental consent to collect a child's personal information, and requires sites collecting information from children to disclose how they plan to use the data.[235] Parental consent is not required for the operator of such a website or online service to collect, use, or disclose such information to respond to judicial process; or to provide information, to the extent permitted under other laws, to law enforcement agencies or for an investigation on a matter related to public safety.[236]

Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Domestic Security/Terrorism Investigations

Revised guidelines were issued by Attorney General Ashcroft in May 2002 which removed prohibitions on the Federal Bureau of Investigation's use of publicly-available sources of information – e.g., libraries or the Internet– except as part of an investigation. The 2002 guidelines authorize the FBI to engage in general topical research, which includes conducting online searches and accessing online sites and forums on the same terms and conditions as members of the public. This will allow the FBI to examine public records, monitor the Internet, survey periodicals and newspapers and commercial databases (like Google or Experian) – not incident to a criminal investigation.[237]

Miscellaneous Provisions

Numerous federal statutes include provisions that regulate the use and disclosure of certain types of information held by the government. For example, the confidentiality and disclosure of tax returns and return information is governed by section 6103 of the Internal Revenue Code,[238] the disclosure of Census data is governed, in part, by 13 U.S.C. § 9 which prohibits the use, publication, or examination of any information collected by the Census Bureau, other than for the statistical purpose for which the information was supplied; records pertaining to the issuance or refusal of visas to enter the United States are governed by 8

---

[235] 15 U.S.C. § 6501.

[236] Children's Online Privacy Protection Rule, 64 Fed. Reg. 59888 (Nov. 13, 1999) at [http://www.ftc.gov/os/1999/9910/64fr59888.pdf]. See CRS Report RL31408, Internet Privacy: Overview and Pending Legislation.

[237] Department of Justice, Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Domestic Security/Terrorism Investigations at VI(B). (May 2002). Available at [http://www.usdoj.gov/olp/generalcrimes2.pdf].

[238] 26 U.S.C. § 6103.

U.S.C. 1202(f); release of passport information in passport files is subject to the provisions of the Freedom of Information Act and the Privacy Act, and handled in accordance with the regulations in 22 CFR Part 171 and 172.

Legal Requirements for Warrants, Subpoenas, Court Orders, and Requests

Federal statutes that limit access to records held by third parties often specify the process that the federal government must use to gain access to these records. While the TIA program appears to envision real-time access, if not concurrent access, none of the means currently available to the government for accessing data appear to afford such an open-ended virtual appropriation of databases, either public or private. Leaving aside the question of whether there is sufficient authority for TIA's continuous monitoring of databases, what follows is a description of common tools available to the government to gain access to information.

Law enforcement officials who seek access to information in records held by third-party custodians have several procedural alternatives that include warrants, grand jury subpoenas, administrative subpoenas, court orders, written requests and oral requests. The complexity of the legal requirements for obtaining warrants, subpoenas, and court orders may be such that TIA would opt for other more expedient avenues of access.[239]

The term "**warrant**" ordinarily refers to a court document, issued by a judge or magistrate pursuant to the demands of the Fourth Amendment, upon the request of a law enforcement officer and without affording other parties an opportunity to object to the issuance or execution of the warrant. A search warrant authorizes a search for evidence in connection with a criminal investigation. Officers seeking a warrant must present sworn statements establishing probable cause to believe that the requested search will result in the discovery of evidence of a crime.[240] After the fact, a property owner is entitled to notice that a search has occurred and to an inventory of any property seized.[241] Notice is limited to those who have a reasonable expectation of privacy and under some circumstances this will not include records concerning an individual in a third party's computerized records

---

[239] John Markoff and John Schwartz, Bush Administration to Propose System for Wide Monitoring of Internet at A22, New York Times (Dec. 20, 2002).

[240] "Probable cause" means "a fair probability that contraband or evidence of a crime will be found in a particular place," Illinois v. Gates, 462 U.S. 213, 238 (1983).

[241] United States v. Ramirez, 523 U.S. 65 (1998).

whose claim to confidentiality has been weakened by making them available to others.[242]

Grand jury subpoena

In the context of its investigation of potential corruption or crime, usually at the request of the prosecuting attorney, the grand jury will issue a subpoena duces tecum – if documents are requested – requiring the record custodian's appearance with the requested documents or records. When subpoena duces tecum are served on record custodians, the government is usually under no obligation to bring the subpoena to the attention of the subject, but the custodian is usually free to do so.

Administrative subpoena

In the context of a civil investigation, an agency pursuant to its statutory authority and in accordance with its rules, may issue a request for information or production of documents, reasonably related to a matter within the jurisdiction of the agency. Generally the subpoena may be challenged in court based on lack of relevance, breadth, or lack of particularity. Often there is no requirement that the subject of the records be notified of the government's request.

Court orders

Generally, parties to litigation have the prerogative of seeking the assistance of the court, through the issuance of an order to produce documents or records or information, to facilitate the discovery process in litigation. In the context of government access to the kinds of information that might be desired for TIA programs two types pf specific court orders, the standards for which are outlined in statutes, are particularly relevant: (1) a court ordered electronic surveillance order under the federal wiretap statute, and (2) a surveillance order under the Foreign Intelligence Surveillance Act (FISA). The first may be issued by any federal court, provided the statutory procedures are complied with, including approval by senior federal officials. The second may only be issued by the FISA court. The suspicion threshold varies according to the situation. For example, the federal wiretap statute uses a "probable cause plus" standard,[243] while the court

[242] Cf., United States v. Miller, 425 U.S. 435 (1976)(no customer expectation of privacy in bank records).

[243] 18 U.S.C. 2518(3)(the order may be issued "if the judge determines on the basis of the facts submitted by the application that—(a) there is probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense enumerated in [18 U.S.C. 2516]; (b) there is probable cause for belief that particular communications concerning that offense will be obtained . . . (c) normal investigative procedures have been tried and have failed or reasonably appear to be unlike to succeed if tried or to be too dangerous; [and] (d) . . . there is probable cause for belief that the facilities from which, or the place where the . . . communications

order authorizing installation of a pen register and trap and trace device calls for a finding that the "investigative officer has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation."[244] The breadth of access varies from statute to statute as well. Often, the standard of suspicion required for issuance of the order coupled with the type of information sought will define the range of access. In some instances, however, Congress has imposed further limitations. Under the federal wiretap statute, for instance, the authority under the court order terminates as soon as the objectives for which the order was sought have been realized.[245] As noted above, "court order" statutes sometimes limit the manner in which officers may use or disclose such evidence. A few statutes expect court orders to be issued following an adversarial hearing;[246] in others the subject of the records receives notice only after the fact;[247] and in still others there are special provisions for extended postponement of notice under some circumstances.[248] The statute that creates the special court order procedure may indicate the grounds and procedure, if any, under which the subject of a record may seek to bar law enforcement access or use. Some may require prior notice.[249] Where the order is issued and access granted prior to notice, the subject may be limited to the exclusion of evidence or civil remedies to the extent that the application, order, execution of the order, or use of the information fail to meet the requirements of the statute.[250]

An **oral or written request** may procure access based on the consent of the third party information custodian. Issuance of such a request would depend upon

---

are to be intercepted are being used, or are about to be used, in connection with the commission of such offense . . .").

[244] 18 U.S.C. 3123(a); see also, 18 U.S.C. 2703(d)(e-mail records may be disclosed pursuant to a court order when the government "offers specific and articulable facts showing . . . reasonable grounds to believe that the . . . records . . . are relevant and material to an ongoing criminal investigation").

[245] 18 U.S.C. 2518(5).

[246] 42 U.S.C. 290dd-2; 42 C.F.R. §2.64 (disclosure of substance abuse treatment records).

[247] 18 U.S.C. 2518(9)(d)(notice of wiretapping under the federal wiretap statute must be given within 90 days of termination of the tap unless postponed by the court).

[248] 18 U.S.C. 2705 not only permits the court to delay notification of the subject whose e-mail records have been disclosed to the government but empowers the court to forbid the e-mail service provider from tipping off the subject.

[249] 42 C.F.R. §2.64 (substance abuse treatment records).

[250] E.g., the federal wiretap statute, 18 U.S.C. 2518(10)(suppression of evidence), 2520 (civil damages).

the rules and procedures governing the operations of the agent making the request.

Congressional Response

The 108th Congress is likely to reexamine existing federal law in terms of barriers to government access to information necessary to prevent and respond to acts of terrorism; while at the same time insuring that information is maintained in a manner that insures its most effective use, protects against its loss, against inappropriate use or disclosure; ensures public and Congressional scrutiny as a form of checks and balances; and otherwise guarantees individual privacy consistent with the Constitution.

According to Senator Shelby of the Senate Intelligence Committee, "[h]ow broadly it [TIA] will ultimately be used is a matter for policymakers to decide if and when the program bears fruit."[251] On January 13, 2003 Senator Harkin requested that the Defense Appropriations Subcommittee hold hearings on the Total Information Awareness (TIA) project. On January 16, 2003, Senator Russ Feingold introduced S. 188, the Data-mining Moratorium Act, which would limit the use of data mining technology by the Defense Department and by the new Department of Homeland Security without Congressional approval and appropriate civil liberties protections. On January 23, 2003 the Senate passed amendment S.Amdt. 59 (introduced by Senator Wyden) to H.J.Res. 2, the Omnibus Appropriations Act for Fiscal Year 2003, imposing limitations on implementation of Total Information Awareness programs, and requiring a detailed report to Congress. Both the House and Senate approved the FY03 omnibus spending bill, H.J.Res. 2, on February 13, 2003 (P.L. 108-7). It includes in section 111, with slight modifications, the language from S.Amdt 59 regarding the Department of Defense's Total Information Awareness (TIA) program. The bill allows the Administration, 90 days after the bill is enacted to submit a report to Congress on the TIA program, instead of 60 days as proposed by the Senate. The provision has also been modified to clarify that the TIA program may be deployed in the United States to assist in the conduct of lawful U.S. foreign intelligence activities against non-United States persons.

Section 111, Limitation on Use of Funds for Research and Development on Total Information Awareness Program, of H. J. Res. 2 imposes limitations on the use of funds for Total Information Awareness programs. It expresses the sense of Congress that the program should not be used to develop technologies for use in conducting intelligence activities or law enforcement activities against United States persons without appropriate consultation with Congress, or without clear adherence to principles to protect civil liberties and privacy. It reiterates the

---

[251] September 11 and the Imperative of Reform in the U.S. Intelligence Community: Additional Views of Senator Richard C. Shelby Vice Chairman, Senate Select Committee on Intelligence at 42 (December 10, 2002), [http://intelligence.senate.gov/shelby.pdf].

primary DOD focus of the Defense Advanced Research Projects Agency. The amendment provides that no funds appropriated or otherwise made available to the Department of Defense, Defense Advanced Research Projects Agency, or to any other department, agency, or element of the Federal Government may be obligated or expended on research and development on the Total Information Awareness program unless a written report, prepared by the Secretary of Defense, the Attorney General, and the Director of Central Intelligence, is submitted to Congress within 90 days after passage of the omnibus spending bill; or the President certifies to Congress in writing that submission of the report to Congress within 90 days is not practicable, and that the cessation of research and development on the Total Information Awareness program would endanger the national security of the United States.

The report to Congress must include a detailed explanation for each project and activity of the Total Information Awareness program – the actual and intended use of funds; the schedule for proposed research and development; and target dates for deployment. It must assess the likely efficacy of systems such as the Total Information Awareness program; the likely impact of the implementation of the Total Information Awareness program on privacy and civil liberties; and provide a list of the laws and regulations that govern the information to be collected by the Total Information Awareness program, and a description of any modifications required to use the information in the manner proposed. The report must include the Attorney General's recommendations for practices, procedures, regulations, or legislation on the deployment, implementation, or use of the Total Information Awareness program to eliminate or minimize adverse affects on privacy and civil liberties.

The amendment prohibits the deployment, implementation, or transfer of the TIA program or a component thereof to any department, agency, or element of the federal government until the Secretary of Defense notifies Congress; and receives from Congress specific authorization for the deployment and a specific appropriation of funds. This limitation does not apply with respect to the deployment or implementation of the Total Information Awareness program, or a component of such program, in support of the lawful military operations of the United States conducted outside the United States, and in support of lawful foreign intelligence activities conducted wholly against non-United States persons.

Another issue that has arisen is whether the Homeland Security Act of 2002 authorizes TIA programs in the newly created Department of Homeland Security (DHS). Although the Homeland Security Act does not expressly authorize Total Information Awareness programs, Congress authorized $500 million for a DHS entity with a name similar to DARPA, Homeland Security Advanced Research Projects Agency(HSARPA). The new law also includes languagethatauthorizes the

utilization of data mining and other advanced analytical tools by the new department.[252]

[252] P.L. 107-296 §201(d)(14), 116 Stat. 2135, 2147.

Data Mining and Homeland Security: An Overview, RL31798 (August 27, 2008).

JEFFREY W. SEIFERT, CONGRESSIONAL RESEARCH SERV., DATA MINING AND HOMELAND SECURITY: AN OVERVIEW (2008), *available at* http://www.intelligencelaw.com/library/secondary/crs/pdf/RL31798_8-27-2008.pdf.

Order Code RL31798
Updated August 27, 2008

Jeffrey W. Seifert
Specialist in Information Policy and Technology
Resources, Science, and Industry Division

Summary

Data mining has become one of the key features of many homeland security initiatives. Often used as a means for detecting fraud, assessing risk, and product retailing, data mining involves the use of data analysis tools to discover previously unknown, valid patterns and relationships in large data sets. In the context of homeland security, data mining can be a potential means to identify terrorist activities, such as money transfers and communications, and to identify and track individual terrorists themselves, such as through travel and immigration records.

While data mining represents a significant advance in the type of analytical tools currently available, there are limitations to its capability. One limitation is that although data mining can help reveal patterns and relationships, it does not tell the user the value or significance of these patterns. These types of determinations must be made by the user. A second limitation is that while data mining can identify connections between behaviors and/or variables, it does not necessarily identify a causal relationship. Successful data mining still requires skilled technical and analytical specialists who can structure the analysis and interpret the output.

Data mining is becoming increasingly common in both the private and public sectors. Industries such as banking, insurance, medicine, and retailing commonly use data mining to reduce costs, enhance research, and increase sales. In the public sector, data mining applications initially were used as a means to detect fraud and waste, but have grown to also be used for purposes such as measuring and improving program performance. However, some of the homeland security data mining applications represent a significant expansion in the quantity and scope of data to be analyzed. Some efforts that have attracted a higher level of congressional interest include the Terrorism Information Awareness (TIA) project (now-discontinued) and the Computer-Assisted Passenger Prescreening

System II (CAPPS II) project (nowcanceled and replaced by Secure Flight). Other initiatives that have been the subject of congressional interest include the Multi-State Anti-Terrorism Information Exchange (MATRIX), the Able Danger program, the Automated Targeting System (ATS), and data collection and analysis projects being conducted by the National Security Agency (NSA).

As with other aspects of data mining, while technological capabilities are important, there are other implementation and oversight issues that can influence the success of a project's outcome. One issue is data quality, which refers to the accuracy and completeness of the data being analyzed. A second issue is the interoperability of the data mining software and databases being used by different agencies. A third issue is mission creep, or the use of data for purposes other than for which the data were originally collected. A fourth issue is privacy. Questions that may be considered include the degree to which government agencies should use and mix commercial data with government data, whether data sources are being used for purposes other than those for which they were originally designed, and possible application of the Privacy Act to these initiatives. It is anticipated that congressional oversight of data mining projects will grow as data mining efforts continue to evolve. This report will be updated as events warrant.

What Is Data Mining?

Data mining involves the use of sophisticated data analysis tools to discover previously unknown, valid patterns and relationships in large data sets.[253] These tools can include statistical models, mathematical algorithms, and machine learning methods (algorithms that improve their performance automatically through experience, such as neural networks or decision trees). Consequently, data mining consists of more than collecting and managing data, it also includes analysis and prediction.

Data mining can be performed on data represented in quantitative, textual, or multimedia forms. Data mining applications can use a variety of parameters to examine the data. They include association (patterns where one event is connected to another event, such as purchasing a pen and purchasing paper), sequence or path analysis (patterns where one event leads to another event, such as the birth of a child and purchasing diapers), classification (identification of new patterns, such as coincidences between duct tape purchases and plastic sheeting purchases), clustering (finding and visually documenting groups of previously unknown facts, such as geographic location and brand preferences), and forecasting (discovering patterns from which one can make reasonable

[253] Two Crows Corporation, Introduction to Data Mining and Knowledge Discovery, Third Edition (Potomac, MD: Two Crows Corporation, 1999); Pieter Adriaans and Dolf Zantinge, Data Mining (New York: Addison Wesley, 1996).

predictions regarding future activities, such as the prediction that people who join an athletic club may take exercise classes).[254]

As an application, compared to other data analysis applications, such as structured queries (used in many commercial databases) or statistical analysis software, data mining represents a difference of kind rather than degree. Many simpler analytical tools utilize a verification-based approach, where the user develops a hypothesis and then tests the data to prove or disprove the hypothesis. For example, a user might hypothesize that a customer who buys a hammer, will also buy a box of nails. The effectiveness of this approach can be limited by the creativity of the user to develop various hypotheses, as well as the structure of the software being used. In contrast, data mining utilizes a discovery approach, in which algorithms can be used to examine several multidimensional data relationships simultaneously, identifying those that are unique or frequently represented. For example, a hardware store may compare their customers' tool purchases with home ownership, type of automobile driven, age, occupation, income, and/or distance between residence and the store. As a result of its complex capabilities, two precursors are important for a successful data mining exercise; a clear formulation of the problem to be solved, and access to the relevant data.[255]

Reflecting this conceptualization of data mining, some observers consider data mining to be just one step in a larger process known as knowledge discovery in databases (KDD). Other steps in the KDD process, in progressive order, include data cleaning, data integration, data selection, data transformation, (data mining), pattern evaluation, and knowledge presentation.[256]

A number of advances in technology and business processes have contributed to a growing interest in data mining in both the public and private sectors. Some of these changes include the growth of computer networks, which can be used to connect databases; the development of enhanced search-related techniques such as neural networks and advanced algorithms; the spread of the client/server computing model, allowing users to access centralized data resources from the

---

[254] For a more technically-oriented definition of data mining, see [http://searchcrm.techtarget.com/gDefinition/0,294236,sid11_gci211901,00.html].

[255] John Makulowich, "Government Data Mining Systems Defy Definition," Washington Technology, 22 February 1999, [http://www.washingtontechnology.com/news/13_22/tech_features/393-3.html].

[256] Jiawei Han and Micheline Kamber, Data Mining: Concepts and Techniques (New York: Morgan Kaufmann Publishers, 2001), p. 7.

desktop; and an increased ability to combine data from disparate sources into a single searchable source.[257]

In addition to these improved data management tools, the increased availability of information and the decreasing costs of storing it have also played a role. Over the past several years there has been a rapid increase in the volume of information collected and stored, with some observers suggesting that the quantity of the world's data approximately doubles every year.[258] At the same time, the costs of data storage have decreased significantly from dollars per megabyte to pennies per megabyte. Similarly, computing power has continued to double every 18-24 months, while the relative cost of computing power has continued to decrease.[259]

Data mining has become increasingly common in both the public and private sectors. Organizations use data mining as a tool to survey customer information, reduce fraud and waste, and assist in medical research. However, the proliferation of data mining has raised some implementation and oversight issues as well. These include concerns about the quality of the data being analyzed, the interoperability of the databases and software between agencies, and potential infringements on privacy. Also, there are some concerns that the limitations of data mining are being overlooked as agencies work to emphasize their homeland security initiatives.

Limitations of Data Mining as a Terrorist Detection Tool

While data mining products can be very powerful tools, they are not self-sufficient applications. To be successful, data mining requires skilled technical and analytical specialists who can structure the analysis and interpret the output that is created. Consequently, the limitations of data mining are primarily data or personnel-related, rather than technology-related.[260]

Although data mining can help reveal patterns and relationships, it does not tell the user the value or significance of these patterns. These types of determinations must be made by the user. Similarly, the validity of the patterns discovered is dependent on how they compare to "real world" circumstances. For example, to assess the validity of a data mining application designed to identify potential terrorist suspects in a large pool of individuals, the user may test the model using data that includes information about known terrorists. However, while possibly

---

[257] Pieter Adriaans and Dolf Zantinge, Data Mining (New York: Addison Wesley, 1996), pp. 5-6.

[258] Ibid., p. 2.

[259] Two Crows Corporation, Introduction to Data Mining and Knowledge Discovery, Third Edition (Potomac, MD: Two Crows Corporation, 1999), p. 4.

[260] Ibid., p. 2.

re-affirming a particular profile, it does not necessarily mean that the application will identify a suspect whose behavior significantly deviates from the original model.

Another limitation of data mining is that while it can identify connections between behaviors and/or variables, it does not necessarily identify a causal relationship. For example, an application may identify that a pattern of behavior, such as the propensity to purchase airline tickets just shortly before the flight is scheduled to depart, is related to characteristics such as income, level of education, and Internet use. However, that does not necessarily indicate that the ticket purchasing behavior is caused by one or more of these variables. In fact, the individual's behavior could be affected by some additional variable(s) such as occupation (the need to make trips on short notice), family status (a sick relative needing care), or a hobby (taking advantage of last minute discounts to visit new destinations).[261]

Beyond these specific limitations, some researchers suggest that the circumstances surrounding our knowledge of terrorism make data mining an ill-suited tool for identifying (predicting) potential terrorists before an activity occurs. Successful "predictive data mining" requires a significant number of known instances of a particular behavior in order to develop valid predictive models. For example, data mining used to predict types of consumer behavior (i.e., the likelihood of someone shopping at a particular store, the potential of a credit card usage being fraudulent) may be based on as many as millions of previous instances of the same particular behavior. Moreover, such a robust data set can still lead to false positives. In contrast, as a CATO Institute report suggests that the relatively small number of terrorist incidents or attempts each year are too few and individually unique "to enable the creation of valid predictive models."[262]

Data Mining Uses

Data mining is used for a variety of purposes in both the private and public sectors. Industries such as banking, insurance, medicine, and retailing commonly use data mining to reduce costs, enhance research, and increase sales. For example, the insurance and banking industries use data mining applications to detect fraud and assist in risk assessment (e.g., credit scoring). Using customer data collected over several years, companies can develop models that predict whether a customer is a good credit risk, or whether an accident claim may be fraudulent and should be investigated more closely. The medical community

---

[261] Ibid., p. 1.

[262] Jeff Jonas and Jim Harper, *Effective Counterterrorism and the Limited Role of Predictive Data Mining*, CATO Institute Policy Analysis No. 584, December 11, 2006 p. 8, [http://www.cato.org/pubs/pas/pa584.pdf].

sometimes uses data mining to help predict the effectiveness of a procedure or medicine. Pharmaceutical firms use data mining of chemical compounds and genetic material to help guide research on new treatments for diseases. Retailers can use information collected through affinity programs (e.g., shoppers' club cards, frequent flyer points, contests) to assess the effectiveness of product selection and placement decisions, coupon offers, and which products are often purchased together. Companies such as telephone service providers and music clubs can use data mining to create a "churn analysis," to assess which customers are likely to remain as subscribers and which ones are likely to switch to a competitor.[263]

In the public sector, data mining applications were initially used as a means to detect fraud and waste, but they have grown also to be used for purposes such as measuring and improving program performance. It has been reported that data mining has helped the federal government recover millions of dollars in fraudulent Medicare payments.[264] The Justice Department has been able to use data mining to assess crime patterns and adjust resource allotments accordingly. Similarly, the Department of Veterans Affairs has used data mining to help predict demographic changes in the constituency it serves so that it can better estimate its budgetary needs. Another example is the Federal Aviation Administration, which uses data mining to review plane crash data to recognize common defects and recommend precautionary measures.[265]

In addition, data mining has been increasingly cited as an important tool for homeland security efforts. Some observers suggest that data mining should be used as a means to identify terrorist activities, such as money transfers and communications, and to identify and track individual terrorists themselves, such as through travel and immigration records. Initiatives that have attracted significant attention include the now-discontinued Terrorism Information Awareness (TIA) project[266] conducted by the Defense Advanced Research

---

[263] Two Crows Corporation, Introduction to Data Mining and Knowledge Discovery, Third Edition (Potomac, MD: Two Crows Corporation, 1999), p. 5; Patrick Dillon, Data Mining: Transforming Business Data Into Competitive Advantage and Intellectual Capital (Atlanta GA: The Information Management Forum, 1998), pp. 5-6.

[264] George Cahlink, "Data Mining Taps the Trends," Government Executive Magazine, October 1, 2000, [http://www.govexec.com/tech/articles/1000managetech.htm].

[265] Ibid.; for a more detailed review of the purpose for data mining conducted by federal departments and agencies, see U.S. General Accounting Office, Data Mining: Federal Efforts Cover a Wide Range of Uses, GAO Report GAO-04-548 (Washington: May 2004).

[266] This project was originally identified as the Total Information Awareness project until DARPA publicly renamed it the Terrorism Information Awareness project in May 2003. Section 8131 of the FY2004 Department of Defense Appropriations Act (P.L. 108-87) prohibited further funding of TIA as a whole, while allowing unspecified subcomponents of the TIA initiative to be funded as

Projects Agency (DARPA), and the now-canceled Computer-Assisted Passenger Prescreening System II (CAPPS II) that was being developed by the Transportation Security Administration (TSA). CAPPS II is being replaced by a new program called Secure Flight. Other initiatives that have been the subject of congressional interest include the Able Danger program and data collection and analysis projects being conducted by the National Security Agency (NSA).

Terrorism Information Awareness (TIA) Program

In the immediate aftermath of the September 11, 2001, terrorist attacks, many questions were raised about the country's intelligence tools and capabilities, as well as the government's ability to detect other so-called "sleeper cells," if, indeed, they existed. One response to these concerns was the creation of the Information Awareness Office (IAO) at the Defense Advanced Research Projects Agency (DARPA)[267] in January 2002. The role of IAO was "in part to bring together, under the leadership of one technical office director, several existing DARPA programs focused on applying information technology to combat terrorist threats."[268] The mission statement for IAO suggested that the emphasis on these technology programs was to "counter asymmetric threats by achieving total information awareness useful for preemption, national security warning, and national security decision making."[269] To that end, the TIA project was to focus on three specific areas of research, anticipated to be conducted over five years, to devlop technologies that would assist in the detection of terrorist groups planning attacks against American interests, both inside and outside the country. The three areas of research and their purposes were described in a DOD Inspector General report as:

> *... language translation, data search with pattern recognition and privacy protection, and advanced collaborative and decision support tools. Language translation technology would enable the rapid analysis of foreign languages, both spoken and written, and allow analysts to quickly search the translated materials for clues about emerging threats. The data search, pattern recognition, and*

---

part of DOD's classified budget, subject to the provisions of the National Foreign Intelligence Program, which restricts the processing and analysis of information on U.S. citizens. For further details regarding this provision, see CRS Report RL31805, Authorization and Appropriations for FY2004: Defense, by Amy Belasco and Stephen Daggett.

[267] DARPA "is the central research and development organization for the Department of Defense (DOD)" that engages in basic and applied research, with a specific focus on "research and technology where risk and payoff are both very high and where success may provide dramatic advances for traditional military roles and missions." [http://www.darpa.mil/].

[268] Department of Defense. May 20, 2003. Report to Congress Regarding the Terrorism Information Awareness Program, Executive Summary, p. 2.

[269] Department of Defense. May 20, 2003. Report to Congress Regarding the Terrorism Information Awareness Program, Detailed Information, p. 1 (emphasis added).

> *privacy protection technologies would permit analysts to search vast quantities of data for patterns that suggest terrorist activity while at the same time controlling access to the data, enforcing laws and policies, and ensuring detection of misuse of the information obtained. The collaborative reasoning and decision support technologies would allow analysts from different agencies to share data.*[270]

Each part had the potential to improve the data mining capabilities of agencies that adopt the technology.[271] Automated rapid language translation could allow analysts to search and monitor foreign language documents and transmissions more quickly than currently possible. Improved search and pattern recognition technologies may enable more comprehensive and thorough mining of transactional data, such as passport and visa applications, car rentals, driver license renewals, criminal records, and airline ticket purchases. Improved collaboration and decision support tools might facilitate the search and coordination activities being conducted by different agencies and levels of government.[272]

In public statements DARPA frequently referred to the TIA program as a research and development project designed to create experimental prototype tools, and that the research agency would only use "data that is legally available and obtainable by the U.S. Government."[273] DARPA further emphasized that these tools could be adopted and used by other agencies, and that DARPA itself would not be engaging in any actual-use data mining applications, although it could "support production of a scalable leave-behind system prototype."[274] In addition, some of the technology projects being carried out in association with the TIA

---

[270] Department of Defense, Office of the Inspector General. December 12, 2003. Information Technology Management: Terrorism Information Awareness Project (D2004033). p. 7.

[271] It is important to note that while DARPA's mission is to conduct research and development on technologies that can be used to address national-level problems, it would not be responsible for the operation of TIA, if it were to be adopted.

[272] For more details about the Terrorism Information Awareness program and related information and privacy laws, see CRS Report RL31730, Privacy: Total Information Awareness Programs and Related Information Access, Collection, and Protection Laws, by Gina Marie Stevens, and CRS Report RL31786, Total Information Awareness Programs: Funding, Composition, and Oversight Issues, by Amy Belasco.

[273] Department of Defense, DARPA, "Defense Advanced Research Project Agency's Information Awareness Office and Total Information Awareness Project," p. 1, [http://www.iwar.org.uk/news-archive/tia/iaotia.pdf].

[274] Ibid., p. 2.

program did not involve data mining.[275] However, the TIA program's overall emphasis on collecting, tracking, and analyzing data trails left by individuals served to generate significant and vocal opposition soon after John Poindexter made a presentation on TIA at the DARPATech 2002 Conference in August 2002.[276]

Critics of the TIA program were further incensed by two administrative aspects of the project. The first involved the Director of IAO, Dr. John M. Poindexter. Poindexter, a retired Admiral, was, until that time, perhaps most well-known for his alleged role in the Iran-contra scandal during the Reagan Administration. His involvement with the program caused many in the civil liberties community to question the true motives behind TIA.[277] The second source of contention involved TIA's original logo, which depicted an "all-seeing" eye atop of a pyramid looking down over the globe, accompanied by the Latin phrase scientia est potentia (knowledge is power).[278] Although DARPA eventually removed the logo from its website, it left a lasting impression.

The continued negative publicity surrounding the TIA program contributed to the introduction of a number of bills in Congress that eventually led to the program's dissolution. Among these bills was S. 188, the Data-Mining Moratorium Act of 2003, which, if passed, would have imposed a moratorium on the implementation of data mining under the TIA program by the Department of Defense, as well as any similar program by the Department of Homeland Security. An amendment included in the Omnibus Appropriations Act for Fiscal Year 2003 (P.L. 108-7) required the Director of Central Intelligence, the Secretary of Defense, and the Attorney General to submit a joint report to Congress within 90 days providing details about the TIA program.[279] Funding for

---

[275] Although most of the TIA-related projects did involve some form of data collection, the primary purposes of some of these projects, such as war gaming, language translation, and biological agent detection, were less connected to data mining activities. For a description of these projects, see [http://www.fas.org/irp/agency/dod/poindexter.html].

[276] The text of Poindexter's presentation is available at [http://www.darpa.mil/DARPATech2002/presentations/iao_pdf/speeches/POINDEXT.pdf]. The slide presentation of Poindexter's presentation is available at [http://www.darpa.mil/DARPATech2002/presentations/iao_pdf/slides/PoindexterIAO.pdf].

[277] Shane Harris, "Counterterrorism Project Assailed By Lawmakers, Privacy Advocates," Government Executive Magazine, 25 November 2002, [http://www.govexec.com/dailyfed/1102/112502h1.htm].

[278] The original logo can be found at [http://www.thememoryhole.org/policestate/iaologo.htm].

[279] The report is available at [http://www.eff.org/Privacy/TIA/TIA-report.pdf]. Some of the information required includes spending schedules, likely effectiveness of the program, likely impact on privacy and civil liberties, and any laws and regulations that may need to be changed to fully deploy TIA. If the report was not submitted within 90 days, funding for the TIA program

TIA as a whole was prohibited with the passage of the FY2004 Department of Defense Appropriations Act (P.L. 108-87) in September 2003. However, Section 8131 of the law allowed unspecified subcomponents of the TIA initiative to be funded as part of DOD's classified budget, subject to the provisions of the National Foreign Intelligence Program, which restricts the processing and analysis of information on U.S. citizens.[280]

Computer-Assisted Passenger Prescreening System (CAPPS II)

Similar to TIA, the CAPPS II project represented a direct response to the September 11, 2001, terrorist attacks. With the images of airliners flying into buildings fresh in people's minds, air travel was now widely viewed not only as a critically vulnerable terrorist target, but also as a weapon for inflicting larger harm. The CAPPS II initiative was intended to replace the original CAPPS, currently being used. Spurred, in part, by the growing number of airplane bombings, the existing CAPPS (originally called CAPS) was developed through a grant provided by the Federal Aviation Administration (FAA) to Northwest Airlines, with a prototype system tested in 1996. In 1997, other major carriers also began work on screening systems, and, by 1998, most of the U.S.-based airlines had voluntarily implemented CAPS, with the remaining few working toward implementation.[281] Also, during this time, the White House Commission on Aviation Safety and Security (sometimes referred to as the Gore Commission) released its final report in February 1997.[282] Included in the commission's report was a recommendation that the United States implement automated passenger profiling for its airports.[283] On April 19, 1999, the FAA issued a notice of proposed rulemaking (NPRM) regarding the security of checked baggage on flights within the United States (docket no. FAA-1999-5536).[284] As part of this still-pending rule, domestic flights would be required to utilize "the FAA-approved computer-assisted passenger screening (CAPS) system to select

---

could have been discontinued. For more details regarding this amendment, see CRS Report RL31786, Total Information Awareness Programs: Funding, Composition, and Oversight Issues, by Amy Belasco.

[280] For further details regarding this provision, see CRS Report RL31805 Authorization and Appropriations for FY2004: Defense, by Amy Belasco and Stephen Daggett.

[281] Department of Transportation, White House Commission on Aviation and Security: The DOT Status Report, February 1998, [http://www.dot.gov/affairs/whcoasas.htm].

[282] The Gore Commission was established by Executive Order 13015 on August 22, 1996, following the crash of TWA flight 800 in July 1996.

[283] White House Commission on Aviation Safety and Security: Final Report to President Clinton. February 12, 1997. [http://www.fas.org/irp/threat/212fin~1.html].

[284] The docket can be found online at [http://www.regulations.gov/fdmspublic/component/main?main=DocketDetail&d=FAA-1999-5536].

passengers whose checked baggage must be subjected to additional security measures."[285]

The current CAPPS system is a rule-based system that uses the information provided by the passenger when purchasing the ticket to determine if the passenger fits into one of two categories; "selectees" requiring additional security screening, and those who do not. CAPPS also compares the passenger name to those on a list of known or suspected terrorists.[286] CAPPS II was described by TSA as "an enhanced system to confirm the identities of passengers and to identify foreign terrorists or persons with terrorist connections before they can board U.S. aircraft."[287] CAPPS II would have sent information provided by the passenger in the passengers name record (PNR), including full name, address, phone number, and date of birth, to commercial data providers for comparison to authenticate the identity of the passenger. The commercial data provider would have then transmitted a numerical score back to TSA indicating a particular risk level.[288] Passengers with a "green" score would have undergone "normal screening," while passengers with a "yellow" score would have undergone additional screening. Passengers with a "red" score would not have been allowed to board the flight, and would have received "the attention of law enforcement."[289] While drawing on information from commercial databases, TSA had stated that it would not see the actual information used to calculate the scores, and that it would not retain the traveler's information.

TSA had planned to test the system at selected airports during spring 2004.[290] However, CAPPS II encountered a number of obstacles to implementation. One obstacle involved obtaining the required data to test the system. Several high-profile debacles resulting in class-action lawsuits have made the U.S.-based airlines very wary of voluntarily providing passenger information. In early 2003,

---

[285] Federal Register, 64 (April 19,1999): 19220.

[286] U.S. General Accounting Office, Aviation Security: Computer-Assisted Passenger Prescreening System Faces Significant Implementation Challenges, GAO Report GAO-04385, February 2004, pp. 5-6.

[287] Transportation Security Administration, "TSA's CAPPS II Gives Equal Weight to Privacy, Security," Press Release, March 11, 2003, [http://www.tsa.gov/public/display ?theme=44&content=535].

[288] Robert O'Harrow, Jr., "Aviation ID System Stirs Doubt," Washington Post, 14 March 2003, p. A16.

[289] Transportation Security Administration, "TSA's CAPPS II Gives Equal Weight to Privacy, Security," Press Release, March 11, 2003, [http://www.tsa.gov/public/ display?theme=44&content=535].

[290] Sara Kehaulani Goo, "U.S. to Push Airlines for Passenger Records," Washington Post, January 12, 2004, p. A1.

Delta Airlines was to begin testing CAPPS II using its customers' passenger data at three airports across the country. However, Delta became the target of a vociferous boycott campaign, raising further concerns about CAPPS II generally.[291] In September 2003, it was revealed that JetBlue shared private passenger information in September 2002 with Torch Concepts, a defense contractor, which was testing a data mining application for the U.S. Army. The information shared reportedly included itineraries, names, addresses, and phone numbers for 1.5 million passengers.[292] In January 2004, it was reported that Northwest Airlines provided personal information on millions of its passengers to the National Aeronautics and Space Administration (NASA) from October to December 2001 for an airline security-related data mining experiment.[293] In April 2004, it was revealed that American Airlines agreed to provide private passenger data on 1.2 million of its customers to TSA in June 2002, although the information was sent instead to four companies competing to win a contract with TSA.[294] Further instances of data being provided for the purpose of testing CAPPS II were brought to light during a Senate Committee on Government Affairs confirmation hearing on June 23, 2004. In his answers to the committee, the acting director of TSA, David M. Stone, stated that during 2002 and 2003 four airlines; Delta, Continental, America West, and Frontier, and two travel reservation companies; Galileo International and Sabre Holdings, provided passenger records to TSA and/or its contractors.[295]

Concerns about privacy protections had also dissuaded the European Union (EU) from providing any data to TSA to test CAPPS II. However, in May 2004, the EU signed an agreement with the United States that would have allowed PNR data for flights originating from the EU to be used in testing CAPPS II, but only after TSA was authorized to use domestic data as well. As part of the agreement, the EU data was to be retained for only three-and-a-half years (unless it is part of a law enforcement action), only 34 of the 39 elements of the PNR were to be

---

[291] The Boycott Delta website is available at [http://www.boycottdelta.org].

[292] Don Phillips, "JetBlue Apologizes for Use of Passenger Records," The Washington Post, 20 September 2003, p. E1; Sara Kehaulani Goo, "TSA Helped JetBlue Share Data, Report Says," Washington Post, February 21, 2004, p. E1.

[293] Sara Kehaulani Goo, "Northwest Gave U.S. Data on Passengers," Washington Post, January 18, 2004, p. A1.

[294] Sara Kehaulani Goo, "American Airlines Revealed Passenger Data," Washington Post, April 10, 2004, p. D12.

[295] For the written responses to the committee's questions, see [http://www.epic.org/privacy/airtravel/stone_answers.pdf]; Sara Kehaulani Goo, "Agency Got More Airline Records,"Washington Post, June 24, 2004, p. A16.

accessed by authorities,[296] and there were to be yearly joint DHS-EU reviews of the implementation of the agreement.[297]

Another obstacle was the perception of mission creep. CAPPS II was originally intended to just screen for high-risk passengers who may pose a threat to safe air travel. However, in an August 1, 2003, Federal Register notice, TSA stated that CAPPS II could also be used to identify individuals with outstanding state or federal arrest warrants, as well as identify both foreign and domestic terrorists (not just foreign terrorists). The notice also states that CAPPS II could be "linked with the

U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) program" to identify individuals who are in the country illegally (e.g., individuals with expired visas, illegal aliens, etc.).[298] In response to critics who cited these possible uses as examples of mission creep, TSA claimed that the suggested uses were consistent with the goals of improving aviation security.[299]

Several other concerns had also been raised, including the length of time passenger information was to be retained, who would have access to the information, the accuracy of the commercial data being used to authenticate a passenger's identity, the creation of procedures to allow passengers the opportunity to correct data errors in their records, and the ability of the system to detect attempts by individuals to use identity theft to board a plane undetected.

Secure Flight

In August 2004, TSA announced that the CAPPS II program was being canceled and would be replaced with a new system called Secure Flight. In the Department of Homeland Security Appropriations Act, 2005 (P.L. 108-334), Congress included a provision (Sec. 522) prohibiting the use of appropriated funds for "deployment or implementation, on other than a test basis," of CAPPS II, Secure Flight, "or other follow on/successor programs," until GAO has certified that such

---

[296] Some information, such as meal preferences, which could be used to infer religious affiliation, and health considerations will not be made available. Goo, Sara Kehaulani, "U.S., EU Will Share Passenger Records," Washington Post, May 29, 2004, p. A2.

[297] Department of Homeland Security, "Fact Sheet: US-EU Passenger Name Record Agreement Signed," May 28, 2004, [http://www.dhs.gov/dhspublic/display?content=3651].

[298] Federal Register. Vol. 68 No. 148. August 1, 2003. p. 45266; U.S. General Accounting Office, Aviation Security: Challenges Delay Implementation of Computer-Assisted Passenger Prescreening System, GAO Testimony GAO-04-504T, March 17, 2004, p. 17.

[299] U.S. General Accounting Office, Aviation Security: Challenges Delay Implementation of Computer-Assisted Passenger Prescreening System, GAO Testimony GAO-04-504T, March 17, 2004, p. 17.

a system has met all of the privacy requirements enumerated in a February 2004 GAO report,[300] can accommodate any unique air transportation needs as it relates to interstate transportation, and that "appropriate life-cycle cost estimates, and expenditure and program plans exist." GAO's certification report[301] was delivered to Congress in March 2005. In its report, GAO found that while "TSA is making progress in addressing key areas of congressional interest ... TSA has not yet completed these efforts or fully addressed these areas, due largely to the current stage of the program's development."[302] In follow-up reports in February 2006[303] and June 2006,[304] GAO reiterated that while TSA continued to make progress, the Secure Flight program still suffered from systems development and program management problems, preventing it from meeting its congressionally mandated privacy requirements. In early 2006 TSA suspended development of Secure Flight in order to "rebaseline" or reassess the program.

In December 2006, the DHS Privacy Office released a report comparing TSA's published privacy notices with its actual practices regarding Secure Flight. The DHS Privacy Office found that there were discrepancies related to data testing and retention, due in part because the privacy notices "were drafted before the testing program had been designed fully." However, the report also points out that

> *material changes in a federal program's design that have an impact on the collection, use, and maintenance of personally identifiable information of American citizens are required to be*

---

[300] The eight issues included establishing an oversight board, ensuring the accuracy of the data used, conducting stress testing, instituting abuse prevention practices, preventing unauthorized access, establishing clear policies for the operation and use of the system, satisfying privacy concerns, and created a redress process. U.S. General Accounting Office, Aviation Security: Computer-Assisted Passenger Prescreening System Faces Significant Implementation Challenges, GAO Report GAO-04-385, February 2004.

[301] U.S. Government Accountability Office, Aviation Security: Secure Flight Development and Testing Under Way, but Risks Should Be Managed as System is Further Developed, GAO Report GAO-05-356, March 2005.

[302] Ibid., p. 4; for a more detailed analysis of the Secure Flight program, see CRS Report RL32802, Homeland Security: Air Passenger Screening and Counterterrorism, by Bart Elias and William Krouse.

[303] U.S. General Accountability Office, Aviation Security: Significant Management Challenges May Adversely Affect the Implementation of the Transportation Security Administration's Secure Flight Program, GAO Testimony GAO-06-374T.

[304] U.S. General Accountability Office, Aviation Security: Management Challenges Remain for the Transportation Security Administration's Secure Flight Program, GAO Testimony GAO-06-864T.

announced in Privacy Act system notices and privacy impact assessments.[305]

In a February 2007 interview, it was reported that TSA Administrator Kip Hawley stated that while TSA has developed a means to improve the accuracy, privacy, and reliability of Secure Flight, it would take approximately one-and-a-half years to complete. This would be followed by an additional year of testing, leading to an anticipated implementation in 2010.[306]

On August 23, 2007, TSA published a notice of proposed rulemaking (NPRM) for implementing Secure Flight, as well as an NPRM proposing Privacy Act exemptions for Secure Flight,[307] in the Federal Register. A Privacy Act System of Records Notice (SORN)[308] was also published in the same edition of the Federal Register. In addition, a Privacy Impact Assessment (PIA) for Secure Flight was posted on the TSA website.[309]

Along with the Secure Flight NPRM, on August 23, 2007, TSA published a related but separate final rule regarding the Advance Passenger Information System (APIS) administered by U.S. Customs and Border Protection (CBP) for screening passengers of international flights departing from or arriving to the United States.[310] TSA states

We propose that, when the Secure Flight rule becomes final, aircraft operators would submit passenger information to DHS through a single DHS portal for both the Secure Flight and APIS programs. This would allow DHS to integrate the watch list matching component of APIS into Secure Flight, resulting in one

---

[305] U.S. Department of Homeland Security, Privacy Office, Report to the Public on the Transportation Security Administration's Secure Flight Program and Privacy Recommendations, December 2006, p.13, [http://www.dhs.gov/xlibrary/assets/privacy/ privacy-secure-flight-122006.pdf].

[306] Eric Lipton, "U.S. Official Admits to Big Delay in Revamping No-Fly Program," New York Times, February 21, 2007, p. A17.

[307] Department of Homeland Security, Transportation Security Administration, "Privacy Act of 1974: Implementation of Exemptions; Secure Flight Records," 72 Federal Register 48397, August 23, 2007.

[308] Department of Homeland Security, Transportation Security Administration, "Privacy Act of 1974: System of Records; Secure Flight Records," 72 Federal Register 48392, August 23, 2007.

[309] See [http://www.tsa.gov/assets/pdf/pia_secureflight.pdf].

[310] Department of Homeland Security, Bureau of Customers and Border Protection, "Advance Electronic Transmission of Passenger and Crew Member Manifests for Commercial Aircraft and Vessels," 72 Federal Register 48320, August 23, 2007.

> *DHS system responsible for watch list matching for all aviation passengers.*[311]

According to the August 23, 2007 Secure Flight NPRM, in accordance with the Intelligence Reform and Terrorism Prevention Act (IRTPA), "TSA would receive passenger and certain non-traveler information, conduct watch list matching against the No Fly and Selectee portions of the Federal Government's consolidated terrorist watch list, and transmit boarding pass printing instructions back to aircraft operators."[312] Currently, air carriers are responsible for comparing passenger information to that on government watch lists.

The NPRM states that TSA would collect Secure Flight Passenger Data that includes a combination of required and optional information. Passengers would be required to provide their full names, "as it appears on a verifying identity document held by that individual."[313] In addition, passengers would be asked, but not required, to provide their date of birth, gender, Redress Number or known traveler number. However, the NPRM does propose circumstances in which aircraft operators would be required to provide the optional information to TSA if it already has obtained that information "in the ordinary course of business." The NPRM states

> *If a covered aircraft operator were to input data required to be requested from individuals into the system where it stores SFPD — such as data from a passenger profile stored by the aircraft operator in the ordinary course of business — the aircraft operator would be required to include that data as part of the SFPD transmitted to TSA, even though the individual did not provide that information at the time of reservation.*[314]

In addition, aircraft operations would be required to provide TSA, if available, a passenger's passport information, and "certain non-personally identifiable data fields" including itinerary information, reservation control number, record sequence number, record type, passenger update indicator, and traveler reference

---

[311] Department of Homeland Security, Transportation Security Administration, "Secure Flight Program," 72 Federal Register 48356, August 23, 2007.

[312] Department of Homeland Security, Transportation Security Administration, "Secure Flight Program," 72 Federal Register 48356, August 23, 2007.

[313] Ibid., p. 48369.

[314] Ibid., p. 48364.

number.[315] Secure Flight would not utilize commercial data to verify identities, nor would it use algorithms to assign risk scores to individuals.[316]

In the NPRM TSA proposes a tiered data retention schedule. The purpose for retaining the records would be to facilitate a redress process, expedite future travel, and investigate and document terrorist events. Under this schedule, the records for "individuals not identified as potential matches by the automated matching tool would be retained for seven days" after the completion of directional travel. The records for individuals identified as "potential matches" would be retained for seven years following the completion of directional travel. The records of individuals identified as "confirmed matches" would be retained for 99 years.[317]

This original NPRM included a 60-day comment period, ending on October 22, 2007. However, in response to deadline extension requests received, on October 24, 2007, TSA published a notice in the Federal Register extending the public comment period an additional 30 days, ending November 21, 2007.[318]

On November 9, 2007, TSA published a final SORN[319] and a final rule regarding Privacy Act exemptions for Secure Flight.[320]

Multistate Anti-Terrorism Information Exchange (MATRIX) Pilot Project

Similar to TIA and CAPPS II, which were born out of an initial reaction to concerns about terrorism, the impetus and initial work on MATRIX grew out of the September 11, 2001 terrorist attacks. MATRIX was initially developed by Seisint, a Florida-based information products company, in an effort to facilitate collaborative information sharing and factual data analysis. At the outset of the project, MATRIX included a component Seisint called the High Terrorist Factor (HTF). Within days of the terrorist attacks, based on an analysis of information

---

[315] Ibid., p. 48359.

[316] Ibid., p. 48363.

[317] Ibid., p. 48356.

[318] Department of Homeland Security, Transportation Security Administration, "Secure Flight Program," 72 Federal Register 60307, October 24, 2007.

[319] Department of Homeland Security, Transportation Security Administration, "Privacy Act of 1974: System of Records; Secure Flight Records," 72 Federal Register 63711, November 9, 2007.

[320] Department of Homeland Security, Transportation Security Administration, "Privacy Act of 1974: Implementation of Exemptions; Secure Flight Records," 72 Federal Register 63706, November 9, 2007.

that included "age and gender, what they did with their drivers license, either pilots or associations to pilots, proximity to 'dirty' addresses/phone numbers, investigational data, how they shipped; how they received, social security number anomalies, credit history, and ethnicity," Seisint generated a list of 120,000 names with high HTF scores, or so called terrorism quotients. Seisint provided this list to the Federal Bureau of Investigation (FBI), the Immigration and Naturalization Service (INS), the United States Secret Service (USSS), and the Florida Department of Law Enforcement (FDLE), which, according to a January 2003 presentation, made by the company, led to "several arrests within one week" and "scores of other arrests."[321] Although the HTF scoring system appeared to attract the interest of officials, this feature was reportedly dropped from MATRIX because it relied on intelligence data not normally available to the law enforcement community and concerns about privacy abuses. However, some critics of MATRIX continued to raise questions about HTF, citing the lack of any publicly available official documentation verifying such a decision.[322]

As a pilot project, MATRIX was administered through a collaborative effort between Seisint, the FDLE,[323] and the Institute for Intergovernmental Research (IIR), a "Florida-based nonprofit research and training organization, [that] specializes in law enforcement, juvenile justice, and criminal justice issues."[324] The Florida Department of Law Enforcement (FDLE) served as the "Security Agent" for MATRIX, administering control over which agencies and individuals had access to the system. FDLE was also a participant state in MATRIX. IIR was responsible for administrative support, and was the grantee for federal funds received for MATRIX.[325]

The analytical core of the MATRIX pilot project was an application called Factual Analysis Criminal Threat Solution (FACTS). FACTS was described as a "technological, investigative tool allowing query-based searches of available state and public records in the data reference repository."[326] The FACTS application allowed an authorized user to search "dynamically combined records from

---

[321] A copy of the presentation is available at [http://www.aclu.org/Files/OpenFile.cfm?id= 15813].

[322] Brian Bergstein, "Database Firm Tagged 120,000 Terrorism 'Suspects' for Feds," The SunHerald, May 20, 2004, [http://www.sunherald.com/mld/sunherald/business/technology/8715327.htm].

[323] The FDLE website is available at [http://www.fdle.state.fl.us/].

[324] The IIR website is available at [http://www.iir.com/].

[325] The MATRIX project website was deactivated at the conclusion of the pilot period. It was previously available at [http://www.matrix-at.org/].

[326] Information originally drawn from the MATRIX website, which is no longer available, at [http://www.matrix-at.org/FACTS_defined.htm].

disparate datasets" based on partial information, and will "assemble" the results.[327] The data reference repository used with FACTS represented the amalgamation of over 3.9 billion public records collected from thousands of sources.[328] Some of the data contained in FACTS included FAA pilot licenses and aircraft ownership records, property ownership records, information on vessels registered with the Coast Guard, state sexual offenders lists, federal terrorist watch lists, corporation filings, Uniform Commercial Code filings, bankruptcy filings, state-issued professional licenses, criminal history information, department of corrections information and photo images, driver's license information and photo images, motor vehicle registration information, and information from commercial sources that "are generally available to the public or legally permissible under federal law."[329] The data reference repository purportedly excluded data such as telemarketing call lists, direct mail mailing lists, airline reservations or travel records, frequent flyer/hotel stay program membership or activity, magazine subscriptions, information about purchases made at retailers or over the Internet, telephone calling logs or records, credit or debit card numbers, mortgage or car payment information, bank account numbers or balance information, birth certificates, marriage licenses, divorce decrees, or utility bill payment information.

Participating law enforcement agencies utilized this information sharing and data mining resource over the Regional Information Sharing Systems (RISS) secure intranet (RISSNET). The RISS Program is an established system of six regional centers that are used to "share intelligence and coordinate efforts against criminal networks that operate in many locations across jurisdictional lines."[330] The RISS Program is used to combat traditional law enforcement targets, such as drug trafficking and violent crime, as well as other activities, such as terrorism and cybercrime. According to its website, RISS has been in operation for nearly 25 years, and has "member agencies in all 50 states, the District of Columbia, U.S. territories, Australia, Canada, and England."[331]

---

[327] Ibid.

[328] Information originally drawn from the MATRIX website, which is no longer available, at [http://www.matrix-at.org/newsletter.pdf].

[329] Information originally drawn from the MATRIX website, which is no longer available, at [http://www.matrix-at.org/data_sources.htm].

[330] For a detailed description of RISS, see [http://www.iir.com/riss/] and [http://www.rissinfo.com/].

[331] [http://www.rissinfo.com/overview2.htm].

Some critics of MATRIX suggested that the original intentions and design of the pilot project echoed those of DARPA's highly criticized TIA program.[332] However, while it is difficult to ascribe intention, an ongoing series of problems did appear to have affected the trajectory of the project. In August 2003, Hank Asher, the founder of Seisint, resigned from the company's board of directors after questions about his criminal history were raised during contract negotiations between Seisint and the Florida Department of Law Enforcement. In the 1980s, Asher was allegedly a pilot in several drug smuggling cases. However, he was reportedly never charged in the cases in exchange for his testimony at state and federal trials. Similar concerns had surfaced in 1999 when the FBI and the U.S. Drug Enforcement Agency (DEA) reportedly cancelled contracts with an earlier company Asher founded, DBT Online, Inc.[333]

Some civil liberties organizations also raised concerns about law enforcement actions being taken based on algorithms and analytical criteria developed by a private corporation, in this case Seisint, without any public or legislative input.[334] Questions also were raised about the level of involvement of the federal government, particularly the Department of Homeland Security and the Department of Justice, in a project that is ostensibly focused on supporting state-based information sharing.[335] It has been reported that the MATRIX pilot project has received a total of $12 million in federal funding — $8 million from the Office of Domestic Preparedness (ODP) at the Department of Homeland Security (DHS), and $4 million from the Bureau of Justice Assistance (BJA) at the Department of Justice (DOJ).[336]

The MATRIX pilot project also suffered some setbacks in recruiting states to participate. The lack of participation can be especially troubling for a networked information sharing project such as MATRIX because, as Metcalfe's Law

---

[332] John Schwartz, "Privacy Fears Erode Support for a Network to Fight Crime," New York Times, 15 March 2004, [http://www.nytimes.com/2004/03/15/technology/15matrix.html].

[333] Cynthia L. Webb, "Total Information Dilemma," Washington Post, May 27, 2004, [http://www.washingtonpost.com/ac2/wp-dyn/A60986-2004May27?language=printer]; Lucy Morgan, "Ex-drug Runner Steps Aside," St. Petersburg Times, August 30, 2003, [http://www.sptimes.com/2003/08/30/State/Ex_drug_runner_steps_.shtml]; Bill Cotterell, and Nancy Cook Lauer, "Bush Defends Pick of Computer Firm, Former Leader's Background Raises Questions," Tallahassee Democrat, May 22, 2004, [http://www.tallahassee.com/mld/tallahassee/news/local/8728776.htm].

[334] Welsh, William Welsh, "Feds Offer to Mend Matrix," Washington Technology, May 24, 2004, [http://www.washingtontechnology.com/news/19_4/egov/23597-1.html].

[335] O'Harrow, Jr., Robert O'Harrow, Jr., "Anti-Terror Database Got Show at White House," Washington Post, May 21, 2004, p. A12.

[336] John Schwartz, "Privacy Fears Erode Support for a Network to Fight Crime," New York Times, March 15, 2004, [http://www.nytimes.com/2004/03/15/technology/15matrix.html].

suggests, "the power of the network increases exponentially by the number of computers connected to it."[337] While as many as 16 states were reported to have either participated or seriously considered participating in MATRIX, several chose to withdraw, leaving a total of four states (Connecticut, Florida, Ohio, and Pennsylvania) at the conclusion of the pilot on April 15, 2005. State officials cited a variety of reasons for not participating in MATRIX, including costs, concerns about violating state privacy laws, and duplication of existing resources.[338]

In its news release announcing the conclusion of the pilot, the FDLE stated that as a proof-of-concept pilot study from July 2003 to April 2005, MATRIX had achieved many "operational successes." Among the statistics cited, the news release stated that

- Between July 2003 and April 2005, there have been 1,866,202 queries to the FACTS application.
- As of April 8, 2005, there were 963 law enforcement users accessing FACTS.
- FACTS assisted a variety of investigations. On average, cases pertained to the following:
    - Fraud — 22.6%
    - Robbery — 18.8%
    - Sex Crime Investigations — 8.6%
    - Larceny and Theft — 8.3%
    - Extortion/Blackmail — 7.0%
    - Burglary/Breaking and Entering — 6.8%
    - Stolen Property — 6.2%
    - Terrorism/National Security — 2.6%
    - Other — 19.1% (e.g., assault, arson, narcotics, homicide)

It was also announced that while the pilot study would not be continued, due to a lack of additional federal funding, that Florida and other participating states were

---

[337] For a more detailed discussion of Metcalfe's Law, see [http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci214115,00.html].

[338] The states that have reportedly decided to withdraw from the pilot project include Alabama, California, Georgia, Kentucky, Louisiana, New York, Oregon, South Carolina, Texas, Utah, and Wisconsin. Larry Greenemeier, "Two More States Withdraw From Database," InformationWeek, March 12, 2004, [http://www.informationweek.com/story/showArticle.jhtml?articleID=18312112]; Diane Frank, "Utah No Longer Part of MATRIX," Federal Computer Week, April 5, 2004, p. 14; Associated Press, "Two More States Withdraw From Controversial Database Program," Star-Telegram, March 12, 2004, [http://www.dfw.com/mld/dfw/business/8170978.htm?1c]; Associated Press, "Matrix Plan Fuels Privacy Fears," Wired News, February 2, 2004, [http://www.wired.com/news/business/0,1367,62141,00.html].

"independently negotiating the continued use of the FACTS application for use within their individual state[s]."[339]

Other Data Mining Initiatives

Able Danger

In summer 2005, news reports began to appear regarding a data mining initiative that had been carried out by the U.S. Army's Land Information Warfare Agency (LIWA) in 1999-2000. The initiative, referred to as Able Danger, had reportedly been requested by the U.S. Special Operations Command (SOCOM) as part of larger effort to develop a plan to combat transnational terrorism. Because the details of Able Danger remain classified, little is known about the program. However, in a briefing to reporters, the Department of Defense characterized Able Danger as a demonstration project to test analytical methods and technology on very large amounts of data.[340] The project involved using link analysis to identify underlying connections and associations between individuals who otherwise appear to have no outward connection with one another. The link analysis used both classified and open source data, totaling a reported 2.5 terabytes.[341] All of this data, which included information on U.S. persons, was reportedly deleted in April 2000 due to U.S. Army regulations requiring information on U.S. persons be destroyed after a project ends or becomes inactive.[342]

Interest in Able Danger was largely driven by controversy over allegations that the data mining analysis had resulted in the identification of Mohammed Atta, one of the 9/11 hijackers, as a terrorist suspect before the attacks took place. While some individuals who had been involved in Able Danger were reportedly prepared to testify that they had seen either his name and/or picture on a chart prior to the attacks, the identification claim was strongly disputed by others.

On September 21, 2005, the Senate Committee on the Judiciary held a hearing on Able Danger to consider how the data could or should have been shared with other agencies, and whether the destruction of the data was in fact required by

---

[339] Florida Department of Law Enforcement (FDLE). "News Release: MATRIX Pilot Project Concludes," April 15, 2005, [http://www.fdle.state.fl.us/press_releases/expired/2005/20050415_matrix_project.html].

[340] Department of Defense, Special Defense Department Briefing, September 1, 2005, [http://www.defenselink.mil/transcripts/2005/tr20050901-3844.html].

[341] Shane Harris, "Homeland Security - Intelligence Designs," National Journal, December 3, 2005, [http://www.govexec.com/dailyfed/1205/120705nj1.htm].

[342] Erik Kleinsmith, Testimony before the Senate Committee on the Judiciary, Able Danger and Intelligence Information Sharing, September 21, 2005, [http://judiciary.senate.gov/ testimony.cfm?id=1606&wit_id=4669].

the relevant regulations. While the Department of Defense directed the individuals involved in Able Danger not to testify at the hearing, testimony was taken from the attorney of one of the individuals, as well as others not directly involved with the project.

On February 15, 2006, the House Committee on Armed Services Subcommittee on Strategic Forces and Subcommittee on Terrorism, Unconventional Threats and Capabilities held a joint hearing on Able Danger. The first half of the hearing was held in open session while the second half of the hearing was held in closed session to allow for the discussion of classified information. Witnesses testifying during the open session included Stephen Cambone, Undersecretary of Defense for Intelligence; Erik Kleinsmith; Anthony Shaffer, and J.D. Smith.

In September 2006, a Department of Defense Inspector General report regarding Able Danger was released. The investigation examined allegations of mismanagement of the Able Danger program and reprisals against Lieutenant Colonel (LTC) Anthony Shaffer, a member of the U.S. Army Reserve and civilian employee of the Defense Intelligence Agency (DIA). The DoD Inspector General "found some procedural oversights concerning the DIA handling of LTC Shaffer's office contents and his Officer Evaluation Reports." However, the investigation found that

> *The evidence did not support assertions that Able Danger identified the September 11, 2001, terrorists nearly a year before the attack, that Able Danger team members were prohibited from sharing information with law enforcement authorities, or that DoD officials reprised against LTC Shaffer for his disclosures regarding Able Danger.* [343]

In December 2006, the then-Chairman and then-Vice Chairman of the Senate Select Committee on Intelligence, Senator Roberts and Senator Rockefeller respectively, released a letter summarizing the findings of a review of Able Danger conducted by Committee staff.[344] According to the letter, the results of the review, begun in August 2005, "were confirmed in all respects by the DoD Inspector General investigation of the Able Danger program (Case Number H05L9790521)." The letter further stated that the review "revealed no evidence to support the underlying Able Danger allegations" and that the Committee considered the matter "closed."

---

[343] Department of Defense, Office of the Inspector General, "Alleged Misconduct by Senior DoD Officials Concerning the Able Danger Program and Lieutenant Colonel Anthony A. Shaffer, U.S. Army Reserve," Report of Investigation, September 18, 2006, [http://www.dodig.mil/fo/foia/ERR/r_H05L97905217-PWH.pdf].

[344] A copy of the letter is available at [http://www.intelligence.senate.gov/abledanger.pdf].

Automated Targeting System (ATS)

On November 2, 2006, DHS posted a System of Records Notice (SORN) in the Federal Register regarding the deployment of the Automated Targeting System (ATS), to screen travelers entering the United States by car, plane, ship, or rail.[345] Originally developed to help identify potential cargo threats, ATS is a module of the Treasury Enforcement Communications System (TECS). TECS is described as an "overarching law enforcement information collection, targeting, and sharing environment." ATS is run by the Bureau of Customs and Border Protection (CPB). The Federal Register notice states that "ATS builds a risk assessment for cargo, conveyances, and travelers based on criteria and rules developed by CPB." The notice further states that "ATS both collects information directly, and derives other information from various systems." Information collected may be retained for up to forty years "to cover the potentially active lifespan of individuals associated with terrorism or other criminal activities."

According to a November 22, 2006 privacy impact assessment, ATS itself is composed of six modules:

- ATS-Inbound — inbound cargo and conveyances (rail, truck, ship, and air)
- ATS-Outbound — outbound cargo and conveyances (rail, truck, ship, and air)
- ATS-Passenger (ATS-P) — travelers and conveyances (air, ship, and rail)
- ATS-Land (ATS-L) — private vehicles arriving by land
- ATS-International (ATS-I) — cargo targeting for CPB's collaboration with foreign customs authorities
- ATS-Trend Analysis and Analytical Selectivity Program (ATS-TAP) (analytical module)[346]

According to DHS, "ATS historically was covered by the SORN for TECS." The November 2, 2006 SORN was "solely to provide increased noticed and transparency to the public about ATS" and "did not describe any new collection of information."[347] However, the disclosure raised a number of issues about various facets of the program, including proposed exemptions from the Privacy Act; opportunities for citizens to correct errors in the records; how the risk assessments are created; if any previous testing has been conducted; and the effectiveness of the system.

---

[345] Department of Homeland Security, Office of the Secretary, "Privacy Act of 1974; System of Records," 71 Federal Register 64543, November 2, 2006.

[346] Department of Homeland Security, Privacy Impact Assessment for the Automated Targeting System, November 22, 2006, p.3, [http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_ats.pdf].

[347] Department of Homeland Security, Office of the Secretary, "Privacy Act of 1974; U.S. Customs and Border Protection, Automated Targeting System, System of Records," 72 Federal Register 43650, August 6, 2007.

In its July 6, 2007 report to Congress, the DHS Privacy Office stated that of the six modules that compose ATS, only two — ATS Inbound and ATS Outbound (which became operational in 1997) — "engage in data mining to provide decision support analysis for targeting of cargo for suspicious activity."[348] In contrast, the DHS Privacy Office report states that the ATS Passenger module does not meet the definition of data mining referred to in H.Rept. 109-699 (this definition is discussed in more detail in "Legislation in the 109th Congress," below). Whereas the ATS Passenger module calls for a search or examination of a traveler based on the traveler's personally identifying travel documents, the data mining definition in H.Rept. 109-699 only includes a search that "does not use a specific individual's personal identifiers to acquire information concerning that individual."[349]

On August 6, 2007, the Privacy Office of the Department of Homeland Security published a notice of proposed rulemaking (NPRM) proposing Privacy Act exemptions for the Automated Targeting System,[350] in the Federal Register. A Privacy Act System of Records Notice (SORN)[351] was also published in the same edition of the Federal Register. In addition, a revised Privacy Impact Assessment (PIA) for ATS was posted on the DHS website.[352]

According to the NPRM, ATS-P module records exempt from the Privacy Act would include "the risk assessment analyses and business confidential information received in the PNR from the air and vessel carriers." Records or information obtained from other systems of records that are exempt from certain provisions of the Privacy Act would retain their exemption in ATS.[353] In the NPRM, DHS states that the exemptions are needed "to protect information relating to law enforcement investigations from disclosures to subjects of

---

[348] Department of Homeland Security, Privacy Office, 2007 Data Mining Report: DHS Privacy Office Response to House Report 109-699, July 6, 2007, [http://www.dhs.gov/xlibrary/assets/privacy/privacy_rpt_datamining_2007.pdf], p. 17.

[349] Ibid., p. 7 and p. 17, footnote 34.

[350] Department of Homeland Security, Office of the Secretary, "Privacy Act of 1974: Implementation of Exemptions; Automated Targeting System," 72 Federal Register 43567, August 6, 2007.

[351] Department of Homeland Security, Office of the Secretary, "Privacy Act of 1974; U.S. Customs and Border Protection, Automated Targeting System, System of Records," 72 Federal Register 43650, August 6, 2007.

[352] See [http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_atsupdate.pdf].

[353] Department of Homeland Security, Office of the Secretary, "Privacy Act of 1974: Implementation of Exemptions; Automated Targeting System," 72 Federal Register 43567, August 6, 2007.

investigations and others who could interfere with investigatory and law enforcement activities."

The August 6, 2007 SORN is a revised version of the November 2, 2006 SORN "which responds to those comments [received in response to the November 2006 SORN], makes certain amendments with regard to the retention period and access provisions of the prior notice, and provides further notice and transparency to the public about the functionality of ATS."[354] The changes include

- Reducing the "general retention period for data maintained in ATS" from 40 to 15 years, and adding a requirement that users obtain supervisory approval to access archived data in the last eight years of the retention period.
- Allowing "persons whose PNR data has been collected and maintained in ATS-P [to] have administrative access to that data under the Privacy Act." Individuals will also be able to "seek to correct factual inaccuracies contained in their PNR data, as it is maintained by CBP."
- Adding booking agents as a category of people from whom information is obtained, in acknowledgment that booking agents' identities are included in itinerary information.
- Amending the categories of people covered by ATS "to include persons whose international itineraries cause their flight to stop in the United States, either to refuel or permit a transfer, and crewmembers on flights that overfly or transit through U.S. airspace."
- Clarifying "the categories of PNR data collected and maintained in ATS-P to more accurately reflect the type of data collected from air carriers."
- Removing "two of the routine uses included in the earlier version of the SORN — those pertaining to using ATS in background checks."

This revised SORN became effective on September 5, 2007.

National Security Agency (NSA) and the Terrorist Surveillance Program

In December 2005 news reports appeared for the first time revealing the existence of a classified NSA terrorist surveillance program, dating back to at least 2002, involving the domestic collection, analysis, and sharing of telephone call information.[355] Controversy over the program raised congressional concerns about both the prevalence of homeland security data mining and the capacity of

---

[354] Department of Homeland Security, Office of the Secretary, "Privacy Act of 1974; U.S. Customs and Border Protection, Automated Targeting System, System of Records," 72 Federal Register 43650, August 6, 2007.

[355] Peter Baker, "President Says He Ordered NSA Domestic Spying," The Washington Post, 18 December 2005, p. A1; Walter Pincus, "NSA Gave Other U.S. Agencies Information From Surveillance," The Washington Post, January 1, 2006, p. A8.

the country's intelligence and law enforcement agencies to adequately analyze and share counterterrorism information. The Senate Committee on the Judiciary held two hearings regarding the issue on February 6 and February 28, 2006.

Although details about the program are classified, statements by President Bush and Administration officials following the initial revelation of the program suggested that the NSA terrorist surveillance program focused only on international calls, with a specific goal of targeting the communications of al Qaeda and related terrorist groups, and affiliated individuals. It was also suggested that the program was reviewed and reauthorized on a regular basis and that key Members of Congress had been briefed about the program.

In his weekly radio address on December 17, 2005, President Bush stated:

> *In the weeks following the terrorist attacks on our nation, I authorized the National Security Agency, consistent with U.S. law and the Constitution, to intercept the international communications of people with known links to al Qaeda and related terrorist organizations. Before we intercept these communications, the government must have information that establishes a clear link to these terrorist networks.*[356]

President Bush also stated during his radio address:

> *The activities I authorized are reviewed approximately every 45 days. Each review is based on a fresh intelligence assessment of terrorist threats to the continuity of our government and the threat of catastrophic damage to our homeland. During each assessment, previous activities under the authorization are reviewed. The review includes approval by our nation's top legal officials, including the Attorney General and the Counsel to the President. I have reauthorized this program more than 30 times since the September the 11th attacks, and I intend to do so for as long as our nation faces a continuing threat from al Qaeda and related groups.*[357]

In a January 27, 2006, public release statement, the Department of Justice stated:

---

[356] President George W. Bush, "President's Radio Address," December 17, 2005, [http://www.whitehouse.gov/news/releases/2005/12/20051217.html].

[357] Ibid.

The NSA program is narrowly focused, aimed only at international calls and targeted at al Qaeda and related groups. Safeguards are in place to protect the civil liberties of ordinary Americans.

- The program only applies to communications where one party is located outside of the United States.
- The NSA terrorist surveillance program described by the President is only focused on members of Al Qaeda and affiliated groups. Communications are only intercepted if there is a reasonable basis to believe that one party to the communication is a member of al Qaeda, affiliated with al Qaeda, or a member of an organization affiliated with al Qaeda.
- The program is designed to target a key tactic of al Qaeda: infiltrating foreign agents into the United States and controlling their movements through electronic communications, just as it did leading up to the September 11 attacks.
- The NSA activities are reviewed and reauthorized approximately every 45 days. In addition, the General Counsel and Inspector General of the NSA monitor the program to ensure that it is operating properly and that civil liberties are protected, and the intelligence agents involved receive extensive training.[358]

On February 6, 2006, in his written statement for a Senate Committee on the Judiciary hearing, U.S. Attorney General Gonzalez stated:

> *The terrorist surveillance program targets communications where one party to the communication is outside the U.S. and the government has "reasonable grounds to believe" that at least one party to the communication is a member or agent of al Qaeda, or an affiliated terrorist organization. This program is reviewed and reauthorized by the President approximately every 45 days. The Congressional leadership, including the leaders of the Intelligence Committees of both Houses of Congress, has been briefed about this program more than a dozen times since 2001. The program provides the United States with the early warning system we so desperately needed on September 10th.*[359]

In May 2006 news reports alleged additional details regarding the NSA terrorist surveillance program, renewing concerns about the possible existence of inappropriately authorized domestic surveillance. According to these reports,

---

[358] U.S. Department of Justice, "The NSA Program to Detect and Prevent Terrorist Attacks Myth v. Reality," January 27, 2006, [http://www.usdoj.gov/opa/documents/nsa_myth_v_ reality.pdf].

[359] The Honorable Alberto Gonzalez, Testimony before the Senate Committee on the Judiciary, Wartime Executive Power and the NSA's Surveillance Authority, February 6, 2006, [http://judiciary.senate.gov/testimony.cfm?id=1727&wit_id=3936].

following the September 11, 2001 attacks, the NSA contracted with AT&T, Verizon, and BellSouth to collect information about domestic telephone calls handled by these companies. The NSA, in turn, reportedly used this information to conduct "social network analysis" to map relationships between people based on their communications.[360]

It remains unclear precisely what information, if any, was collected and provided to the NSA. Some reports suggest that personally identifiable information (i.e., names, addresses, etc.) were not included. It also has been reported that the content of the calls (what was spoken) was not collected. Since the emergence of these news reports, BellSouth has issued a public statement saying that according to an internal review conducted by the company, "no such [alleged] contract exists" and that the company has "not provided bulk customer calling records to the NSA."[361] Similarly, Verizon has issued a public statement saying that due to the classified nature of the NSA program, "Verizon cannot and will not confirm or deny whether it has any relationship to the classified NSA program," but that "Verizon's wireless and wireline companies did not provide to NSA customer records or call data, local or otherwise."[362] Together, AT&T, Verizon, and BellSouth are the three largest telecommunications companies in the United States, serving more than 200 million customers, accounting for hundreds of billions of calls each year.[363]

In a January 17, 2007 letter to the Senate Committee on the Judiciary, then-Attorney General Gonzalez wrote that:

> *a Judge of the Foreign Intelligence Surveillance Court issued orders authorizing the Government to target for collection international communications into or out of the United States where there is probable cause to believe that one of the communicants is a member or agent of al Qaeda or an associated terrorist organization. As a result of these orders, any electronic surveillance that was occurring as part of the Terrorist*

---

[360] Leslie Cauley, "NSA has Massive Database of Americans' Phone Calls," USA Today, May 11, 2006, p. 1A; Stephen Dinan and Charles Hurt, "Bush Denies Report of 'Trolling' by NSA," The Washington Times, May 12, 2006, p. A1; Barton Gellman and Arshad Mohammed, "Data on Phone Calls Monitored," The Washington Post, May 12, 2006, p. A1.

[361] BellSouth Corporation, "BellSouth Statement on Government Data Collection," May 15, 2006, [http://bellsouth.mediaroom.com/index.php?s=press_releases&item=2860].

[362] Verizon, "Verizon Issues Statement on NSA News Media Coverage," May 16, 2006, [http://newscenter.verizon.com/proactive/newsroom/release.vtml?id=93450&PROACTIVE_ID=cecdc6cdc8c8cbcacbc5cecfcfcfc5cecdcecfc6cacacac6c7c5cf].

[363] Barton Gellman and Arshad Mohammed, "Data on Phone Calls Monitored," The Washington Post, May 12, 2006, p. A1.

Surveillance Program will now be conducted subject to the approval of the Foreign Intelligence Surveillance Court.[364]

The letter further stated that "the President has determined not to reauthorize the Terrorist Surveillance Program when the current authorization expires."

The program and the alleged involvement of telecommunications companies has been the subject of several lawsuits. For a discussion of these legal issues, see CRS Report RL33424, Government Access to Phone Calling Activity and Related Records: Legal Authorities, by Elizabeth B. Bazan, Gina Marie Stevens, and Brian T. Yeh. In July 2008, Congress passed and the President signed into law H.R. 6304, the FISA Amendments Act of 2008 (P.L. 110-261). Among its provisions, Title VIII of the act provides a measure of protection from civil actions to telecommunications companies that provided assistance to government counterterrorism surveillance activities between September 11, 2001, and January 17, 2007. For a discussion of this legislation, see CRS Report RL34279, The Foreign Intelligence Surveillance Act: An Overview of Selected Issues, by Elizabeth B. Bazan, and CRS Report RL33539, Intelligence Issues for Congress, by Richard A. Best, Jr.

Novel Intelligence from Massive Data (NIDM) Program

As part of its efforts to better utilize the overwhelming flow of information it collects, NSA has reportedly been supporting the development of new technology and data management techniques by funding grants given by the Advanced Research Development Activity (ARDA). ARDA is an intelligence community (IC) organization whose mission is described as "to sponsor high-risk, high-payoff research designed to leverage leading edge technology to solve some of the most critical problems facing the Intelligence Community (IC)."[365] ARDA's research support is organized into various technology "thrusts" representing the most critical areas of development. Some of ARDA's research thrusts include Information Exploitation, Quantum Information Science, Global Infosystems Access, Novel Intelligence from Massive Data, and Advanced Information Assurance.

The Novel Intelligence from Massive Data (NIMD) program focuses on the development of data mining and analysis tools to be used in working with

---

[364] Senator Patrick Leahy, "Letter of Attorney General Alberto Gonzales to the Chairman and Ranking Member of the Senate Judiciary Committee ordered printed without objection," remarks in the Senate, Congressional Record, daily edition, vol. 153 (January 17, 2001), pp. S646-S647.

[365] [https://rrc.mitre.org/cfp06.pdf].

massive data.[366] Novel intelligence refers to "actionable information not previously known." Massive data refers to data that has characteristics that are especially challenging to common data analysis tools and methods. These characteristics can include unusual volume, breadth (heterogeneity), and complexity. Data sets that are one petabyte (one quadrillion bytes) or larger are considered to be "massive." Smaller data sets that contain items in a wide variety of formats, or are very heterogeneous (i.e., unstructured text, spoken text, audio, video, graphs, diagrams, images, maps, equations, chemical formulas, tables, etc.) can also be considered "massive." According to ARDA's website (no longer available)[367] "some intelligence data sources grow at a rate of four petabytes per month now, and the rate of growth is increasing." With the continued proliferation of both the means and volume of electronic communications, it is expected that the need for more sophisticated tools will intensify. Whereas some observers once predicted that the NSA was in danger of becoming proverbially deaf due to the spreading use of encrypted communications, it appears that NSA may now be at greater risk of being "drowned" in information.

Data Mining Issues

As data mining initiatives continue to evolve, there are several issues Congress may decide to consider related to implementation and oversight. These issues include, but are not limited to, data quality, interoperability, mission creep, and privacy. As with other aspects of data mining, while technological capabilities are important, other factors also influence the success of a project's outcome.

Data Quality

Data quality is a multifaceted issue that represents one of the biggest challenges for data mining. Data quality refers to the accuracy and completeness of the data. Data quality can also be affected by the structure and consistency of the data being analyzed. The presence of duplicate records, the lack of data standards, the timeliness of updates, and human error can significantly impact the effectiveness of the more complex data mining techniques, which are sensitive to subtle differences that may exist in the data. To improve data quality, it is sometimes necessary to "clean" the data, which can involve the removal of duplicate records, normalizing the values used to represent information in the database (e.g., ensuring that "no" is represented as a 0 throughout the database, and not sometimes as a 0, sometimes as an N, etc.), accounting for missing data points, removing unneeded data fields, identifying anomalous data points (e.g., an

---

[366] Shane Harris, "NSA Spy Program Hinges on State-of-the-Art Technology," Government Executive Magazine, January 20, 2006, [http://www.govexec.com/dailyfed/0106/012006nj1.htm]; Wilson P. Dizard III, "NSA Searches for Novel Intel Answers in the Glass Box," Government Computer News, June 20, 2005, [http://www.gcn.com/24_15/news/ 36139-1.html].

[367] ARDA's website was previously available at [http://www.ic-arda.org].

individual whose age is shown as 142 years), and standardizing data formats (e.g., changing dates so they all include MM/DD/YYYY).

Interoperability

Related to data quality, is the issue of interoperability of different databases and data mining software. Interoperability refers to the ability of a computer system and/or data to work with other systems or data using common standards or processes. Interoperability is a critical part of the larger efforts to improve interagency collaboration and information sharing through e-government and homeland security initiatives. For data mining, interoperability of databases and software is important to enable the search and analysis of multiple databases simultaneously, and to help ensure the compatibility of data mining activities of different agencies. Data mining projects that are trying to take advantage of existing legacy databases or that are initiating first-time collaborative efforts with other agencies or levels of government (e.g., police departments in different states) may experience interoperability problems. Similarly, as agencies move forward with the creation of new databases and information sharing efforts, they will need to address interoperability issues during their planning stages to better ensure the effectiveness of their data mining projects.

Mission Creep

Mission creep is one of the leading risks of data mining cited by civil libertarians, and represents how control over one's information can be a tenuous proposition. Mission creep refers to the use of data for purposes other than that for which the data was originally collected. This can occur regardless of whether the data was provided voluntarily by the individual or was collected through other means.

Efforts to fight terrorism can, at times, take on an acute sense of urgency. This urgency can create pressure on both data holders and officials who access the data. To leave an available resource unused may appear to some as being negligent. Data holders may feel obligated to make any information available that could be used to prevent a future attack or track a known terrorist. Similarly, government officials responsible for ensuring the safety of others may be pressured to use and/or combine existing databases to identify potential threats. Unlike physical searches, or the detention of individuals, accessing information for purposes other than originally intended may appear to be a victimless or harmless exercise. However, such information use can lead to unintended outcomes and produce misleading results.

One of the primary reasons for misleading results is inaccurate data. All data collection efforts suffer accuracy concerns to some degree. Ensuring the accuracy of information can require costly protocols that may not be cost effective if the data is not of inherently high economic value. In well-managed data mining projects, the original data collecting organization is likely to be aware of the data's limitations and account for these limitations accordingly. However, such awareness may not be communicated or heeded when data is used for other

purposes. For example, the accuracy of information collected through a shopper's club card may suffer for a variety of reasons, including the lack of identity authentication when a card is issued, cashiers using their own cards for customers who do not have one, and/or customers who use multiple cards. [368] For the purposes of marketing to consumers, the impact of these inaccuracies is negligible to the individual. If a government agency were to use that information to target individuals based on food purchases associated with particular religious observances though, an outcome based on inaccurate information could be, at the least, a waste of resources by the government agency, and an unpleasant experience for the misidentified individual. As the March 2004 TAPAC report observes, the potential wide reuse of data suggests that concerns about mission creep can extend beyond privacy to the protection of civil rights in the event that information is used for "targeting an individual solely on the basis of religion or expression, or using information in a way that would violate the constitutional guarantee against self-incrimination."[369]

Privacy

As additional information sharing and data mining initiatives have been announced, increased attention has focused on the implications for privacy. Concerns about privacy focus both on actual projects proposed, as well as concerns about the potential for data mining applications to be expanded beyond their original purposes (mission creep). For example, some experts suggest that anti-terrorism data mining applications might also be useful for combating other types of crime as well.[370] So far there has been little consensus about how data mining should be carried out, with several competing points of view being debated. Some observers contend that tradeoffs may need to be made regarding privacy to ensure security. Other observers suggest that existing laws and regulations regarding privacy protections are adequate, and that these initiatives do not pose any threats to privacy.

Still other observers argue that not enough is known about how data mining projects will be carried out, and that greater oversight is needed. There is also some disagreement over how privacy concerns should be addressed. Some observers suggest that technical solutions are adequate. In contrast, some privacy advocates argue in favor of creating clearer policies and exercising stronger oversight. As data mining efforts move forward, Congress may consider a variety of questions including, the degree to which government agencies should use and

---

[368] Technology and Privacy Advisory Committee, Department of Defense. Safeguarding Privacy in the Fight Against Terrorism, March 2004, p. 40.

[369] Ibid., p. 39.

[370] Drew Clark, "Privacy Experts Differ on Merits of Passenger-Screening Program," Government Executive Magazine, November 21, 2003, [http://www.govexec.com/dailyfed/1103/112103td2.htm].

mix commercial data with government data, whether data sources are being used for purposes other than those for which they were originally designed, and the possible application of the Privacy Act to these initiatives.

Legislation in the 108th Congress

During the 108th Congress, a number of legislative proposals were introduced that would restrict data mining activities by some parts of the federal government, and/or increase the reporting requirements of such projects to Congress. For example, on January 16, 2003, Senator Feingold introduced S. 188 the Data-Mining Moratorium Act of 2003, which would have imposed a moratorium on the implementation of data mining under the Total Information Awareness program (now referred to as the Terrorism Information Awareness project) by the Department of Defense, as well as any similar program by the Department of Homeland Security. S. 188 was referred to the Committee on the Judiciary.

On January 23, 2003, Senator Wyden introduced S.Amdt. 59, an amendment to H.J.Res. 2, the Omnibus Appropriations Act for Fiscal Year 2003. As passed in its final form as part of the omnibus spending bill (P.L. 108-7) on February 13, 2003, and signed by the President on February 20, 2003, the amendment requires the Director of Central Intelligence, the Secretary of Defense, and the Attorney General to submit a joint report to Congress within 90 days providing details about the TIA program.[371] Some of the information required includes spending schedules, likely effectiveness of the program, likely impact on privacy and civil liberties, and any laws and regulations that may need to be changed to fully deploy TIA. If the report was not submitted within 90 days, funding for the TIA program could have been discontinued.[372] Funding for TIA was later discontinued in Section 8131 of the FY2004 Department of Defense Appropriations Act (P.L. 108-87), signed into law on September 30, 2003.[373]

On March 13, 2003, Senator Wyden introduced an amendment to S. 165, the Air Cargo Security Act, requiring the Secretary of Homeland Security to submit a report to Congress within 90 days providing information about the impact of CAPPS II on privacy and civil liberties. The amendment was passed by the Committee on Commerce, Science, and Transportation, and the bill was forwarded for consideration by the full Senate (S.Rept. 108-38). In May 2003, S. 165 was passed by the Senate with the Wyden amendment included and was sent

---

[371] The report is available at [http://www.eff.org/Privacy/TIA/TIA-report.pdf].

[372] For more details regarding this amendment, see CRS Report RL31786, Total Information Awareness Programs: Funding, Composition, and Oversight Issues, by Amy Belasco.

[373] For further details regarding this provision, see CRS Report RL31805, Authorization and Appropriations for FY2004: Defense, by Amy Belasco and Stephen Daggett.

to the House where it was referred to the Committee on Transportation and Infrastructure.

Funding restrictions on CAPPS II were included in section 519 of the FY2004 Department of Homeland Security Appropriations Act (P.L. 108-90), signed into law October 1, 2003. This provision included restrictions on the "deployment or implementation, on other than a test basis, of the Computer-Assisted Passenger Prescreening System (CAPPSII)," pending the completion of a GAO report regarding the efficacy, accuracy, and security of CAPPS II, as well as the existence of a system of an appeals process for individuals identified as a potential threat by the system.[374] In its report delivered to Congress in February 2004, GAO reported that "As of January 1, 2004, TSA has not fully addressed seven of the eight CAPPS II issues identified by the Congress as key areas of interest."[375] The one issue GAO determined that TSA had addressed is the establishment of an internal oversight board. GAO attributed the incomplete progress on these issues partly to the "early stage of the system's development."[376]

On March 25, 2003, the House Committee on Government Reform Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census held a hearing on the current and future possibilities of data mining. The witnesses, drawn from federal and state government, industry, and academia, highlighted a number of perceived strengths and weaknesses of data mining, as well as the still-evolving nature of the technology and practices behind data mining.[377] While data mining was alternatively described by some witnesses as a process, and by other witnesses as a productivity tool, there appeared to be a general consensus that the challenges facing the future development and success of government data mining applications were related less to technological concerns than to other issues such as data integrity, security, and privacy. On May 6 and May 20, 2003 the Subcommittee also held hearings on the potential

---

[374] Section 519 of P.L. 108-90 specifically identifies eight issues that TSA must address before it can spend funds to deploy or implement CAPPS II on other than a test basis. These include 1. establishing a system of due process for passengers to correct erroneous information; 2. assess the accuracy of the databases being used; 3. stress test the system and demonstrate the efficiency and accuracy of the search tools; 4. establish and internal oversight board; 5. install operational safeguards to prevent abuse; 6. install security measures to protect against unauthorized access by hackers or other intruders; 7. establish policies for effective oversight of system use and operation; and 8. address any privacy concerns related to the system.

[375] General Accounting Office, Aviation Security: Computer-Assisted Passenger Prescreening System Faces Significant Implementation Challenges, GAO-04-385, February 2004, p. 4.

[376] Ibid.

[377] Witnesses testifying at the hearing included Florida State Senator Paula Dockery, Dr. Jen Que Louie representing Nautilus Systems, Inc., Mark Forman representing OMB, Gregory Kutz representing GAO, and Jeffrey Rosen, an Associate Professor at George Washington University Law School.

opportunities and challenges for using factual data analysis for national security purposes.

On July 29, 2003, Senator Wyden introduced S. 1484, The Citizens' Protection in Federal Databases Act, which was referred to the Committee on the Judiciary. Among its provisions, S. 1484 would have required the Attorney General, the Secretary of Defense, the Secretary of Homeland Security, the Secretary of the Treasury, the Director of Central Intelligence, and the Director of the Federal Bureau of Investigation to submit to Congress a report containing information regarding the purposes, type of data, costs, contract durations, research methodologies, and other details before obligating or spending any funds on commercially available databases. S. 1484 would also have set restrictions on the conduct of searches or analysis of databases "based solely on a hypothetical scenario or hypothetical supposition of who may commit a crime or pose a threat to national security."

On July 31, 2003, Senator Feingold introduced S. 1544, the Data-Mining Reporting Act of 2003, which was referred to the Committee on the Judiciary. Among its provisions, S. 1544 would have required any department or agency engaged in data mining to submit a public report to Congress regarding these activities. These reports would have been required to include a variety of details about the data mining project, including a description of the technology and data to be used, a discussion of how the technology will be used and when it will be deployed, an assessment of the expected efficacy of the data mining project, a privacy impact assessment, an analysis of the relevant laws and regulations that would govern the project, and a discussion of procedures for informing individuals their personal information will be used and allowing them to opt out, or an explanation of why such procedures are not in place.

Also on July 31, 2003, Senator Murkowski introduced S. 1552, the Protecting the Rights of Individuals Act, which was referred to the Committee on the Judiciary. Among its provisions, section 7 of S. 1552 would have imposed a moratorium on data mining by any federal department or agency "except pursuant to a law specifically authorizing such data-mining program or activity by such department or agency." It also would have required

> *The head of each department or agency of the Federal Government that engages or plans to engage in any activities relating to the development or use of a data-mining program or activity shall submit to Congress, and make available to the public, a report on such activities.*

On May 5, 2004, Representative McDermott introduced H.R. 4290, the Data-Mining Reporting Act of 2004, which was referred to the House Committee on Government Reform Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census. H.R. 4290 would have required

> *each department or agency of the Federal Government that is engaged in any activity or use or develop data-mining technology shall each submit a public report to Congress on all such activities of the department or agency under the jurisdiction of that official.*

A similar provision was included in H.R. 4591/S. 2528, the Civil Liberties Restoration Act of 2004. S. 2528 was introduced by Senator Kennedy on June 16, 2004 and referred to the Committee on the Judiciary. H.R. 4591 was introduced by Representative Berman on June 16, 2004 and referred to the Committee on the Judiciary and the Permanent Select Committee on Intelligence.

Legislation in the 109th Congress

Data mining continued to be a subject of interest to Congress in the 109th Congress. On April 6, 2005, H.R. 1502, the Civil Liberties Restoration Act of 2005 was introduced by Representative Berman and was referred to the Committee on the Judiciary[378], the Permanent Select Committee on Intelligence, and the Committee on Homeland Security. Section 402, Data-Mining Report, of H.R. 1502 would have required that

> *The Head of each department or agency of the Federal Government that is engaged in any activity to use or develop data-mining technology shall each submit a public report to Congress on all such activities of the department or agency under the jurisdiction of that official.*

As part of their content, these reports would have been required to provide, for each data mining activity covered by H.R. 1502, information regarding the technology and data being used; information on how the technology would be used and the target dates for deployment; an assessment of the likely efficacy of the data mining technology; an assessment of the likely impact of the activity on privacy and civil liberties; a list and analysis of the laws and regulations that would apply to the data mining activity and whether these laws and regulations would need to be modified to allow the data mining activity to be implemented; information on the policies, procedures, and guidelines that would be developed and applied to protect the privacy and due process rights of individuals, and ensure that only accurate information is collected and used; and information on how individuals whose information is being used in the data mining activity will be notified of the use of their information, and, if applicable, what options will be available for individual to opt-out of the activity. These reports would have been due to Congress no later than 90 days after the enactment of H.R. 1502, and would have been required to be updated annually to include "any new data-mining technologies."

---

[378] H.R. 1502 was referred to the Subcommittee on Immigration, Border Security, and Claims on May 10, 2005, and later discharged by the subcommittee on July 8, 2005.

On June 6, 2005, S. 1169, the Federal Agency Data-Mining Reporting Act of 2005 was introduced by Senator Feingold, and was referred to the Senate Committee on the Judiciary. Among its provisions, S. 1169 would have required any department or agency engaged in data mining to submit a public report to Congress regarding these activities. These reports would have been required to include a variety of details about the data mining project, including a description of the technology and data to be used, a discussion of the plans and goals for using the technology when it will be deployed, an assessment of the expected efficacy of the data mining project, a privacy impact assessment, an analysis of the relevant laws and regulations that would govern the project, and a discussion of procedures for informing individuals their personal information will be used and allowing them to opt out, or an explanation of why such procedures are not in place.

On July 11, 2005, H.R. 3199, the USA PATRIOT Improvement and Reauthorization Act of 2005 was introduced. On July 21, 2005, Representative Berman introduced H.Amdt. 497 to H.R. 3199, which would required the Attorney General to submit a report to Congress on the data mining initiatives of the Department of Justice and other departments and agencies as well. The provision stated, in part;

> *The Attorney General shall collect the information described in paragraph (2) from the head of each department or agency of the Federal Government that is engaged in any activity to use or develop data-mining technology and shall report to Congress on all such activities.*

H.Amdt. 497 was passed on July 21, 2005 by a 261-165 recorded vote and appeared as Section 132 of H.R. 3199. Also on this day, H.R. 3199 was passed by the House and sent to the Senate. On July 29, 2005, the Senate passed an amended version of H.R. 3199. The Senate version did not contain a comparable provision on data mining. The bill went to a House-Senate conference in November 2005. Section 126 of the conference report (H.Rept. 109-333) filed on December 8, 2005 included a provision for a report on data mining by the Department of Justice alone, rather than other departments and agencies as well. The provision stated, in part:

> *Not later than one year after the date of enactment of this Act, the Attorney General shall submit to Congress a report on any initiative of the Department of Justice that uses or is intended to develop pattern-based data mining technology…*

The bill was signed into law as P.L. 109-177 on March 9, 2006.

On October 6, 2005, H.R. 4009, the Department of Homeland Security Reform Act of 2005, was introduced by Representative Thompson, and was referred to

the Committee on Homeland Security, the Permanent Select Committee on Intelligence, and the Committee on Transportation and Infrastructure. Section 203(c)(16) would have directed the Chief Intelligence Officer, as established in Section 203(a):

> *To establish and utilize, in conjunction with the Chief Information Officer of the Department, a secure communications and information technology infrastructure, including data-mining and other advanced analytical tools, in order to access, receive, and analyze data and information in furtherance of the responsibilities under this section, and to disseminate information acquired and analyzed by the Department, as appropriate.*

On December 6, 2005, H.R. 4437, the Border Protection, Antiterrorism, and Illegal Immigration Control Act of 2005 was introduced by Representative Sensenbrenner and was referred to the Committee on the Judiciary and the Committee on Homeland Security. On December 8, 2005, the Committee on the Judiciary held a markup session and ordered an amended version of H.R. 4437 to be reported. On December 13, 2005, the Committee on Homeland Security discharged the bill, which was subsequently referred to and discharged from the Committee on Education and the Workforce and the Committee on Ways and Means. On December 16, 2005, H.R. 4437 was passed by the House and sent to the Senate, where it was referred to the Committee on the Judiciary.

Section 1305, Authority of the Office of Security and Investigations to Detect and Investigate Immigration Benefits Fraud, of H.R. 4437 would have granted the Office of Security and Investigations of the United States Citizenship and Immigration Services at the Department of Homeland Security the authority to:

> *(1) to conduct fraud detection operations, including data mining and analysis;*
> *(2) to investigate any criminal or noncriminal allegations of violations of the Immigration and Nationality Act or title 18, United States Code, that Immigration and Customs Enforcement declines to investigate;*
> *(3) to turn over to a United States Attorney for prosecution evidence that tends to establish such violations; and*
> *(4) to engage in information sharing, partnerships, and other collaborative efforts with any —*
> *(A) Federal, State, or local law enforcement entity;*
> *(B) foreign partners; or*
> *(C) entity within the intelligence community (as defined in section 3(4) of the National Security Act of 1947 (50 U.S.C. 401a(4)).*

On July 12, 2006, Senator Feingold introduced S.Amdt 4562 to H.R. 5441, the Homeland Security Department FY2007 appropriations bill. S.Amdt. 4562 is substantively similar to S. 1169, although only applies to departments and

agencies within the Department of Homeland Security, rather than the entire federal government. S.Amdt. 4562 was agreed to by unanimous consent and was included in the Senate-passed version of H.R. 5441 as Section 549. According to the conference report (H.Rept. 109-699) Section 549 was deleted from the final bill that was passed into law (P.L. 109-295).[379] However, the conference report also included a statement on data mining by the conference managers expressing concern about the development and use of data mining technology and;

> *"direct[s] the DHS Privacy Officer to submit a report consistent with the terms and conditions listed in section 549 of the Senate bill. The conferees expect the report to include information on how it has implemented the recommendation laid out in the Department's data mining report received July 18, 2006."*[380]

Legislation and Hearings in the 110th Congress

Data mining has been the subject of some of the earliest proposed bills and hearings of the 110th Congress. On January 10, 2007, S. 236, the Federal Agency Data-Mining Reporting Act of 2007 was introduced by Senator Feingold and Senator Sununu, and was referred to the Senate Committee on the Judiciary. Among its provisions, S. 236 would require any department or agency engaged in data mining to submit a public report to Congress regarding these activities. These reports would be required to include a variety of details about the data mining project, including a description of the technology and data to be used, a discussion of the plans and goals for using the technology when it will be deployed, an assessment of the expected efficacy of the data mining project, a privacy impact assessment, an analysis of the relevant laws and regulations that would govern the project, and a discussion of procedures for informing individuals their personal information will be used and allowing them to opt out, or an explanation of why such procedures are not in place.[381]

Also in the Senate, the Committee on the Judiciary held a hearing on January 10, 2007 entitled "Balancing Privacy and Security: The Privacy Implications of Government Data Mining Programs." The witnesses included a former Member of Congress and several individuals from research centers and think tanks. Collectively, they highlighted a number of perceived strengths and weaknesses of data mining, as well as the continually evolving nature of the technology and

---

[379] See p. 180.

[380] Ibid., p. 117. The DHS Privacy Office delivered the requested report to Congress on July 6, 2007. A copy of the report is available at [http://www.dhs.gov/xlibrary/assets/privacy/privacy_rpt_datamining_2007.pdf].

[381] On April 12, 2007, the Committee voted to approve a revised version of S. 236, which was sent to the full Senate. A description of this version of the bill is discussed later in the chronology of this section of the report.

practices behind data mining.[382] The witnesses also addressed the inherent challenge of simultaneously protecting the nation from terrorism while also protecting civil liberties.

On February 28, 2007, Senator Reid introduced S.Amdt. 275 to S. 4 the Improving America's Security by Implementing Unfinished Recommendations of the 9/11 Commission Act of 2007. Section 504 of this amendment, entitled the Federal Agency Data Mining Report Act of 2007, was identical to S. 236, as introduced. During the Senate floor debates held on S. 4 in early March 2007, several amendments to the data mining section of S. 4 were introduced.

On March 6, 2007, Senator Kyl introduced S.Amdt. 357 to S.Amdt. 275 of S. 4. The purpose of S.Amdt. 357 was described as "to amend the data-mining reporting requirement to protect existing patents, trade secrets, and confidential business processes, and to adopt a narrower definition of data mining in order to exclude routine computer searches."[383] Later on March 6, 2007, Senator Kyl offered a modification to S.Amdt. 357 that used definitions of data mining and database very similar to those that appear in P.L. 109-177 the USA PATRIOT Improvement and Reauthorization Act of 2005, and that slightly changed the original language of S.Amdt. 357 regarding protection of patents and other proprietary business information.

On March 8, 2007, Senator Feingold introduced S.Amdt. 429 to S.Amdt. 275. S.Amdt. 429 is very similar to S. 236, as introduced, with a few differences. One difference is that the initial description used to partially define data mining is changed to include "a program involving pattern-based queries, searches, or other analyses of 1 or more electronic databases...." Another difference is that the data mining reporting requirement excludes data mining initiatives that are solely for "the detection of fraud, waste, or abuse in a Government agency or program; or the security of a Government computer system."[384] Another difference is the inclusion of language requiring that the data mining reports be "produced in coordination with the privacy officer of that department or agency."[385] S.Amdt. 429 also includes language detailing the types of information that should be included in the classified annexes of the data mining reports (i.e.,

---

[382] Witnesses testifying at the hearing included former Representative Robert Barr of Liberty Strategies, LLC; James Carafano of the Heritage Foundation; Jim Harper of the CATO Institute; Leslie Harris of the Center for Democracy and Technology; and Kim Taipale of the Center for Advanced Studies in Science and Technology.

[383] Congressional Record, vol. 153, March 6, 2007, p. S2670.

[384] Congressional Record, vol. 153, March 8, 2007, p. S2949.

[385] Ibid.

classified information, law enforcement sensitive information, proprietary business information, and trade secrets), and states that such classified annexes should not be made available to the public.

Later on March 8, 2007, Senator Feingold introduced S.Amdt. 441 to S.Amdt.

357. S.Amdt. 441 is substantively the same as S.Amdt. 429, but with a technical modification.

On March 13, 2007, S.Amdt. 441 was agreed to by unanimous consent, and S.Amdt. 357, as modified, and as amended by S.Amdt. 441 was agreed to by unanimous consent. Also on March 13, 2007, S. 4 passed the Senate by a 60-38 vote. The data mining provision appears as Section 604 in S. 4. As originally passed by the House in January 2007, the House version of S. 4, H.R. 1, did not contain a comparable provision on data mining.

On March 21, 2007, the House Committee on Appropriations Subcommittee on Homeland Security held a hearing entitled "Privacy and Civil Rights in Homeland Security." The witnesses included Hugo Teufel III, the Chief Privacy Officer at DHS; Daniel Sutherland of the Office of Civil Rights and Civil Liberties at DHS; and the Government Accountability Office (GAO). Collectively they addressed some of the data mining activities being carried out by DHS, in particular the use of the Analysis, Dissemination, Visualization, Insight, and Semantic Enhancement (ADVISE) data mining tool, and the precautions taken by DHS to protect citizens' privacy and civil liberties.

On April 12, 2007, the Senate Committee on the Judiciary voted to approve a revised version of S. 236, the Data Mining Act of 2007. On June 4, 2007, the Committee reported the bill. With one exception, this revised version of S. 236 is substantively identical to data mining provision passed as Section 604 in S. 4, and later as Section 804 of P.L. 110-53 in July 2007 (discussed below). As passed by the Committee, S. 236 includes a provision regarding penalties for the unauthorized disclosure of classified information contained in the annex of any reports submitted to Congress.

On June 15, 2007, the House of Representatives passed H.R. 2638, concerning FY2008 appropriations for the Department of Homeland Security. The accompanying House Report (H.Rept. 110-181) includes language prohibiting funding for the Analysis, Dissemination, Visualization, Insight, and Semantic Enhancement (ADVISE) data mining program until DHS has completed a privacy impact assessment for the program. ADVISE is alternatively described as a technology framework, or a tool, for analyzing and visually representing large amounts of data. ADVISE is being developed by the Directorate for Science and Technology at DHS. The accompanying Senate Report (S.Rept. 110-84) for S. 1644, concerning FY2008 DHS appropriations, also includes similar language recommending that no funding be allocated for ADVISE until a program plan and privacy impact assessment is completed.

On July 9, 2007, the Senate took up H.R. 1, struck all language following the enacting clause, substituted the language of S. 4 as amended, and passed the bill by unanimous consent. Differences between H.R. 1 and S. 4 were resolved in conference later that month. The data mining provision that appeared as Section 604 in S. 4 was retained as Section 804 in the agreed upon bill. On July 26, 2007, the Senate agreed to the conference report (H.Rept. 110-259) in a 85-8 vote. On July 27, 2007, the House agreed to the conference report in a 371-40 vote. On August 3, 2007, the bill was signed into law by the President as P.L. 110-53.

For Further Reading

CRS Report RL32802, Homeland Security: Air Passenger Prescreening and Counterterrorism, by Bart Elias and William Krouse. Out of print; available from author (7-8679).

CRS Report RL32536, Multi-State Anti-Terrorism Information Exchange (MATRIX)Pilot Project, by William J. Krouse.

CRS Report RL30671, Personal Privacy Protection: The Legislative Response, by Harold C. Relyea. Out of print; available from author (7-8679).

CRS Report RL31730, Privacy: Total Information Awareness Programs and Related Information Access, Collection, and Protection Laws, by Gina Marie Stevens.

CRS Report RL31786, Total Information Awareness Programs: Funding, Composition, and Oversight Issues, by Amy Belasco.

DARPA, Report to Congress Regarding the Terrorism Information Awareness Program, May 20, 2003, [http://www.eff.org/Privacy/TIA/TIA-report.pdf].

Department of Defense, Office of the Inspector General, Information Technology

Management: Terrorism Information Awareness Program (D-2004-033), December 12, 2003 [http://www.dodig.osd.mil/audit/reports/FY04/04-033.pdf].

Department of Homeland Security, Office of the Inspector General, Survey of DHS Data Mining Activities (OIG-06-56), August 2006 [http://www.dhs.gov/xoig/ assets/mgmtrpts/OIG_06-56_Aug06.pdf].

Department of Homeland Security, Office of Legislative Affairs, Letter Report Pursuant to Section 804 of the Implementing Recommendations of the 9/11 Commission Act of 2007, February 11, 2008, [http://www.dhs.gov/xlibrary/assets/privacy/privacy_rpt_datamining_2008.pdf].

Department of Homeland Security, Privacy Office, 2007 Data Mining Report: DHS Privacy Office Response to House Report 109-699, July 6, 2007, [http://www.dhs.gov/xlibrary/assets/privacy/privacy_rpt_datamining_2007.pdf].

Department of Homeland Security, Privacy Office, Report to the Public on the Transportation Security Administration's Secure Flight Program and Privacy Recommendations, December 2006, [http://www.dhs.gov/xlibrary/assets/privacy/privacy-secure-flight-122006.pdf].

Department of Homeland Security, Privacy Office, Report to the Public Concerning the Multistate Anti-Terrorism Information Exchange (MATRIX) Pilot Project, December 2006, [http://www.dhs.gov/xlibrary/assets/privacy/privacy-secure -flight-122006.pdf].

Jeff Jonas and Jim Harper, Effective Counterterrorism and the Limited Role of Predictive Data Mining, CATO Institute Policy Analysis No. 584, December 11, 2006 [http://www.cato.org/pubs/pas/pa584.pdf].

Office of the Director of National Intelligence, Data Mining Report, February 15, 2008, [http://www.dni.gov/reports/data_mining_report_feb08.pdf].

Total Information Awareness Programs: Funding, Composition, and Oversight Issues, RL31786 (March 21, 2003).

AMY BELASCO, CONGRESSIONAL RESEARCH SERV., TOTAL INFORMATION AWARENESS PROGRAMS: FUNDING, COMPOSITION, AND OVERSIGHT ISSUES (2003), *available at* http://www.intelligencelaw.com/library/secondary/crs/pdf/RL31786_3-21-2003.pdf.

Order Code RL31786
Report for Congress
Updated March 21, 2003

Amy Belasco
Specialist in National Defense
Foreign Affairs, Defense, and Trade Division

Summary

Late last year controversy erupted about a Department of Defense (DOD) R&D effort called Total Information Awareness (TIA) under an office headed by retired Admiral John D. Poindexter within the Defense Advanced Research Projects Agency (DARPA). By integrating various new tools designed to detect, anticipate, train for, and provide warnings about potential terrorist attacks, DARPA hopes to develop a prototype Total Information Awareness system. This system would integrate a number of ongoing R&D efforts, referred to in this paper as Total Information Awareness programs. While concern has centered primarily on privacy issues, accounts of the program's funding have also differed. This report covers the funding, composition, oversight, and technical feasibility of TIA programs. The privacy implications are addressed in CRS Report RL31730, Privacy: Total Information Awareness Programs and Related Information Access, Collection, and Protection Laws, by Gina Marie Stevens.

In a press interview, Under Secretary of Defense for Acquisition, Technology and Logistics, Edward C. "Pete" Aldridge, stated that the Total Information Awareness project is funded at $10 million in FY2003 and $20 million in FY2004. Other reports indicated higher funding levels of over $100 million in FY2003 and over $200 million for the three-year period, FY2001 - FY2003.

Different accounts of funding levels reflect the fact that DARPA is funding both an integrative effort called the TIA system, as well as 16 individual R&D efforts or TIA programs that could be combined to create that system. In FY2003, DARPA is dedicating $10 million to integrate various R&D efforts into a prototype TIA system, and $137.5 million for the various R&D programs that could make up that system and that are managed by the Information Awareness Office (IAO) headed by Poindexter. Funding for these programs total $137.5 million in

FY2003 and $317.0 million for FY2001-FY2003. DOD is requesting $169.2 million for TIA programs in FY2004 and $170.3 in FY2005, and $20 million in FY2004 and $24.5 million in FY2005 for the TIA system integration. These TIA programs are ongoing.

In response to concerns about TIA programs, Congress included special oversight provisions – known as the Wyden amendment – in the FY2003 Consolidated Appropriations Resolution (P.L. 108-7) requiring that the Secretary of Defense, the Director of Central Intelligence and the Attorney General submit a detailed joint report on TIA programs within ninety days or face a cutoff in funding. Senator Feingold, Senator Grassley and other Members also proposed restrictions on data mining in the DOD and the new Department of Homeland Security.

In light of the report required by P.L. 108-7, hearings on TIA programs are likely in the 108th Congress. In addition to privacy concerns, Congress may also address several oversight issues for TIA programs including monitoring collaboration between DARPA and potential users in the law enforcement and intelligence communities and assessing the technical feasibility of the project. This report will be updated as necessary.

Current Controversy over Total Information Awareness Programs

Established in January 2002 under retired Admiral John Poindexter, USN, the mission of the Information Awareness Office (IAO) in the Defense Advanced Research Project Agency (DARPA) is to develop new tools to detect, anticipate, train for, and provide warnings about potential terrorist attacks.[386] Within three to five years, DARPA envisions that these tools would be integrated into a prototype Total Information Awareness (TIA) system to provide better intelligence support to senior government officials. If proven effective, Under Secretary of Defense for Acquisition, Technology and Logistics Edward C. "Pete" Aldridge has suggested that the TIA technology prototypes will be turned over to "intelligence, counterintelligence and law enforcement communities as a tool to help them in their battle against domestic terrorism."[387]

In a press conference on November 20, 2002, Under Secretary Aldridge stated that funding for the Total Information Awareness System (TIA) is $10 million in

---

[386] The larger issue of the types of intelligence tools needed to combat terrorism is extensively discussed in Report of the Markle Foundation Task Force, Protecting America's Freedom in the Information Age, October 2002; see especially, pp. 25ff, 37ff, 53ff, and 81ff.

[387] Under Secretary of Defense Aldridge as quoted in Defense Department Briefing Transcript, November 20, 2002, p. 10; see [http://www. defenselink.mil].

FY2003.[388] On February 7, 2003, he reiterated that funding for the TIA project is $10 million in FY2003 and $20 million in FY2004. The Electronic Privacy Information Center (EPIC), a non-profit organization specializing in privacy issues, calculated that TIA-related programs totaled $112 million in FY2003 and $240 million for the three-year period, FY2001-FY2003.[389] Press reports also cited funding of over $200 million over three years.[390]

These alternative funding levels reflect the difference between the $10 million in funding for the R&D specifically labeled the "Total Information Awareness System" that would integrate various R&D technology efforts, and the $137.5 million in funding for various R&D efforts managed by the Information Awareness Office that could become part of that system. Funding for TIA programs that are managed by the Information Awareness Office includes R&D efforts to develop technologies to improve data mining so as to allow DOD to sift through and analyze patterns in vast amounts of information, to translate large volumes of foreign language materials electronically, to strengthen DOD's information infrastructure, and to devise new tools for high-level decision makers trying to anticipate, train, and respond to terrorist attacks. (See Appendix below for descriptions of individual projects).[391]

To proponents, TIA R&D holds out the promise of developing a sophisticated system that would develop new technologies to find patterns from multiple sources of information in order to give decision makers new tools to use to detect, pre-empt and react to potential terrorist attacks. To opponents, TIA has the potential to violate the privacy of individuals by giving the government access to vast amounts of information about individuals as well as possibly mis-identifying individuals as potential terrorists.

Reflecting both these viewpoints, P.L. 108-7 (H.J.Res. 2) the FY2003 Consolidated Appropriations Resolution requires that the Secretary of Defense, the Director of Central Intelligence (DCI), and the Attorney General submit to Congress a detailed report on TIA by May 21, 2003 or face a cutoff in funding (see Restrictions on TIA in FY2003 Consolidated Appropriations Resolution later in

---

[388] Under Secretary of Defense Aldridge as quoted in Defense Department Briefing Transcript, November 20, 2002, p. 10; see [http://www. defenselink.mil].

[389] See Electronic Privacy Information Center, "Total Information Awareness (TIA) Budget" on web site: [http://www.epic.org/].

[390] William Safire, New York Times, "You are a Suspect," November 14, 2002, see [http://nytimes.com/2002/22/14/opinion/14AF.html].

[391] See description of TIA in DARPA, RDT&E Descriptive Summaries for FY2003 (or the R-2), available at the DARPA web site: [http://www.dtic.mil/comptroller/fy2003budget/budget_justification/pdfs/rdtande/darpa_vol1.pdf].

this report for more details). In the meantime, TIA programs are continuing.[392] DARPA has, for example, obligated $7.4 million of the $10 million available in FY2003 for TIA system integration.[393]

On March 13, 2003, Paul McHale, the new Assistant Secretary of Defense for Homeland Security, testified that although he considered it appropriate for DARPA to develop TIA technologies, once completed, DOD did not anticipate using the technology because of the desire that " this kind of intrusive but perhaps essential capability" be operated by civilian rather than military personnel.[394] Instead, he anticipated that the TIA system would be transferred to civilian law enforcement agencies and be subject to the judicial and congressional oversight.[395]

FY2001-FY2003 Funding Levels

According to DARPA, technology developed in some or all of the sixteen R&D efforts managed by the Information Awareness Office may be integrated into the TIA system.[396] DARPA's FY2003 request for the R&D efforts managed by the Information Awareness Office totaled $137.5 million in FY2003 (see Table 1 below), including $10 million for the integrative efforts specifically labeled the Total Information Awareness System, a new start in FY2003.

Technology Currently Linked to the TIA System

DARPA's FY2003 budget materials state that TIA will integrate technology and components from at least 8 of the 16 R&D efforts (including the integration itself) that are managed by the Information Awareness Office.[397] According to DARPA, TIA is "the assured transition of a system-level prototype that integrates technology and components developed in other DARPA programs including [italics added] Genoa and Genoa II ... TIDES ..., Genisys, EELD, WAE, HID, and

---

[392] Press reports indicating that TIA programs have been terminated are inaccurate.

[393] Information provided to CRS by DARPA, February 2003.

[394] Testimony of Paul McHale before the Subcommittee on Special Oversight Panel on Terrorism, Unconventional Threats and Capabilities, House Armed Services Committee, Hearing on Force Protection, March 13, 2003.

[395] Ibid.

[396] See table and appendix for how R&D linked to TIA is shown in DARPA's budget justification materials. DARPA provided CRS with the list of 16 R&D efforts that are managed by the Information Awareness Office.

[397] Eight counts Genoa and Genoa II as one project, and includes TIA integration as one of the components.

Bio-Surveillance ..."[398] (See Table 2 and the Appendix for funding and description of these R&D efforts).

Funding for these eight R&D efforts totals $110.6 million in FY2003, $83.8 million in FY2002, and $65.0 million in FY2001 (see Table 1). Three follow-on machine translation efforts under the Information Awareness Office will probably also be incorporated into the TIA system.

Information Awareness Office-Managed R&D

According to DARPA, the TIA system may also exploit the results of other R&D efforts that are under the Information Awareness office, other DARPA efforts, or R&D conducted outside of DARPA.[399] Several DARPA R&D efforts under other offices appear to have similar purposes to those specifically linked to TIA.[400] DARPA also hopes to exploit commercial data mining technology and R&D developed by other agencies like the National Security Agency. According to the Director of DARPA, all funding managed by the Information Awareness Office is considered to be Total Information Awareness programs.[401]

Funding for projects managed by the Information Awareness Office totals $137.5 million in FY2003, $99.5 million in FY2002, and $80 million in FY2001. Over the three-year period, FY2001- FY2003, funding totals $317.0 million. The increase in FY2003 reflects several new starts in FY2003 for Genisys, a comprehensive data mining effort, MIDGET, a system designed to prevent contamination of open databases, Rapid Analytic Wargaming, a tool for decision makers, and the TIA integration effort (see Table 2 below and Appendix).

Although the TIA system was first proposed as an integrated entity in the FY2003 budget shortly after establishment of the Information Awareness Office, some of

---

[398] See description of TIA in DARPA, RDT&E Descriptive Summaries for FY2003; see [http://www.dtic.mil/comptroller/fy2003budget/budget_justification/pdfs/rdtande/darpa_vol1.pdf].

[399] See Briefing by John Poindexter, Director, Information Awareness Office, to Congressional Authorizing Committees Staff, February 26, 2002. For example, DARPA spokesman suggested that TIDES system could be combined with OASIS, a system designed to protect DOD's information systems from cyber attack; see 23rd DARPA System and Technology Symposium July 29-August 2, 2002 on web site shown below. [http://www.darpa.mil/DARPATech2002/presentation.html].

[400] For example, other DARPA offices manage Software for Situational Analysis and Rapid Knowledge Foundation, two programs designed to find ways to exploit multiple data bases, in this case to identify biowarfare threats, just as Genisys and EELD, two TIA-linked efforts, analyze and mine data to identify potential terrorists.

[401] Statement during briefing to congressional staff by Dr. Tony Tether, Director of DARPA, "DARPA's Information Technology Initiative on Countering Terrorism, January 27, 2003. on January 27, 2003.

the R&D efforts that could become part of that system have been underway for a number of years. In fact, several of the R& D efforts, e.g. Project Genoa and machine translation of languages, first received funds in 1996 and 1997 respectively. For comparative purposes, Table 1 above and the more detailed Table 2 below show funding from FY2001 through FY2003 for all the elements now managed by the Information Awareness Office that could become part of the Total Information Awareness system.

Authorization and Appropriation of DOD RDT&E Programs

Funding for DARPA, as for the Research, Development, Test & Evaluation (RDT&E) programs of the services, is authorized and appropriated annually at the account level. In the case of DARPA, funding is included within the RDT&E, Defensewide account.[402] The TIA system, like other R&D efforts, is not specifically identified in statutory language in the FY2003 DOD authorization or appropriation acts.

Congressional intent about the funding levels for individual R&D efforts, however, may be included in committee reports, and is considered binding. The FY2003 DOD authorization and appropriation conference reports did not include any specific language about the TIA system, and the House and Senate appropriators voiced different views about various Total Information Awareness components.[403]

FY2001-FY2003 Funding for Individual R&D Efforts

Based on their primary purpose, the sixteen R&D efforts managed by the Information Awareness Office have been grouped into the four categories below. Table 2 below shows the funding for FY2001-FY2003 for the individual R&D efforts managed by the Information Awareness Office, including those R&D

---

[402] DARPA provides detailed descriptions of its programs and projects in budget justification materials submitted to Congress annually.

[403] The FY2003 appropriation conference report mentions only one TIA component, Genisys, suggesting that delays might justify lower funding; see Committee of Conference on Appropriations, Making Appropriations for the Department of Defense for the Fiscal Year Ending September 30, 2003, and for other purposes, H.Rept. 107-732, p. 305. The House and Senate versions of the FY2003 DOD Authorization Act made different recommendations about Program Element 0602301E, which funds some of the R&D managed by IAO. The House recommended no reductions and commended DARPA's overall information awareness programs, and the Senate recommended cuts in two R&D efforts under IAO, the Bio-Surveillance and Genisys R&D efforts. For House action, see House Armed Services Committee, Bob Stump National Defense Authorization Act for Fiscal Year 2003, May 3, 2002, H.Rept. 107-436, p. 239 and p. 241. For Senate action, see Senate Armed Services Committee, National Defense Authorization Act for Fiscal Year 2003, May 14, 2002, S.Rept. 107-151, p. 230.

efforts currently designated as part of the TIA system.[404] The Appendix briefly describes each R&D efforts.

New Data Mining and Analysis Technologies

These R&D efforts are designed to develop technologies that would be capable of sifting through large data bases, e.g. financial, communications, travel, to detect patterns associated with terrorists' activities. Total funding for these efforts was $29.2 million in FY2001, $38.2 million in FY2003 and $53.0 million in FY2003. Increases reflect initiation of the Bio-surveillance effort in FY2002 and the Genisys program in FY2003, both of which have raised privacy concerns.

New Machine Translation Technologies

These R&D efforts are intended to develop new software technology to translate large volumes of foreign language material, both written and oral, that would be collected from sources ranging from electronic sources to battlefield transmissions. At $36 million annually, funding for these efforts was stable between FY2001 and FY2003.

Protection of Critical Information Infrastructure

These R&D efforts are intended to protect DOD's information infrastructure and detect mis-information in open-source data that DOD may collect. Funding in this area grew from zero in FY2001 to $2.0 million in FY2002 with the initiation of DefenseNet, and jumped to $9.5 million with the new Mis-Information Detection and Generation effort.

Tools for High-Level Decision Makers

These R&D efforts are intended to develop tools, ranging from war-gaming simulations to collaborative reasoning processes, designed to help high-level decision makers anticipate, train for, pre-empt, or react to terrorist acts. Funding for these efforts increased from $14.4 million to $23.5 million in FY2002 with the doubling in the funding level for Wargaming the Asymmetric Environment. That funding jumped to $39.5 million with the initiation of Total Information Awareness System, the integrative effort.

---

[404] The 16 R&D efforts have been grouped into categories based on Department of Defense, FY2003 Budget Estimate, Research, Development, Test and Evaluation, Defense-wide, Volume 1, Defense Advanced Research projects Agency, and briefings by project managers to the 23rd DARPA System and Technology Symposium, July 29 - August 2, 2002; see [http://www.dtic.mil/comptroller/fy2003budget/budget_justification/pdfs/rdtande/darpa_vol1.pdf] and [http://www.darpa.mil/DARPATech2002/presentation.html]. Table 2 in this report shows how the various TIA components are included in program elements and projects in DARPA's FY2003 Budget Estimate.

Future Funding for Information Awareness Office Programs

For FY2004, DARPA is requesting $169.2 million for TIA programs and $170.3 million in FY2005.[405] If DARPA funds the R&D efforts that are managed by the Information Awareness Office comparably to funding in previous years, annual funding for TIA programs would average about $145 million annually.[406] The higher levels requested by DOD in the FY2004 budget suggest additional emphases by DARPA on this program. If past funding trends hold, DARPA could spend about $600 million for TIA-related R&D in the next four years, at which point the project is slated to be complete. This funding would be in addition to the $317 million spent from FY2001-FY2003.

Ongoing DARPA Collaboration

DARPA's goals for TIA programs call for sharing of information and analysis among DOD, the intelligence community, counter-intelligence, law enforcement and high-level policy and operational decision makers who could exploit both commercial data mining and analysis systems and new tools being developed in TIA programs. DARPA has also consulted with other DOD offices, such as Strategic Command.[407] Thus far, DARPA's collaboration with agencies outside DOD has been informal, including an unsigned memorandum of understanding developed with the FBI and meetings with Office of Homeland Security officials.[408]

Within DOD, DARPA has established a site at the Army's Information Dominance Center at Fort Belvoir to test potential elements of the TIA system, such as Genoa, by applying various tools in an operational environment using data about U.S. persons that is available to the intelligence community under existing laws and policies. That information includes 13 categories of

---

[405] DARPA, "Paper in response to questions from CRS," February 2003. DOD submits a two-year budget but Congress appropriates only one year of funding.

[406] DARPA's FY2003 budget justification material includes funding estimates for FY2004 -FY2007 at the project level. The average share of TIA-related R&D in the relevant projects for FY2001-FY2003 can be used to project funding levels for future years. For example, all funding in DARPA for Project ST-28, Asymmetric Threat in Program Element 0602301E, which is solely dedicated to TIA-related projects, can be included. In addition, about half of the funding in Project ST-11, Intelligent Systems and Software, and about 15% of the total for Project CCC-01, Command & Control Information Systems in PE 0603760E, may also be dedicated to TIA based on their shares in earlier years.

[407] Briefing by Dr. Tony Tether, Director, DARPA to Congressional staffers, "DARPA's Information Technology Initiative on Countering Terrorism, January 27, 2003.

[408] DARPA's Director, Dr. Tony Tether, stated that DARPA has a draft unsigned MOU with the FBI during the January 27, 2003 briefing to Congressional staffers.

information ranging from publicly available data to information about potential intelligence sources.[409]

DARPA is also testing other potential TIA components, like Genisys, by using fictitious data and mock "Red" or terrorist teams who create potential terrorist scenarios, as well as experimenting with linking its intelligence information with a variety of commercially available data mining systems as and systems developed by other government agencies like the National Security Agency.[410] Through these various experiments, DARPA hopes to test the utility of various data mining tools in identifying potential terrorists. In addition, DARPA has tried out some of its tools on information obtained from prisoners at the U.S. naval base at Guantanamo, Cuba.

Restrictions on TIA in FY2003 Consolidated Appropriations Resolution and Other Legislative Proposals

The FY2003 Consolidated Appropriations Resolution, P.L. 108-7 (H.J.Res. 2) includes a provision requiring that the Secretary of Defense, the Attorney General and the Director of Central Intelligence submit a joint, detailed report to Congress within ninety days or face a cutoff of funding. These restrictions on TIA were originally proposed by Senator Wyden. The required report on TIA programs is to:

- explain and show planned spending and schedules for each TIA project and activity;
- identify target dates for deployment of each component;
- evaluate the system's likely effectiveness in predicting terrorist activities;
- assess the likely impact of implementation on privacy and civil liberties;
- list laws and regulations governing collection efforts and identify any changes that would be needed with deployment of TIA; and

[409] DOD Regulation 5241.1-R, Procedure 2 lists 13 types of information about U.S. persons that DOD intelligence components are permitted to collect: information obtained with consent, that is publicly available, foreign intelligence, counterintelligence, sources that could assist intelligence, sources that could help identify or protect intelligence information, information about potential suspects threatening DOD security, personnel security investigations, communications security investigations, narcotics suspects, threats to safety, information available from general overhead reconnaissance, and collected for administrative purposes. See following web site for this and related regulations: [http://www.dtic.mil/whs/directives/corres/pdf/d52401_042588/d52401p.pdf].

[410] DOD Briefing Transcript, November 20, 2002; [http://www.defenselink.mil].

- include recommendations from the Attorney General about procedures, regulations or legislation that would eliminate or minimize adverse effects of any TIA programs on privacy and civil liberties.[411]

If no report is submitted, the funding cutoff can be avoided if the President certifies in writing to Congress that submitting the report is not practicable and that ending R& D on Total Information Awareness programs would endanger national security.

In addition, the provision requires that DOD notify Congress and receive specific appropriations and authorization for any deployment or transfer to another federal agency of any TIA component unless the component is to be used for overseas military operations or for foreign intelligence activities conducted against non-U.S. persons.[412]

Other Members of Congress have also signaled concerns about the TIA system. On January 16, 2003, Senator Feingold and others introduced S. 188, the Data Mining Moratorium Act of 2003 that would place restrictions on data mining activities in DOD and other agencies. In November 2002, Senator Grassley asked the DOD Inspector General to conduct an audit of TIA programs and asked Attorney General Ashcroft to provide by February 10, 2003 information about any involvement that the Department of Justice or the FBI have had with the TIA program. Senator Grassley has not yet received a reply.[413]

Issues for Congress

In addition to concerns raised by members of Congress and public interest groups about protecting the privacy of U.S. citizens, Congress may continue to address oversight issues, including:

- developing monitoring mechanisms for TIA programs; and
- assessing the technical feasibility of the program.

---

[411] See Division M, Section 111 of H.J.Res. 2 in Congressional Record, February 12, 2003, Part Two.

[412] The final version changes the original Wyden amendment (SA59) by extending the amount of time for submission of the report from sixty to ninety days and by clarifying that TIA components could be used in the U.S. if they were applied to non-U.S. persons. See Congressional Record, January 17, 2003, p. S1165 for original version of the Wyden amendment; compare to H.Rept. 108-10 on H.J.Res. 2, FY2003 Consolidated Appropriations Resolution in Congressional Record, February 12, 2003, Book Two. For the changes to the Wyden amendment, compare Division M, Section 111 (a) (1) and (c) (2) (B).

[413] Senator Chuck Grassley, Press Release, January 21, 2003, and conversation with Judiciary Committee staff, March 12, 2003.

Monitoring TIA Programs

DARPA suggests that its role in developing prototype technologies for a TIA system is consistent with both its mission and history of sponsoring basic research for the mid and long-term that crosses service lines, and has multiple potential users, both inside and outside DOD. Previous examples of DARPA-developed technology with wide-ranging implications include stealth technology, Global Positioning System (GPS), and development of the Internet.[414] Based on recent testimony by Assistant Secretary of Defense Paul McHale emphasizing that DOD did not expect to use a TIA system but would turn the system over to civilian law enforcement agencies, TIA may not have a defense mission.[415] In describing plans for the TIA system, DARPA's Director, Dr. Tony Tether, cited collaboration with potential users in other federal agencies as a key part of their approach.[416]

Yet that collaboration – between the law enforcement community and the intelligence community, for example – has raised concerns among some observers about the roles of different agencies in gathering and sharing intelligence on potential threats from terrorists located in the United States. Those concerns reflect the experiences of the 1960s and 1970s when the FBI's counterintelligence program targeted civil rights and anti-war organizations as part of its efforts to pursue domestic terrorists.[417]

DARPA's efforts at collaboration reflect the fact that there are potentially many users of any tools that DARPA develops to predict terrorist threats. Currently, several agencies are or will be collecting or analyzing intelligence on potential terrorist threats, including the Counterterrorist Center under the CIA, the FBI's Joint Terrorist Task Forces, the new Department of Homeland Security. Another new user would be President Bush's proposed new Terrorist Threat Integration Center to be established May 1, 2003 with the mission of integrating all of U.S. government information and analysis about potential terrorist threats.[418] DARPA envisions working with potential users in the design of its tools for decision

---

[414] Tether briefing, January 2003.

[415] Testimony of Paul McHale before the Subcommittee on Special Oversight Panel on Terrorism, Unconventional Threats and Capabilities, House Armed Services Committee, Hearing on Force Protection, March 13, 2003.

[416] Briefing by Dr. Tony Tether, Director, DARPA to Congressional staffers, "DARPA's Information Technology Initiative on Countering Terrorism, January 27, 2003.

[417] Markle Foundation report, " A Primer on the Changing Role of Law Enforcement and intelligence in the War on terrorism," by Robert M. McNamara, Jr., p. 85.

[418] See CRS Report RS21283, Homeland Security: Intelligence Support by Richard Best.

makers, a practice, that could be difficult with restrictions on transfer of TIA components.

Sharing information among several users makes it more difficult to protect both intelligence sources and the privacy of individuals. For that reason, DARPA is sponsoring some research on developing 'fire walls' that would protect the sources of intelligence gatherers and prevent potential leakage among users. The distributed type of system that DARPA envisions could make those challenges greater. Early collaboration with potential users, for which DARPA has been praised, could also create problems with ensuring privacy and preventing misuse of intelligence sources and data on individuals, particularly if DARPA tries to exploit multiple data bases and to share data across agencies.[419]

Developing tools to ensure that the privacy of both sources and individuals is both a technical challenge and a policy issue. DARPA's Genisys program, a TIA component intended to integrate and query large data bases that has raised privacy concerns, also includes R&D on tools to ensure privacy. These tools may include "partitioning," which segregates transactions from the identity of the individual, filters to limit access to information and software agents that would delete unrelated information. According to a technical group tasked by DARPA to look into technological solutions to privacy issues, the Information Science and Technology panel (ISAT), there are significant difficulties in developing tools and protocols to protect privacy. This group called on DARPA to devote significant research resources in this area, and to establish a citizen advisory board to privacy policy standards.[420]

On February 7, 2003, the Department of Defense established two boards to monitor TIA programs.[421] Made up of high-level DOD officials, the internal TIA oversight board is tasked with setting policies and procedures for use of TIA tools within DOD and establishing protocols for transferring TIA capabilities outside of DOD to ensure consistency with privacy laws and policies. DOD also established an outside advisory board including experts in privacy issues, to advise the Secretary of Defense on policy and legal issues raised by using advanced technology to identify and predict terrorists threats.[422] In separate statements to

---

[419] Report of the Markle Foundation Task Force, Protecting America's Freedom in the Information Age, October 2002, p. 14-15, 22, 26, and 27.

[420] Information Science And Technology (ISAT) study Group, Security with Privacy, 13 December 2002.

[421] See, DOD Press Release, " Total Information Awareness Update, February 7, 2003; see [http//www.defenselink.mil/news/Feb2003/b02072003_bt060-03.html].

[422] DOD Press Release, "Total Information Awareness (TIA) Update," February 7, 2003. Members of the advisory board would be Newton Minow, Northwestern University, Zowe Baird, president Markle Foundation, Floyd Abrams, civil rights attorney, Gerhard Casper, Former president of

reporters, Senator Wyden and a spokesman for the American Civil Liberties Union each suggested that the new boards proposed by the Pentagon did not eliminate the need for Congressional oversight."[423]

P.L. 108-7, passed by both houses the following week, requires that DOD inform and get Congressional authorization for any transfers between agencies or for deployment of any TIA components. Under P.L. 108-7, testing outside of DOD may also be subject to rigorous oversight. In its current research, DARPA has been careful to use 'dummy' or fictitious data on individuals to test the effectiveness of various models for detecting potential terrorists, or to use only data that is currently legally permissible for intelligence gathering purposes (see discussion of ongoing DARPA collaboration above). If DARPA's technology efforts - in data mining or model development - are to be fully tested, however, real data, with all its flaws, may need to be used, and using real data may raise privacy issues. To decrease the potential for significant errors in the prototype models and systems under development, extensive testing efforts could be desirable.

Assessing Technical Feasibility

While some observers see great potential in DARPA's TIA proposals to exploit a wide range of data bases and develop models to identify terrorists, other observers are skeptical even models with sophisticated algorithms could pick terrorists out from large data bases, the proverbial problem of finding a needle in a haystack. DARPA's description suggests that the TIA system will be developed using a variety of data mining techniques coupled with models developed by analysts. Although there does not appear to be any simple definition, data mining has been defined as exploiting a variety of tools to extract predictive information from large data bases.[424]

Several major technical problems are inherent in data mining and model development that would need to be solved to develop an effective TIA system including:

- identifying and getting access to appropriate data bases;
- cleaning up "dirty" or inaccurate data in data bases;
- integrating disparate data bases;
- developing models or algorithms to identify likely terrorists;

Stanford University, Griffin Bell, former U.S. Attorney General and judge, William T. Coleman, CEO of BEA, Lloyd Cutler, former White House Counsel.

[423] New York Times, "Pentagon Forms 2 Panels To Allay Fears on Spying," February 8, 2003; Boston Globe, "2 Panels to Monitor Eavesdropping, Pentagon Hopes to Assuage Critics of Defense Plan," February 8, 2003.

[424] See Puhpa Ramachandran M, Mining for Gold, White Paper, December 2001.

- mis-identifying suspects because of large numbers of false leads; and
- dealing with timing and cost dilemmas.

Data Base Problems

Getting access, 'cleaning up,' and integrating large data bases may pose significant challenges in developing a TIA system. While DARPA is currently looking at links between military intelligence data and other sources at its Army testing site, there could be complications in linking to other data bases and ensuring that only permissible data is included.[425] In addition, any data base includes a significant number of errors – a problem routinely discussed by data mining experts – and it is not clear that there are adequate methods for catching errors. Linking large and disparate data bases is not only a challenging task in itself but could compound the number of errors.

Searching large data bases with large numbers of errors could both reduce the likelihood that terrorists would be identified and magnify the possibility that individuals who are not terrorists would be tagged. Erroneous data may be included either inadvertently by those entering the data or intentionally by "identity threat" where individuals deliberately impersonate others, worrisome problems to technical and privacy experts alike. The quality of the data could be diluted further if disparate data bases are linked.

Developing Ways To Identify Terrorists

DARPA plans to use both quantitative and qualitative data mining techniques to develop tools to identify terrorists. Data mining techniques are currently widely used for commercial purposes, ranging from targeted marketing to detecting credit card fraud, as well as for law-enforcement (e.g., to catch drug smugglers). In these cases, however, analysts and statisticians develop, test and re-test algorithms or quantitative relationships in order to hone formulas and improve their accuracy in detecting patterns. In the case of credit card fraud, for example, statistical algorithms or pattern identifying techniques can be refined with follow-up checks of billing records.

According to DARPA's descriptions, TIA components would develop technologies using both statistically-based algorithms to detect patterns in multiple data sources from a wide range of sources – financial, telephonic, foreign messages, intelligence traffic – and models of terrorist behavior based on analysis of historical experiences and scenarios developed by analysts. DARPA anticipates that by speculating, analysts will develop scenarios of particular terrorist attacks and then back into the types of activities that would be necessary to carry out those attacks. Some observers have suggested that it could be difficult to

---

[425] Letter from Barbara Simons, Ph.D., and Eugene H. Spafford, Ph.D, Co-Chairs, U.S. Association for Computing Machinery to Senators John Warner and Carl Levin, Senate Armed Services Committee, January 23, 2003. See [http://www.acm.org/usacm].

anticipate terrorist acts, and our success in anticipating previous terrorist attacks has been limited. With the enormous increases in the speed of processing information and the proliferation of data mining techniques, DARPA sees new opportunities for exploiting a variety of information sources using quantitative techniques like data mining.

Technology experts and others, however, have questioned whether the problem of detecting potential terrorists is susceptible to the data mining techniques routinely done by commercial companies in light of the difficulty in predicting terrorist behavior. The problem is made all the more difficult by the likelihood that the number of Al Qaeda members in the U.S. is small; a widely-quoted FBI estimate of 5,000 was later dismissed as too high, a small number compared to the large number of transactions that are analyzed in commercial data mining applications.[426]

In response, DARPA suggests that its research would not simply search data bases for potential terrorists but instead would develop templates, based on studies of past attacks and captured terrorists documents, that would be used to focus searches of databases more narrowly. In addition, the process would be iterative, in other words, analysts would use a variety of techniques, sequentially, to identify potential terrorists.[427]

The Problem of False Leads

A key element in assessing the viability of the TIA system is whether the technologies developed will be sufficiently accurate to limit the number of potential suspects and minimize the number of false leads so as to avoid misidentifying individuals as suspects.[428] If the number of potential suspects or false leads proves to be large, the timeliness of warnings, as well as the cost of conducting followup checks, could also make a TIA system problematic. Some observers are also concerned that if DOD or intelligence agencies identified significant numbers of false leads, the pressures of time and urgency could lead to violations of the rights of individuals.

DARPA contends that concerns about false leads (called false alarms or "false positives" by statisticians) are exaggerated. In credit card fraud, for example, a false alarm or false positive would mistakenly identify a transaction as fraudulent. To avoid false alarms, DARPA argues that a TIA system would use multiple means to identify suspects, ranging from models developed by "Red

---

[426] New York Times, "5,000 Al Qaeda Operatives in The U.S.," February 16, 2003.

[427] Briefing to Congressional Staff by Dr. Tony Tether, DARPA, January 2003.

[428] Shane Harris, Government Executive, "Total Information Awareness official responds to criticism," January 31, 2003.

Teams" envisioning terrorist scenarios to patterns detected by linking intelligence data with commercially developed data mining techniques. Using such a tiered approach, DARPA contends that suspects would only be tagged after multiple checks.

Some observers have questioned whether these techniques could successfully cull the number of suspects. But assuming that DARPA's approach could reduce the number, capturing a certain number of false leads is inherent in statistical techniques. For example, consider the extensive work of the credit card industry in developing techniques to identify credit card fraud. In a controlled trial, researchers tested the effectiveness of combining several statistical tools to identify credit card fraud using a large, real testing sample of 500,000 transactions, deliberately seeded with 100,000 fraudulent transactions in order to refine statistical algorithms.[429] (See Table 3).

The researchers found that by combining several statistical tools, they could catch about 50% of the actual fraudulent transactions with a false alarm rate of about 20%. In other words, while 50,000 of the fraudulent cases were identified, (50% of 100,000), another 80,000 cases were mistakenly tagged as fraudulent (20% of 400,000 legitimate transactions) at the same time. Investigators therefore would need to investigate 130,000 cases to catch 50,000 wrongdoers, or about 2.6 cases for every 1 wrongdoer. In the case of credit card fraud, algorithms have been extensively refined using large amounts of real data, and followup checks on leads are routine as anyone who has received a phone call after making an unusually large charge knows.

Even in the case of credit card fraud, however, the incidence of wrongdoers is likely to be below 20%. (The actual fraud rate is a closely-guarded industry secret.) When the incidence of fraud is lower, the chances of identifying wrongdoers decrease.[430] Press reports last summer cited an FBI estimate of 5,000 Al Qaeda operatives in the U.S., but that estimate was later dismissed by the government, and experts suggested that hundreds rather than thousands was the more likely number.[431] In light of the relatively small number of terrorists, the likelihood of catching them, even with targeted data bases, could be far lower.

---

[429] Researchers have to know the composition of the data in order to test the effectiveness of their tools. These examples were developed by CRS with the help of a member of the Association for Computing Machinery using the article, Stolfo, Fan, Prodromidia, and Chan, "Credit Card Fraud Detection Using Meta-Learning: Issues and Initial Results; " see paper on following web site: [http://www.cs.fit.edu/~pkc/papers/].

[430] Ibid. In this research case, the fraud catching rate drops from 80% to 50% when the incidence of fraud decreases from 50% to 20%.

[431] New York Times, "5,000 Al Qaeda Operatives in The U.S," February 15, 2003, and Washington Times, "5,000 in U.S. Suspected of Ties to Al Qaeda," July 11, 2002.

The chance, as well as the cost to individuals of mis-identifying suspects, could also be far greater.

An illustrative case using statistical algorithms to identify terrorists that would increase the chances that a TIA system would work could be based on the following assumptions:

- the data base would be limited to 1,000,000 transactions because DARPA had successfully culled the number of suspects; and
- there are 5,000 terrorists in the data base, an incidence rate of 1/2 %.

The number of terrorists to be identified would then be 5,000 (1/2% of 1,000,000).

At the same time, assume optimistically that a combination of data mining and modeling tools could identify 30% or 1,500 of the 5,000 terrorists but that the false alarm rate was 30% because the difficulty of identifying terrorists is greater than detecting credit card fraud. In this case, investigators would need to check a total of 300,000 cases to catch the 1,500 terrorists (30% of 5,000 terrorists + 30% of 995,000 other suspects). For every terrorist identified, some 200 other suspects would have to be investigated.

Some computer experts think that even this case is optimistic. If DARPA's data base was larger, the number of false alarms could be far greater, even with a high accuracy rate. In examples proposed by computer experts that assumed a highly accurate TIA system was applied to the entire U.S. population, the number of false alarms could be 3 million people annually.[432] Either case would pose considerable challenges to investigators, particularly in cases where a threat was considered imminent. If the number of potential suspects identified was significant, the cost of implementing the system could also grow, as substantial personnel would be needed to investigate potential leads and ensure that false leads were eliminated.

Appendix: Description of R&D Efforts Managed by the Information Awareness Office By Category

(* = R&D efforts specifically linked to the TIA system by DARPA)

Data Mining Technologies

- **Human Identification at a Distance (HumanID).*** This project aims to use information from sensors about human characteristics such as

---

[432] See Letter from Barbara Simons, Ph.D., and Eugene H. Spafford, Ph.D, Co-Chairs, U.S. Association for Computing Machinery to Senators John Warner and Carl Levin, Senate Armed Services Committee, January 23, 2003; see [www.acm.org/usacm/].

gait or face, to identify individuals at any time of the day or night and in all weather conditions, for instance, within a large crowd.

- **Evidence Extraction and Link Discovery (EELD).*** This project is an effort to identify terrorist groups by developing a suite of technologies to detect patterns between people, organizations, places and things from intelligence messages and law enforcement records, and then use those patterns or links to gather additional information from vast amounts of textual or transactional data including web sites, sensor data, and news reports.
- **Genisys.*** This project is a new effort in 2003 to put together old and new databases so that they can be readily queried. This "ultra-large all-source information repository" could include information about potential terrorists and possible supporters, purchase of terrorist types of material, training and rehearsal activities, potential targets, and status of defenses, as well as research into methods of protecting privacy.[433]
- **Bio-surveillance (re-named Bio-ALIRT IN FY2004):*** This project is an effort to collect and analyze information from non-traditional human, agricultural and animal health data bases in order to develop indicators and models, and set up a prototype bio-surveillance system for a citywide area like Norfolk, Virginia to increase DOD's ability to detect a clandestine biological warfare attack.

Machine Translation Projects

- **Translingual Information Detection, Extraction and Summarization (TIDES).*** TIDES is designed to get critical information quickly for intelligence analysts and operators by developing tools that can rapidly find, summarize, and translate key information in foreign languages.
- **Effective Affordable Reusable Speech-to-Text (EARS)**: Anticipated to increase the speed of translation from oral sources by ten to 100-fold (including broadcasts and telephone), as well as extract clues about the identity of speakers, EARS is intended to serve the military, intelligence and law enforcement communities.
- **Multispeaker Environments (MUSE) and Global Autonomous Language Exploitation (GALE)**: MUSE and GALE are successor programs to EARS. MUSE is to produce transcripts from command centers and meeting rooms and GALE is to develop techniques for detecting key intelligence in massive amounts of foreign language transmissions.

---

[433] Department of Defense, FY2003 Budget Estimate, Research, Development, Test and Evaluation, Defense-wide, Volume 1, Defense Advanced Research projects Agency, February 2002; web site address above.

- **Communicator**: Designed to enable military personnel to get logistical support and tactical information when in the field, prototypes of this "smart phone" have already been deployed on Navy ships.
- **Babylon**: Another battlefield system likely to be deployed in Afghanistan in the next few months, Babylon is intended to aid those in the field by translating foreign phrases for the service member.[434]

Protection of Critical Information Infrastructure

- **DefenseNet (DNET)**: This effort is intended to increase the security and performance of DOD's information infrastructure in handling large volumes of information.
- **Mis-Information Detection and Generation (MIDGET)**: A new project in 2003, this effort is designed to detect and reduce DOD's vulnerability to mis-information about adversaries that appears in open-source data.

Tools for High-Level Decision Makers

- **Rapid Analytic Wargaming (RAW)**: This project is intended to develop gaming technologies that simulate asymmetric threats to be used by the major commands in training and operational settings.
- **War Gaming the Asymmetric Environment (WAE).*** This effort is an initiative to develop tools and models to help analysts and decision makers predict the behavior and the reactions of terrorists to U.S. actions.
- **GENOA/GENOA II:*** Project Genoa attempts to improve collaborative reasoning, estimate plausible futures, and create actionable options among intelligence analysts in various organizations. Genoa II seeks to enhance collaboration between people and machines in order to improve support provided by intelligence analysts to policymakers at the military command level, to high level DOD civilian officials, NSA and the Joint Chiefs of Staff for dealing with terrorist threats.
- **Total Information Awareness.*** TIA is to integrate some or all of the efforts above into a prototype system or systems that would create and exploit large-scale, counter-terrorist data bases, develop new analytical techniques and models for mining those data bases so as to improve our ability to detect, anticipate, pre-empt, and respond to terrorist attacks. R&D efforts specifically linked to the TIA system in FY2003 are Human ID at a Distance, EELD, Genisys, Bio-surveillance, TIDES, WAE, Project Genoa and Genoa II, and the TIA integrative effort.

---

[434] Although Communicator and Babylon are primarily battlefield systems, some elements may be incorporated into the TIA system.

Terrorist Identification, Screening, and Tracking Under Homeland Security Presidential Directive 6, RL32366 (April 21, 2004).

WILLIAM J. KROUSE, CONGRESSIONAL RESEARCH SERV., TERRORIST IDENTIFICATION, SCREENING, AND TRACKING UNDER HOMELAND SECURITY PRESIDENTIAL DIRECTIVE 6 (2004), *available at* http://www.intelligencelaw.com/library/secondary/crs/pdf/RL32366_4-21-2004.pdf.

Order Code RL32366
April 21, 2004

William J. Krouse
Analyst in Social Legislation
Domestic Social Policy Division

Summary

In Homeland Security Presidential Directive 6 (HSPD-6), the Administration announced plans to establish a Terrorist Screening Center (TSC), as a multi-agency effort to be administered by the Federal Bureau of Investigation (FBI), where several watch lists are being consolidated into a single terrorist screening database (TSDB). The TSC is the latest of three multi-agency efforts undertaken by the Administration to better identify, screen, and track known terrorists, suspected terrorists, and their supporters. The other two are the Foreign Terrorist Tracking Task Force (FTTTF) and the Terrorist Threat Integration Center (TTIC). According to the Administration, the TSC complements the FBI-led FTTTF's efforts to prevent terrorists from entering the United States, and to track and remove them if they manage to enter the country. The TTIC serves as a single locale where terrorism-threat data from all sources are further analyzed to more critically focus on terrorism.

Certain terrorist identification and watch list functions previously performed by the Department of State's Bureau of Intelligence and Research (INR) have been transferred to the TTIC and TSC under HSPD-6. At the TTIC, intelligence analysts are building a Terrorist Identities Database (TID) based on TIPOFF — the U.S. government's principal terrorist watch list database prior to HSPD-6. From TID records, TSC analysts are building a consolidated TSDB. The Administration plans to widen access to, and use of, lookout records by making them available in a "sensitive but unclassified" format to authorized federal, state, local, territorial and tribal authorities; to certain private sector entities; and to certain foreign governments.

Merging watch lists will not likely require integrating entire systems, but there are likely to be technological impediments to merging watch list records. From

system to system, and watch list to watch list, there remains no standardization of data elements, such as, name, date of birth, place of birth, nationality, or biometric identifiers. While elevating and expanding the terrorist identification and watch list function is an important step in the wider war on terrorism, additional work will remain to upgrade and integrate other consular and border management systems, criminal history record systems, and biometric systems.

HSPD-6 presents significant opportunities to more effectively share data and increase security, but there are risks as well, not the least of which is the potential loss of privacy and the erosion of civil liberties. In recent hearings, Members of Congress have raised several related issues. For example, is the TSDB fast, accurate, comprehensive, and accessible? Have procedures been established to allow persons, who may be misidentified as terrorists or terrorist supporters, some form of redress and remedy if they are denied civil rights or unduly inconvenienced by a screening agency? Does the establishment of the TSDB require new guidelines and oversight mechanisms to protect privacy and other civil liberties? Or, are existing agency policies under which such data is collected sufficient? Is the FBI the best agency to administer the TSDB? Are the TSC and TSDB, and by extension the TTIC, temporary or permanent solutions? This report will be updated as needed.

Introduction

This report analyzes Homeland Security Presidential Directive 6 (HSPD-6) and issues relating to (1) the establishment of a Terrorist Screening Center (TSC), (2) the transfer of certain terrorist identification and lookout record distribution functions from the Department of State to the Terrorist Threat Integration Center (TTIC) and the TSC, and (3) the consolidation of terrorist watch lists into a single, stand-alone, terrorist screening database (TSDB) under the direction of the Federal Bureau of Investigation (FBI) at the TSC. In recent hearings, Members of Congress have raised several issues regarding the establishment of the TSDB. For example,

- Has the Administration committed enough resources to ensure the timely establishment of an integrated terrorism watch list (the TSDB)?
- Is the TSDB fast, accurate, comprehensive, and accessible?
- Have procedures been established to allow persons, who may be misidentified as terrorists or terrorist supporters, some form of redress and remedy if they are denied civil rights or unduly inconvenienced by a screening agency?
- Does the establishment of the TSDB require new guidelines and oversight mechanisms to protect privacy and other civil liberties? Or, are existing agency policies under which such data is collected sufficient?
- Is the FBI the best agency to administer the TSDB?
- Are the TSC and TSDB, and by extension the TTIC, temporary or permanent solutions?

While this report identifies some privacy issues associated with the establishment of a consolidated terrorist screening database, it is not intended to serve as an in-depth legal analysis of the issues related to national security, privacy, and the government's need for information to combat terrorism. Rather, it is a systematic examination of the mission and functions of the TSC in relation to other entities like the TTIC. It also identifies and describes key watch lists, residing in several computerized systems and databases,[435] that likely will be consolidated at the TSC.

HSPD-6 and Terrorist Watch List Consolidation

In HSPD-6[436] and an accompanying memorandum of understanding (MOU),[437] the Administration announced plans to establish the TSC, as a multi-agency effort to be administered by the FBI, where several watch lists will be consolidated into a single terrorist screening database (TSDB).[438] The *MOU on the Integration and Use of Screening Information to Protect Against Terrorism* was signed by Secretary of State Colin Powell, Attorney General John Ashcroft, Secretary of Homeland Security Thomas Ridge, and Director of Central Intelligence (DCI) George Tenet on September 16, 2003. The measures outlined in HSPD-6 and the MOU can be viewed as an outgrowth of the Administration's National Strategy for Homeland Security, which reported in July 2002 that the

---

[435] A computer system is composed of computer(s), peripheral equipment such as disks, printers and terminals, and the software necessary to make them operate together (according to the American National Standards Institute/Institute of Electrical and Electronic Engineers (ANSI/IEEE) Standard 729-1983). A database is an organized body of machine readable data that can be cross-referenced, updated, retrieved, and searched by computer.

[436] The White House, Homeland Security Presidential Directive/HSPD-6, Subject: Integration and Use of Screening Information (Washington, Sept. 16, 2003). Available at [http://www.whitehouse.gov/news/releases/2003/09/20030916-5.html].

[437] The Terrorist Screening Memorandum of Understanding accompanying HSPD-6 is available at [http://www.fas.org/irp/news/2003/09/tscmou.pdf].

[438] Presidents may exercise executive authority by issuing various kinds of directives. Among the oldest of these are executive orders and proclamations, both of which today are usually published in the Federal Register. For example, President George W. Bush established the Office of Homeland Security and the initial Homeland Security Council with E.O. 13228 of Oct. 8, 2001. With the establishment of the National Security Council in 1947, there have emerged a series of variously denominated national security directives, but these are not published. Recently, President Bush inaugurated a similar series of Homeland Security Presidential Directives, the first such being issued on Oct. 29, 2001. While these homeland security directives are not published in the Federal Register, they are available from the White House Website and appear in the Weekly Compilation of Presidential Documents. For further information see CRS Report 98-61, Presidential Directives: Background and Overview, by Harold C. Relyea.

FBI would be establishing a consolidated terrorism watch list that would be "fully accessible to all law enforcement officers and the intelligence community."[439]

According to the Administration's timetable, the TSC was to be operational on December 1, 2003.[440] According to press accounts, however, the Administration informed Representative Jim Turner, the ranking member of the Select Committee on Homeland Security, that the TSC was not "fully" operational as of the end of December 2003 and that the Nation's multiple terrorist watch lists have yet to be consolidated.[441] On March 25, 2004, the TSC Director — Donna Bucella — testified that the TSC had established an unclassified, but law enforcement sensitive TSDB. In addition, the TSC was assisting federal screening agencies in identifying terrorists and their supporters with greater certainty, and TSDB lookout records had been made available to nearly 750,000 state and local law enforcement officers.[442]

The TSC is the latest of three multi-agency efforts undertaken by the Administration to better identify, screen, and track known terrorists, suspected terrorists, and their supporters. The other two are the FTTTF and the TTIC. According to the Administration, the TSC complements the FBI-led FTTTF's efforts to prevent terrorists from entering the United States, and to track and remove them if they manage to enter the country. Under the oversight of the DCI, the TTIC serves as a single locale where terrorism-threat data from all sources, foreign and domestic, are further analyzed to more critically focus on terrorism. As part of that function, under HSPD-6, the TTIC will assume a greater role in identifying individuals who are known, or suspected, to be terrorists, or their supporters.

The Administration has transferred certain terrorist identification and watch list functions previously performed by the Department of State's (DOS's) INR to the TTIC and TSC. Through a system known as TIPOFF, the DOS's INR identified known and suspected terrorists, produced lookout records, and distributed those records for inclusion in consular and border inspection systems. Prior to HSPD-

---

[439] The White House, Office of Homeland Security, National Strategy for Homeland Security (July 2002), p. 57.

[440] The White House, Fact Sheet: New Terrorist Screening Center Established (Washington, Sept. 16, 2003), at [http://www.whitehouse.gov/news/releases/2003/09/20030916-8.html].

[441] Chris Strohm, "Congressman Blasts Bush on Terrorist Screening Efforts," Government Executive Magazine, Jan. 13, 2004, at [http://www.govexec.com/dailyfed/0104/011304c1.htm].

[442] This testimony was given by TSC Director Donna Bucella on Mar. 25, 2004, before a joint hearing held by the House Judiciary Subcommittee on Crime, Terrorism, and Homeland Security and the Select Homeland Security Subcommittee on Intelligence and Counterterrorism.

6, TIPOFF was the Nation's principal terrorist watch list.[443] Based in part on TIPOFF, the member agencies of TTIC have built a TID into which all international terrorist-related data available to the U.S. government will be stored in a single repository.[444] With TID records, the TSC is building a consolidated international terrorist watch list, which will be merged with domestic terrorist watch list records, in the TSDB.

Under HSPD-6 the Administration plans to widen access to, and use of, watch list records by making them available in a "sensitive but unclassified"[445] format to authorized federal, state, local, territorial and tribal authorities; to certain private sector entities; and to certain foreign governments.

Hence, HSPD-6 has elevated and expanded the terrorist identification and watch-list functions, which were previously performed by the DOS's INR for immigration-screening purposes. Moreover, under HSPD-6, the use of watch lists will be expanded to include data taken from on-going criminal and national security investigations that are related to terrorism. The purpose of these measures is to better identify, watch-list, and screen known and suspected terrorists at U.S. consulates abroad and international ports of entry. Such measures could also better enable the

U.S. government to track terrorists within the United States if they manage to enter the country. Yet, at the same time, there are significant risks as well, not the least of which is the potential loss of individual privacy and an erosion of civil liberties. In the Intelligence Authorization Act for Fiscal Year 2004,[446] Congress

---

[443] Watch lists are just that, lists of persons who are of interest to visa issuance and border inspection agencies or law enforcement. Persons may be on watch lists to prevent them from acquiring a visa or to prevent them from entering the country, or both. Persons can be excludable from entry for reasons ranging from public health concerns to tax-motivated citizen renunciates, in addition to being known and suspected terrorists, or their supporters. They may also be wanted by law enforcement agencies for questioning or arrest.

[444] The TID is nearly identical to the system that section 343 of the Intelligence Authorization Act for Fiscal Year 2003 (P.L. 107-306, 116 Stat. 2399) required the DCI to establish.

[445] There is no governmentwide definition of "sensitive but unclassified (SBU)." Within certain limits set out in statutes and presidential directives, agencies have discretion to define SBU in ways that serve their needs to safeguard information that is unclassified but should be withheld from the public for a variety of reasons. The reasons for safeguarding such information, are likely to include maintaining the privacy rights of individuals and the integrity of ongoing inquiries and investigations. A provision in the Homeland Security Act of 2002 (§892 of P.L. 107-296, 116 Stat. 2253) requires the President to implement procedures to safeguard SBU information that is homeland security-related. For further information, see CRS Report RL31845, "Sensitive But Unclassified" and Other Federal Security Controls on Scientific and Technical Information: History and Current Controversy, by Genevieve J. Kneso.

[446] P.L. 108-177, Stat. 2622-2625.

has required the President to report back to Congress on the operations of both the TTIC and TSC.

Terrorist Watch-Listing Prior to HSPD-6

A primary goal of lookout systems and watch lists has been to prevent terrorist attacks, by excluding known or suspected terrorists and their supporters from entry into the United States. Under HSPD-6, the use of watch lists would be expanded to better screen such persons at consular offices and international ports of entry, and to better track them both abroad and, if they manage to enter the United States, at home.

Watch Lists and Lookout Books

The DOS's Bureau of Consular Affairs (CA) and the federal border inspection services, until recently the U.S. Customs Service and the Immigration and Naturalization Service (INS), have long maintained watch lists (or lookout books) for the purpose of excluding "undesirable" persons from the United States. Customs and immigration inspection activities are now carried out by the Bureau of Customs and Border Protection (CBP) at the Department of Homeland Security (DHS).[447] While these watch lists/lookout books were just that— bound paper volumes — the development of computers, computer software, and computer connectivity/networking, allowed these agencies to develop and more efficiently search watch list records during the 1970s and 1980s. Beginning in 1987, the DOS began keeping watch list (lookout) records on known and suspected terrorists through a system known as TIPOFF. While the DOS had maintained computerized visa records since 1965, including watch lists, the events surrounding the first World Trade Center bombing in 1993 prompted the CA to accelerate the development of the Consular Lookout and Security System (CLASS), so that, among other records, TIPOFF-generated terrorist watch list records could be more easily and efficiently searched by computer at U.S. consular posts and embassies abroad. Consular, intelligence, immigration, and law enforcement officers nominate individuals for inclusion in TIPOFF.

The INS, meanwhile, maintained its own watch list database known as the National Automated Immigration Lookout System II (NAILS II) — a system that is currently maintained by the DHS's Bureau of Immigration and Customs

---

[447] Until the establishment of DHS, federal border inspection services included the Department of the Treasury's Customs Service, the Department of Justice's INS, the Department of Agriculture's Animal and Plant Health Inspection Service (APHIS), and the Department of Health and Human Service's Public Health Service. The Homeland Security Act dismantled INS and transferred its constituent parts, along with Customs and elements of APHIS, to DHS. The border inspection programs of these agencies have been consolidated in DHS's Border and Transportation Security Directorate, as the CBP.

Enforcement (ICE).[448] While the bulk of NAILS II records are related to aliens who have either been removed, failed to depart, or failed to show up for removal hearings, NAILS II includes terrorism-related lookouts as well.

In 1988, Congress mandated the development of the Interagency Border Inspection System (IBIS). This system, previously maintained by the Customs Service, allowed the DOS, INS, and Customs to share watch lists, including terrorist lookout records, at international ports of entry. This system is currently maintained by the DHS's CBP.

Prior to HSPD-6, DOS's INR culled through terrorism-related reports produced by the Intelligence Community[449] to identify individuals as known or suspected terrorists, or their supporters. INR also processed cables — known as Visa Vipers — from consular officers abroad when they learn of individuals associated with terrorism. And, INR processed similar data provided by federal law enforcement agencies to produce terrorism-related lookout records. These records were stored in TIPOFF — a classified system. Declassified TIPOFF records were then exported into CLASS, IBIS, and NAILS II. Also, lookout records produced by immigration officers were exported from NAILS II into TIPOFF. See Figure 1 below.

As underscored in recent public testimony, however, watch lists were only as good as the information contained in them, and the agencies responsible for producing these lookout records — principally DOS's INR and DOJ's INS — were dependent upon the information they received from the Intelligence Community and federal law enforcement.[450]

---

[448] Following the establishment of the DHS, pursuant to P.L. 107-296 (116 Stat. 2135), the Administration merged the investigation branches of the former INS and Customs Service into ICE, along with the immigration detention and removal program, Customs Air and Marine Interdiction program, and the Federal Protective Service. More recently, the Air Marshals program was transferred from the Transportation Security Administration (TSA) to ICE.

[449] The Intelligence Community includes the Central Intelligence Agency (CIA); the National Security Agency (NSA); the Defense Intelligence Agency (DIA); the National Geospatial-Intelligence Agency (GIA); the National Reconnaissance Office (NRO); the other DOD offices that specialize in national intelligence through reconnaissance programs; the intelligence components of the Army, Navy, Air Force, Marine Corps, and Air Force, the FBI, the Department of Energy, and the Coast Guard; the INR at the DOS, the Office of Intelligence and Analysis at Department of the Treasury, and elements of the DHS that are concerned with the analyses of foreign intelligence information (50 U.S.C. §401a(4)).

[450] See testimony of Mary Ryan, former Assistant Secretary of State for Consular Affairs, Department of State, and Doris Meissner, former Commissioner, Immigration and Naturalization Service, Department of Justice, before the National Commission on Terrorist Attacks upon the United States, Jan. 26, 2004. At [http://www.9-11commission.gov/hearings/hearing7.htm].

Terrorism-Related Ground for Inadmissability

According to the U.S. government, the term "terrorism" means "the premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents, usually intended to influence an audience."[451] Prompted by the assassination of President William McKinley in 1901, Congress passed legislation in 1903 to exclude from entry into the United States noncitizens who were anarchists, or who advocated the violent overthrow of the U.S. government.[452] As a security measure during the First World War, the DOS and Department of Labor (DOL)[453] jointly issued an order in 1917, which required noncitizens to acquire visas from U.S. Consuls abroad and present their visas and passports to U.S. inspectors upon arrival in the United States. This wartime requirement was codified in 1918,[454] and was made a permanent feature of U.S. immigration law in 1924.[455] This requirement was continued by the Immigration and Nationality Act (INA) of 1952.[456]

Visa issuance has long been viewed as a means of preventing undesirable persons, including suspected spies, saboteurs and subversives, from entering the United States. In the Immigration Act of 1990, Congress amended and substantially revised the grounds for exclusion in the INA, including new provisions related to the exclusion of terrorists from the United States.[457] These terrorist exclusion provisions were subsequently amended and widened by the

---

[451] This definition of "terrorism" is taken from 22 U.S.C. §2656f(d). U.S. Department of State, Patterns of Global Terrorism 2002 (Washington, Apr. 2003), p. xiii.

[452] P.L. 57-162, 32 Stat. 1213.

[453] In 1891, Congress established the office of Superintendent of Immigration in the Department of the Treasury. The immigration functions remained at Treasury until 1903, when they were transferred by Congress to the Department of Commerce and Labor. In 1906, the immigration and naturalization functions were consolidated in the Bureau of Immigration and Naturalization. In 1913, Congress transferred the Bureau to the newly established DOL, splitting the immigration functions between a Bureau of Immigration and a Bureau of Naturalization. The immigration and naturalization functions were combined again in 1933, as the Immigration and Naturalization Service (INS). In 1940, President Franklin Delano Roosevelt transferred INS to the Department of Justice. The Homeland Security Act of 2002 (P.L. 107-296) abolished INS, transferring its immigration functions to the DHS.

[454] Act of May 22, 1918, 40 Stat. 559.

[455] Act of May 26, 1924, 43 Stat. 153, 156, 161.

[456] INA §§211, 212(a)(7), 221, 8 U.S.C §§1181, 1182(a)(7), 1201.

[457] INA §212(a)(3)(B)(i), 8 U.S.C. §1182(a)(3)(B)(i), as amended by the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001 (P.L. 107-56).

Antiterrorism and Effective Death Penalty Act[458] and the Illegal Immigration and Immigrant Responsibility Act in 1996,[459] and by the USA PATRIOT Act in 2001.[460]

Under the INA, an alien is inadmissible if there is reasonable ground to believe the alien (1) has engaged in terrorist activity; (2) is engaged or is likely to engage in terrorist activity; (3) has, under certain circumstances, indicated an intention to cause death or serious bodily harm, or incited terrorist activity; (4) is a representative of a foreign terrorist organization designated by the Secretary of State, or a political, social, or other similar group whose public endorsement of acts or terrorist activity the Secretary of State has determined undermines U.S. efforts to reduce or eliminate terrorist activities; (5) is a member of a foreign terrorist organization designated by the Secretary of State; or (6) has used his/her position of prominence within any country to endorse or espouse terrorist activity, in a way that the Secretary of State has determined undermines United States activity to reduce or eliminate terrorism activities.[461]

Diplomatic Considerations

More than 2½ years following the September 11, 2001 attacks, there is considerable momentum to watch-list additional persons as known or suspected terrorists, or their supporters. Nevertheless, the exclusion or watch-listing of persons for ideological or political beliefs has long been a source of controversy. While it is clearly within the U.S. government's mandate to screen and track persons who are intent on inciting or engaging in terrorist activities, the determination of who may be a member or supporter of a foreign terrorist organization and, therefore, be prevented from entering the United States or be subject to police surveillance is ultimately a subjective consideration made by intelligence analysts and special agents based on the best information available.[462]

---

[458] P.L. 104-132, 110 Stat. 1214.

[459] P.L. 104-208, 110 Stat. 3009-546.

[460] P.L. 107-56, 115 Stat. 272.

[461] P.L. 101-649, 104 Stat. 4978. For more information on the process of designation of foreign terrorist organizations and other related foreign terrorist lists, see CRS Report RL32120, The "FTO List" and Congress: Sanctioning Designated Foreign Terrorist Organizations; and CRS Report RL32223, Foreign Terrorist Organizations, both by Audrey Cronin.

[462] Section 212(d) of the INA provides the Secretary of Homeland Security with authority to waive the inadmissibility of members and supporters of foreign terrorist organizations, if it is in the national interest to do so. Under current law, such visa denial waivers would be granted at the request of the Secretary of State.

Failures to Identify, Watch-List, and Screen 9/11 Hijackers

Despite measures following the first World Trade Center bombing to more effectively identify and screen known and suspected terrorists, all 19 hijackers who participated in the September 11, 2001 attacks had been issued visas by the DOS in accordance with statutorily required watch-list name checks and other visa issuance requirements, and had entered the country legally. While watch lists will never contain the names of all terrorists, it is generally agreed that members of the Intelligence Community possessed sufficient information to watch-list at least two, possibly three, of the al Qaeda hijackers. Better use of watch lists may have at least disrupted the activities of the September 11, 2001 hijackers.

According to the congressional 9/11 Joint Inquiry, the Intelligence Community missed repeated opportunities to watch-list two of the hijackers, Khalid al-Mihdhar and Nawaf al-Hazmi.[463] By January 2001, the CIA had identified al-Mihdhar and al-Hazmi from surveillance photos of a major meeting of known al Qaeda operatives in Kuala Lumpur, Malaysia on January 5 and 8, 2000. In the same month, the CIA obtained a copy of al-Mihdhar's Saudi passport. It was also known that al-Mihdhar had been issued a U.S. visa in Jeddah, Saudi Arabia, in April 1999, which was valid through April 2000. Nevertheless, the CIA did not watch-list him.[464]

On January 15, 2000, al-Mihdhar and al-Hazmi entered the United States at Los Angeles International Airport (LAX). By March 2000, the CIA had learned that al-Hazmi — an experienced Mujahadeen[465] — had entered the United States through LAX. For about five months, al-Mihdhar and al-Hazmi stayed in San Diego, taking flight lessons. In addition to being in contact with an FBI confidential informant in San Diego, they were also in contact with another September 11, 2001 coconspirator — Hani Hanjour, who subsequently piloted American Airlines Flight 77 into the Pentagon. On June 10, 2000, al-Mihdhar departed the United States; on July 12, al-Hazmi applied to the INS for a visa

---

[463] U.S. Congress, U.S. Senate Select Committee on Intelligence and U.S. House Permanent Select Committee on Intelligence, Joint Inquiry Into Intelligence Community Activities Before and After The Terrorist Attacks of September 11, 2001, 107th Congress, 2nd sess., S.Rept. 107-351, H.Rept. 107-792 (Washington: GPO, 2002), p. 12.

[464] Ibid., p. 145.

[465] Mujahadeen, in the sense used here, are fighters trained in insurgent and terrorist techniques, often in training camps sponsored by or associated with al Qaeda. In the context of the 1979-1989 war in Afghanistan, the Mujahadeen were often Muslim men from other countries who fought with the indigenous Afghan guerillas against the Soviets. Some of these Mujahadeen later formed the core of the al Qaeda movement.

extension. Al-Hazmi moved to Phoenix, AZ, linked up with Hanjour, and subsequently overstayed his visa.[466]

By late May 2001, the CIA transferred to the FBI the surveillance photos of the January 2000 Kuala Lumpur meeting. While al-Mihdhar and al-Hazmi were identified, along with Khallad bin-Atash, a leading al Qaeda operative and planner of the USS Cole bombing, neither the CIA nor the FBI watch-listed them. On June 13, 2001, with a new passport, al-Mihdhar obtained another U.S. visa in Jeddah. He falsely stated on the visa application that he had never been to the United States. He reentered the United States at John F. Kennedy (JFK) airport in New York City on July 4, 2001.

On the request of the CIA, al-Mihdhar and al-Hazmi were watch-listed on August 23, 2001 — less than three weeks before the September 11, 2001 terrorist attacks.[467] While FBI agents in Phoenix and Minneapolis were following up other leads that may have led them to the September 11, 2001 conspirators, the repeated failures by the Intelligence Community — principally the CIA and FBI — to watch-list al-Mihdhar and al-Hazmi were crucial lost opportunities associated with the September 11, 2001 attacks, according to the 9/11 Joint Inquiry.[468]

More recently, the National Commission on the Terrorist Attacks Upon the United States, known as the Kean Commission for its Chair — Thomas H. Kean, characterized these lost opportunities to watch-list al-Mihdhar and al-Hazmi as "failures." The Commission purports that there was evidence to watch-list Salem al-Hazmi — Nawaf al-Hazmi's brother as well. Despite the efforts of key INR officials who developed TIPOFF, the Kean Commission found that within the Intelligence Community "watchlisting" was not viewed as integral to intelligence work; rather it was viewed as "a chore off to the side...."[469]

Elevating and Expanding Terrorist Identification, Screening, and Tracking under HSPD-6

On September 16, 2003, the White House issued HSPD-6, which set in motion several measures to improve intelligence gathering and analysis on terrorists and their activities by establishing additional mechanisms to ensure secure, effective, and timely interagency information sharing. In other words, getting the right information to the right people, securely and at the right time. The centerpiece of

---

[466] U.S. Congress, Joint Inquiry Into Intelligence Community Activities Before and After The Terrorist Attacks of September 11, 2001, p. 148.

[467] Ibid., p. 152.

[468] Ibid., p. 81.

[469] National Commission on Terrorist Attacks upon the United States, "Three 9/11 Hijackers: Identification, Watchlisting, and Tracking," Staff Statement no. 2, (Washington, 2004), p. 1.

HSPD-6 is the establishment of the TSC — the latest of three multi-agency efforts undertaken by the Administration to better identify, screen, and track known terrorists, suspected terrorists, and their supporters. The other two are the FTTTF and the TTIC, both of which are described in greater detail below.[470]

Besides establishing the TSC, HSPD-6 transferred the terrorist identification and watch list functions previously performed by the DOS's INR to the TTIC and TSC. The TIPOFF system was developed by the DOS's INR to identify, watch-list, and screen terrorists and their supporters. Consular, immigration, and customs officers used TIPOFF-generated lookout records to exclude terrorists from entry into the United States and, if they managed to enter, to remove them from the United States. As part of its larger mission to assess terrorist threats, under HSPD-6, TTIC's member elements are now charged with identifying foreign terrorists as well. The TSC is charged with consolidating terrorist watch lists and making that data available in a useful format to screening agencies, and the FTTTF, with assisting federal law enforcement agencies with tracking foreign terrorists at home and abroad.

Foreign Terrorist Tracking Task Force (FTTTF)

On October 30, 2001, President George W. Bush directed that the FTTTF be established as part of Homeland Security Presidential Directive 2 (HSPD-2).[471] On August 6, 2002, the Attorney General placed the FTTTF administratively within the FBI. As a multi-agency effort, the mission of the FTTTF is to provide federal law enforcement agencies with the best possible information to: (1) prevent foreign terrorists and their supporters from entering the United States; and (2) locate, detain, prosecute, or remove them if they manage to enter the United States. Since the issuance of HSPD2, the mission of the FTTTF has evolved. While the FTTTF continues to assist federal investigators in locating terrorism-related suspects, much of its original mission to screen terrorists at ports of entry has been passed on to the TSC, as is more fully described below.

In many areas, the FTTTF has facilitated and coordinated information sharing agreements among participating agencies and commercial data providers. By accessing and analyzing this data, the FTTTF assists counterterrorism investigations being conducted by the FBI's National Joint Terrorism Task Force

---

[470] Other examples of interagency groups include the Secret Service's Document Security Alliance Groups, the Migrant Smuggling and Trafficking in Persons Coordination Center, and the Data Management Improvement Act Task Force. For further information on interagency efforts, see CRS Report RL31357, Federal Interagency Coordinative Mechanisms: Varied Types and Numerous Devices, by Frederick M. Kaiser.

[471] The White House, Homeland Security Presidential Directive-2, Subject: Combatting Terrorism Through Immigration Policies, Oct. 29, 2001. Click on [http://www.whitehouse.gov/news/releases/2001/10/20011030-2.html].

(National JTTF)[472] and 84 regional Joint Terrorism Task Forces (JTTFs).[473] By data-mining public and proprietary data systems, the FTTTF can track the "electronic footprints" of known and suspected terrorists.[474] In so doing, the FTTTF assists the 85 JTTFs nationwide, the 56 FBI field offices, the 46 FBI legal attaches[475] abroad, and the DHS in locating suspected terrorists and their supporters.

Besides the FBI, key FTTTF players include the DOD, the DHS CBP and ICE, the DOS, the Social Security Administration, the Office of Personnel Management, the Department of Energy, and the CIA. The FTTTF has also established liaisons with Canada, Australia, and the United Kingdom. The FTTTF was funded for FY2004 as a stand alone line item in the FY2004 Consolidated Appropriations Act in the amount of nearly $62 million.[476] Congress provided the same amount in FY2003 as well.[477]

Terrorist Threat Integration Center (TTIC)

In the State of the Union Address, on January 28, 2003, President George W. Bush announced the establishment of the TTIC. On the same date, the While House issued a *Fact Sheet: Strengthening Intelligence to Better Protect America*, which outlined the Center's mission and functions.[478] They include

- to optimize the use of terrorist threat-related information, expertise, and capabilities to conduct threat analysis and inform collection strategies;

---

[472] The FBI established the National JTTF in 2002 at the Bureau's Washington command center. The mission of the National JTTF is to collect terrorism-related intelligence and funnel it to the JTTFs, other FBI terrorism units, and partner agencies. Representatives from nearly 30 different agencies are detailed to the National JTTF, bringing outside expertise that includes intelligence, public safety, and state and local law enforcement.

[473] Several JTTFs were first formed in the early 1980s as teams of state and local law enforcement officers, FBI Special Agents, and other federal law enforcement officers. According to the FBI, by combining the assets of different agencies, the JTTFs act as "force multipliers" that allow for greater coverage in the war on terror. There are currently 84 JTTFs.

[474] For further information on issues related to data mining, see CRS Report RL31798, Data Mining: An Overview, by Jeffrey W. Seifert.

[475] As part of the Foreign Attache Program, the FBI has established 46 foreign legation offices overseas to establish cooperative efforts with foreign police partners as part of the FBI's domestic law enforcement mission.

[476] P.L. 108-199, 118 Stat. 3.

[477] P.L. 108-7, 117 Stat. 56.

[478] This fact sheet is available on the White House website, at [http://www.whitehouse.gov/news/releases/2003/01/20030128-12.html].

- to create a structure that ensures information sharing across agency lines;
- to integrate domestic and foreign terrorist-related information and form the most comprehensive possible threat picture; and
- be responsible and accountable for providing terrorist threat assessments for our national leadership.

TTIC became operational on May 1, 2003. John Brennan, a career CIA official, was appointed by the Administration to be the Director of TTIC. An FBI special agent serves as the Center's Deputy Director. Funding for TTIC is provided by participating agencies, including the DHS, DOS, DOJ, DOD, and the Intelligence Community. While TTIC is under the DCI, the Administration emphasizes that it is a "multi-agency joint venture," and is not part of the CIA. TTIC's mission is to form the most comprehensive threat picture possible by serving as a central hub for the fusion and analysis of all-source information collected from foreign and domestic sources on international terrorist threats.

TTIC's operations will encompass elements of both the FBI's Counterterrorism Division (CTD)[479] and the DCI's Counterterrorism Center (CTC).[480] In September 2003, there were about 100 analysts on board at TTIC, and the Administration plans to have about 300 analysts total on board in May 2004, when the Center is scheduled to be moved to a location outside of the CIA.[481] Collocating the DCI's CTC and the FBI's CTD at TTIC is designed to encourage greater cooperation and information sharing between the wider Intelligence Community and the FBI.[482]

In the past, information sharing between the CIA and FBI has been hampered by differing priorities and methods. The CIA is banned from having any role in domestic law enforcement or internal security functions by the National Security Act of 1947,[483] and the DCI is mandated to protect "sources and methods from unauthorized disclosure."[484] Like the CIA, the FBI also protects its sources and

---

[479] The mission of the FBI's CTD is to detect and deter terrorist acts within the United States, and to investigate terrorist attacks against U.S. interests and the American people at home and abroad.

[480] The mission of the DCI's CTC is to exploit all-source intelligence to produce in-depth strategic and tactical analyses of terrorist groups. The CTC also coordinates the Intelligence Community's counterterrorism activities and operations.

[481] Kevin Whitelaw, "Inside the Government's New Terrorism Threat Integration Center," U.S. News & World Report, Sept. 15, 2003, p. 31.

[482] See also, CRS Report RL32336, FBI Intelligence Reform Since September 11, 2001: Issues and Options for Congress, by Alfred Cumming and Todd Masse.

[483] 50 U.S.C. §403-3(d)(1).

[484] 50 U.S.C. §403-3(c)(7).

methods — particularly the identities of confidential informants, so as not to jeopardize on-going investigations.

The FBI, however, is also bound by other criminal laws and guidelines related to protecting grand jury information and limiting criminal investigations, undercover operations, and covert surveillance that are, in large part, designed to protect privacy and civil liberties. Consequently, the CIA takes a long-term strategic view of intelligence gathering and analysis, while the FBI takes a short-term tactical view that is geared towards resolving investigations.[485]

Nevertheless, according to the Administration, TTIC will not collect intelligence; instead, as the primary consumer of terrorism-related intelligence, one of the Center's core functions is to ensure information-sharing across agency lines. TTIC is also responsible for setting requirements and tasking other federal agencies in the area of shared databases. The Attorney General is responsible for ensuring that the FBI's information technology modernization programs are configured to share information easily with TTIC.

In terms of more broadly disseminating intelligence reports, an administration official has recently testified that TTIC's Information Sharing Program Office has worked to reduce the number of terrorism-related documents and records that are not under "originator control," meaning the information contained in those records could compromise sources and methods. Consequently, before another agency uses that document or record, it must gain the permission of the originating agency.

Other methods being employed more frequently at TTIC are "writing for release" and "tear lines."[486] Writing for release means producing useful, but less sensitive intelligence reports. Tear lines are employed to divide reports. The substance of the information appears above the tear line, and the sources and methods by which the information was acquired appears below the tear line.

To effect rapid interagency information-sharing, TTIC has established a classified web-accessible service — TTIC Online. TTIC is developing less sensitive mirror

---

[485] Frederick P. Hitz and Brian J. Weiss, "Helping the CIA and FBI Connect the Dots in the War on Terror," International Journal of Intelligence and Counterintelligence, spring 2004, vol. 17, no. 1, p. 13.

[486] Russell E. Travers, TTIC Associate Director for Defense Issues, Statement Before the National Commission on Terrorist Attacks Upon the United States, Jan. 26, 2004, p. 7.

images of TTIC Online to more broadly disseminate information and analysis to appropriate entities.[487] See Figure 2 below.

TTIC will also establish and maintain the TID, which will be a repository for all-source information on known and suspected terrorists.[488] The TID is envisioned as becoming the primary source for international terrorist data provided by TTIC to the TSC. Such information will include names, aliases, dates and places of birth, identification and travel documents, unique and distinguishing physical features, biometric data, and individuals' past affiliation with terrorist acts or groups. In the past, much of this information was stored in disparate databases maintained by several agencies. Consolidating and expanding this data could remedy systemic weaknesses that in the past prevented intelligence analysts and investigators from positively identifying known and suspected terrorists.

To build the TID and prevent duplication of effort, functions of the DOS Bureau of Intelligence and Research's TIPOFF system — particularly those aspects related to the identification of foreign terrorists — have been transferred to TTIC. The entire TIPOFF database of about 120,000 names is now the core of the TID. TIPOFF staff have been split, with part going to the TTIC and part going to the TSC. Under HSPD-6, the President directed all heads of executive departments and agencies to provide to TTIC on a continual basis all appropriate data regarding terrorists and related activities to the extent that the law allows. In turn, TTIC is to provide the TSC with all appropriate information. See Figure 2 below.

TTIC and IAIP Reporting Requirements

Unlike the FTTTF, the establishment of TTIC has generated some controversy.[489] Some Members of Congress have questioned whether the functions currently assigned to TTIC, like intelligence fusion and threat assessment, would not be better housed in DHS's Directorate for Information Analysis and Infrastructure Protection (IAIP), as the Homeland Security Act gave responsibility for all-source

---

[487] Testimony of John Brennan, Terrorist Threat Integration Center Director, in U.S. Congress, Senate Judiciary Subcommittee on Immigration and Border Security (Washington, Sept. 23, 2003), p. 2.

[488] The TID is nearly identical to a system required under section 343 of the Intelligence Authorization Act for Fiscal Year 2003 (P.L. 107-306, 116 Stat. 2399), which requires the DCI to establish a "terrorist identification classification system" that would be a list of individuals who are known or suspected terrorists, and organizations that are known or suspected terrorist organizations.

[489] For further information, see CRS Report RS21283, Homeland Security: Intelligence Support, by Richard A. Best, Jr.

terrorist threat analysis to the new department.[490] In September 2003, William Parrish — the former DHS Acting Assistant Secretary for Information Analysis — testified that DHS will overlay TTIC-generated threat assessments on IAIP-identified vulnerabilities, so that protective measures can be developed and implemented.[491] In other words, with TTIC-generated threat information, IAIP could be better equipped to identify and prioritize the nation's critical infrastructure that needs to be more closely guarded so that security resources can be more efficiently deployed.

Regarding the respective roles of the DHS's IAIP and the DCI's TTIC, Section 359 in Intelligence Authorization Act for Fiscal Year 2004[492] requires the President to submit a report to the appropriate committees of Congress[493] by May 1, 2004, on the operations on both the IAIP Directorate and TTIC. This provision sets out that this report should include the following elements:

- an assessment of the operations of the IAIP and TTIC;
- an assessment of the ability of TTIC to carry out the responsibilities assigned to it by the President;
- an assessment of the ability of IAIP to carry out the responsibilities assigned to it under section 201 of the Homeland Security Act;[494]
- an action plan to bring TTIC to full operational capacity as outlined in the President's State of the Union address, including milestones, funding, and sources of funding;
- a delineation of responsibilities and duties for the IAIP and TTIC;
- a delineation and summary of overlapping areas of responsibilities and duties carried out by IAIP, TTIC, and any other element of the federal government;
- an assessment of where these areas of overlap, if any, represent an inefficient use of resources;

---

[490] The House Select Committee on Homeland Security and the Committee on the Judiciary held a hearing on TTIC on July 22, 2003. The Senate Judiciary Subcommittee on Immigration and Border Security held a hearing on HSPD-6, in which the role of TTIC was questioned, on Sept. 23, 2003.

[491] Testimony of William Parrish, Acting Assistant Secretary for Information Analysis, in U.S. Congress, Senate Judiciary Subcommittee on Immigration and Border Security (Washington, Sept. 23, 2003), p. 2.

[492] P.L. 108-177, 117 Stat. 2622.

[493] For purposes of this provision the appropriate committees of Congress include the Senate committees on Intelligence, Governmental Affairs, the Judiciary, and Appropriations; and in the House, the committees on Intelligence, Homeland Security, the Judiciary, and Appropriations.

[494] P.L. 107-296, 116 Stat. 2145.

- a description of the policies and procedures adopted by IAIP and TTIC to ensure compliance with the Constitution, any applicable statues, executive orders, and regulations of the United States;
- an assessment of the practical impact that TTIC operations, if any, may have on individual liberties and privacy; and
- any other information the President deems appropriate that provides a fuller explanation as to why TTIC should be established as a "joint venture" of participating agencies rather than as an element of IAIP.

This provision sets out further that the report be presented in an unclassified format, which may include a classified annex if necessary.

Terrorist Screening Center (TSC)

According to the Administration, the primary mission of the TSC is to consolidate all federal terrorist watch lists into a consolidated terrorist screening database, so that all federal agencies would have access to the best and most complete information. A TSA official, Donna Bucella, has been detailed to the FBI and appointed head of the TSC. A DHS official, Richard Kopel, has been appointed second-in-command at the TSC. As a multi-agency effort, the Center's staff will include designees from the DOS, DOJ, and DHS, as well as other intelligence community entities. TSC personnel are to be given access to TTIC databases, including the TID, as well as any relevant intelligence that advances terrorist screening.

Under HSPD-6, the Administration envisions that terrorist watch lists will be used much more frequently in the future. In the past, terrorism-related watch lists were used principally for purposes of screening noncitizens applying for visas abroad at consular offices and at the border when applying for admission at international ports of entry. Today, as described more fully below, state and local law enforcement officers are able to screen persons stopped for routine traffic violations against terrorist TSDB lookout records. See Figure 2 above.

The TTIC Director, the TSC Director, the heads of federal departments or agencies, or their designees "nominate" persons for inclusion in the TSDB by notifying either the TTIC or the FBI. The TSC Director is responsible for establishing procedures to review these records when new information is developed concerning the persons about whom the records are maintained. According to the Administration, TTIC is providing international terrorism data, and the FBI is providing domestic terrorism data for inclusion in the TSDB. Both sets of data are merged in the TSC-maintained TSDB.

According to the FBI, international terrorists include those persons who carry out terrorist activities under foreign direction. For this purpose, they may include citizens or noncitizens, under the rationale that citizens could be recruited by foreign terrorist groups. Or, noncitizens (aliens) could immigrate to the United States and naturalize (become citizens), having been unidentified terrorists

before entry, or having been recruited as terrorists sometime after their entry into the United States. By comparison, domestic terrorists are not under foreign direction, and operate entirely within the United States. According to the Administration, when appropriate, both sets of data will include information on "United States persons."[495] Criteria for the inclusion of U.S. persons in the database will be developed by an interagency working group. The term "United States persons" includes U.S. citizens and legal permanent residents (immigrants).

For agencies responsible for screening terrorists, the TSC Director and agency designees will determine the "screening processes" that will be supported and the amount and type of data that will be provided, depending on an agency's mission. Based on recent congressional testimony, it is clear that the TSC is supporting the screening missions of the DOS's CA and DHS's CBP. It is less clear how much support the TSC is providing the DHS's TSA and ICE. To determine whether to allow screening agencies access to certain records, the TSC is to consider, but not be limited to, the following elements:

- the nature of the person's association with terrorism;
- the quality of data, including credibility, reliability, and extent of corroboration;
- the extent of uniquely identifying personal data;
- the authority or authorities under which the data were obtained, and any restrictions on how these data may be shared or used;
- the authority or authorities of the screening entity;
- the circumstances, including changes in the Homeland Security Alert Level, under which screening will occur; and
- the action the screening agency will take if a person is identified as a person in the TSC's terrorist screening database.

These elements serve as a rough guide to what should be included in lookout records. Nevertheless, HSPD-6 does not speak to the issue that the FBI-administered TSC will need to fully assess the missions of many different agencies in order to provide the appropriate amount of information and handling codes in the lookout records, which will then be disseminated from the consolidated TSDB. While departmental and agency designees will have a voice at the table, and each agency will determine which known or suspected terrorists are placed in the respective lookout systems under HSPD-6, the FBI will be the lead agency and likely play an important role in the final decision.

---

[495] The definition of "United States person" is found at 50 U.S.C. §1801(i): a citizen of the United States, an alien lawfully admitted for permanent residence (as defined §1101(a)(2) of Title 8), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in subsection (a)(1), (2), or (3) of this section.

Expanding Use of Terrorist Watch Lists

Prior to September 11, 2001, watch lists were used principally for federal border and transportation security, and law enforcement. In HSPD-6, the Administration has clearly signaled that the use of watch lists will be expanded beyond those purposes traditionally associated with border and transportation security, and federal law enforcement. Under HSPD-6, to the extent permitted by law, the consolidated TSDB will be made available to:

- state, local, territorial, and tribal law enforcement agencies;
- other appropriate state, local, territorial, and tribal authorities;
- private sector entities charged with managing critical infrastructure or organizers of large events (e.g., the Salt Lake City Winter Olympics); and
- foreign governments that have entered into immigration agreements with the United States or that are engaged in the global war on terrorism as partners with the United States.

As described below, the Administration has made such records available to state and local law enforcement, and plans to make such records available in limited cases with foreign governments through the FBI's National Crime Information Center (NCIC) in a sensitive but unclassified format. NCIC is an FBI-administered telecommunications system that allows authorized law enforcement officers, including state and local officers, to access and search several automated databases pertaining to fugitives, missing persons, stolen property, and criminal histories.

In regard to noncitizens, the Attorney General, in consultation with the Secretary of Homeland Security, or their designees at the TSC, is to determine which records are entered into NCIC. For all other persons, the Attorney General is to determine which records relating to alleged terrorists are entered into NCIC. The Secretary of Homeland Security, or his TSC designee, is to determine whether such records should be available to other non-law enforcement authorities at the state, local, territorial, and tribal levels for other purposes. Such purposes may include screening persons when they apply for driver's licenses or licenses to transfer hazardous material. The Secretary of State, in consultation with the Attorney General, Secretary of DHS, and the DCI, will determine which records will be made available to foreign governments.

TSC Level of Operations

According to the Administration's timetable, TSC operations were to be phased in rapidly, and the center was to be operational by December 1, 2003.[496] According to press accounts, however, the Administration informed Representative Jim Turner, the ranking Member of the Select Committee on Homeland Security, that the TSC was not "fully" operational as of the end of December and that the Nation's multiple terrorist watch lists had yet to be consolidated.[497] Director Bucella publically testified that the TSC was operational on December 1, 2003.[498] According to that testimony, as part of phase one, the TSC has had the ability to

- provide the names and identifying information of known or suspected terrorists to federal, state, and local law enforcement;
- review whether a known or suspected terrorist should be included in the agency watch lists or should be deleted from such lists;
- ensure that persons, who may share a name with a known or suspected terrorist, are not unduly inconvenienced by screening processes conducted by the U.S. government; and
- adjust or delete outdated or incorrect information to prevent problems arising from misidentifications.[499]

On March 25, 2004, Director Bucella testified before a joint hearing of the House Judiciary Committee's Crime, Terrorism and Homeland Security Subcommittee and the Select Homeland Security Committee's Intelligence and Counterterrorism Subcommittee.[500] In that testimony, Director Bucella reported that phase two of the TSC's implementation had been completed and an unclassified but law enforcement sensitive TSDB had been established. As of April 1, 2004, the TSDB contained about 79,289 lookout records.

Through March, the TSC had provided DOS's CA with 54,000 security advisory opinions, of which 90 were related to terrorism, and 56 resulted in visa revocations. In addition, the CBP's National Targeting Center Director, Charles Bartoldus, testified that CBP officers were routinely working with the TSC to evaluate and assess potential matches between terrorist lookout records and individuals applying for admission into the United States. With TSC's assistance, CBP inspectors are currently able to resolve potential matches more

---

[496] U.S. Department of Justice, Fact Sheet: Terrorist Screening Center, Sept. 16, 2003, at [http://www.fbi.gov/pressrel/pressrel03/tscfactsheet091603.htm].

[497] Chris Strohm, "Congressman Blasts Bush on Terrorist Screening Efforts," Government Executive Magazine, Jan. 13, 2004, at [http://www.govexec.com/dailyfed/0104/011304c1.htm].

[498] Donna Bucella, Terrorist Screening Center Director, Testimony Before the National Commission on Terrorist Attacks Upon the United States, Jan. 26, 2004, p. 1.

[499] Ibid., p. 2.

[500] This hearing can be viewed by webcast at [http://www.house.gov/judiciary/crime.htm].

expeditiously, resulting in the more timely release of individuals who have been misidentified. Members also asked Director Bucella about the TSC's interactions with the DHS's TSA, but it was less clear from her responses whether TSA was consulting with the TSC about terrorism-related hits in the Computer Assisted Passenger Profiling System.

Furthermore, TSDB-generated lookout records are currently being disseminated to state and local law enforcement officers through the NCIC. The unclassified portion of TSDB-generated lookout records (name, date of birth, passport number, and country of origin) have been loaded into the NCIC's Violent Gang and Terrorist Organizations File (VGTOF). According to Director Bucella, the TSC has set up a protocol for when NCIC queries by state or local law enforcement officers result in a terrorism-related hit.

When NCIC terrorism-related hits occur, the state and local officers stand by, while their dispatchers contact the TSC. Through the dispatchers, the TSC operators will elicit certain information from the state or local officers to determine whether there is a match. Such information could include identifiers, like height, weight, eye color, hair color, tattoos, or scars, which may be classified. If the TSC deems that a match has been made, the TSC will contact the FBICounterterrorism Watch unit (CT Watch unit) at FBI headquarters.

If needed, the CT Watch unit will contact and consult the appropriate JTTF and designated case officer. Following such consultations, the TSC operators will provide the state and local officers with the most appropriate course of action. Such actions include four possible scenarios: arrest, detain and question, question and release, or proceed with normal police procedure. According to Director Bucella, the TSC is able to process most state and local NCIC terrorism-related hits within 20 to 30 minutes.

The TSC is presently engaged in a large-scale outreach program to inform state and local law enforcement agencies about the TSC. Some Members at the hearing, however, questioned whether most state and local agencies were aware of the TSC or the changes to NCIC's VGTOF. They also questioned whether some federal law enforcement units, like the Border Patrol, had access to NCIC, and whether such queries were routinely made on aliens attempting to enter the country between ports of entry.

As part of this outreach process, the TSC is also working with those agencies to determine if the TSDB could be incorporated into screening processes conducted by those agencies. In addition, the TSC is contacting other federal agencies to determine whether they have terrorism-related records that would be of use to the TSC. In this regard, several members raised concerns that the Department of Defense had not done enough to transfer terrorism-related data to the TSC, and possibly the TTIC, concerning al Qaeda and Taliban combatants who had been previously detained at Guantanamo, but who had subsequently been released.

Director Bucella indicated that some data regarding these persons had been transferred to the TSC.

Director Bucella outlined phase three of the TSC implementation. By December 2004, the TSC is scheduled to use the TSDB as a single, integrated system for entering known and suspected terrorist identities. At that point, the TSDB will be integrated ("dynamically linked") into all appropriate screening processes. In addition, selected private sector entities, such as operators of critical infrastructure facilities or organizers of large events, will be allowed to submit lists of persons associated with those events to the U.S. government to be screened for any connection with terrorism. Meanwhile, the DOS is working to establish mechanisms by which terrorist screening information can be shared with foreign countries cooperating with the United States in global efforts to counter terrorism.

Legal Safeguards

The TSC Director is responsible for developing policies and procedures related to criteria for inclusion into the database; and measures to be taken in regard to misidentifications, erroneous entries, outdated data, and privacy concerns. As described above, according to TSC Director Bucella, procedures have been developed regarding the inclusion of persons in the TSDB, the correction of erroneous data, the purging of outdated data, and the incorporation of new data to prevent further misidentifications of persons who share the same or similar names as persons for whom terrorism-related lookout records exist.

The Administration maintains that since the TSC does not collect intelligence, and has no authority to do so, that all intelligence or data entered into the TSDB has been collected in accordance with the preexisting authorities of the collecting agencies. Nonetheless, these existing agency policy and procedures probably do not address information sharing with private entities for security purposes. Members of Congress and other outside observers have questioned whether there should be new policy and procedures at different levels (such as, visa issuance, border inspections, commercial aviation security, domestic law enforcement, and security of public events) for the inclusion of persons in the TSDB.[501]

Also, Members have asked how a person would find out if they were in the TSDB, and if so, how did they get there? In congressional testimony, Director Bucella surmised that a person would learn of being in the TSDB when a screening agency encountered them and, perhaps, denied them a visa or entry into the United States, or arrested them. Director Bucella also suggested that the TSC

[501] For further information, see CRS Report RL31730, Privacy: Total Information Awareness Programs and Related Information Access, Collection, and Protection Laws, by Gina Marie Stevens.

would probably be unable to confirm or deny whether the person was in the TSDB under current law.

Consequently, persons who have been identified or misidentified as terrorists or their supporters by the TSC would have to pursue such matters through the screening agency. However, the screening agency might not have been the source of the record in which case, a lengthy process of referrals may have to be initiated. Under such conditions, persons identified as terrorists or their supporters may turn to the Freedom of Information Act (FOIA) or the Privacy Act as a last alternative.

Under FOIA,[502] any person, including a noncitizen or nonpermanent resident, may file a request with any executive branch agency or department, such as the DOS or DHS, for records indicating they are on a watch list. Under national security and law enforcement FOIA exemptions, the Departments may withhold records on whether an individual is on a watch list.[503]

In addition to a FOIA request, a citizen or legal permanent resident may file a Privacy Act[504] request with DHS and/or Justice to discern whether the TSA or the FBI has records on them. However, the law enforcement exemption under the Privacy Act may permit the Departments to withhold such records. Under the Privacy Act, a citizen or legal permanent resident may request an amendment of their record if information in the record is inaccurate, untimely, irrelevant, or incomplete. Under both FOIA and the Privacy Act, there are provisions for administrative and judicial appeal. If a request is denied, the citizen or legal permanent resident is required to exhaust their administrative remedies prior to bringing an action in U.S. District Court to challenge the agency's action.

The Administration has pledged that terrorist screening information will be gathered and employed within constitutional and other legal parameters. While the Privacy Act generally does not restrict information-sharing related to known and suspected terrorists who are not U.S. persons for the purposes of visa issuance and border inspections, it does restrict the sharing of information on U.S. persons (citizens and legal permanent residents) for purely intelligence purposes, who are not the subject of on-going foreign intelligence or criminal investigations.[505]

---

[502] 5 U.S.C. §522.

[503] 5 U.S.C. §§522(b), (c), 522a(j).

[504] 5 U.S.C. § 522a.

[505] Department of State, Testimony to the Joint Congressional Intelligence Committee, p. 5.

Consequently, legal questions concerning the inclusion of U.S. persons in these systems under criminal or national security predicates may arise. Protocols have been established for state and local law enforcement to cover the eventuality that a positive NCIC VGTOF hit indicates that they have encountered a known or suspected terrorist. However, it is unclear whether protocols have been established for false positives if a person is misidentified. In addition, questions of compensation for persons mistakenly damaged by inclusion in these databases will likely be an issue.

TSC Reporting Requirements

Section 360 of the Intelligence Authorization Act for Fiscal Year 2004[506] requires the President to submit a report to Congress by September 16, 2004 on the operations of the TSC, as established under HSPD-6. This provision sets out that this report should include the following elements:

- an analysis of TSC operations to ensure that the TSC does not violate the Constitution, or any statute, executive order, or regulation of the United States;
- a description of the TSC database architecture, including the number of databases operated or maintained by the TSC, and an assessment of the extent to which these databases have been integrated;
- a determination of whether the data from all the watch lists, enumerated in the GAO report entitled Information Technology: Terrorist Watch Lists Should be Consolidated to Promote Better Integration and Sharing (described below), have been incorporated into the consolidated terrorist screening database system;
- a determination of whether any other databases ought to be integrated into the consolidated terrorist screening database;
- a schedule setting out the dates by which identified databases, which are not yet integrated into the consolidated terrorist screening database system, would be integrated into that system;
- a description of the protocols that have been established to ensure the protection of classified and sensitive information that is contained within the consolidated terrorist screening database;
- a description of processes that have been established to ensure that the information in the consolidated terrorist screening database is systematically and frequently reviewed for timeliness and accuracy;
- a description of the mechanism that has been established to ensure that the information in the consolidated terrorist screening database is synchronized and replicated throughout that database;

[506] P.L. 108-177, 117 Stat. 2623.

- a description of the extent to which, and the criteria under which, the TSC makes the information in the consolidated terrorist screening database available to the private sector and critical infrastructure components;
- the number of individuals listed in the consolidated terrorist screening database;
- the estimated budget of, and sources of funding for, the TSC for each of the fiscal years 2004, 2005, and 2006;
- an assessment of the impact of the TSC and the consolidated terrorist screening database on current law enforcement systems;
- the practical impact, if any, of TSC operations on individual liberties and privacy; and
- such recommendations as the President deems appropriate for modifications to law or policy to ensure the continued operations of the TSC.

This provision requires further that the report be presented in an unclassified format, which may include a classified annex if necessary.

Selected Watch List, Criminal, and Biometric Systems

To provide border and transportation security, a number of federal agencies have long maintained watch lists, or lookout books, for the purposes of excluding certain "undesirable" aliens, including known and suspected terrorists, from travel to, and entry into, the United States. These watch lists reside on consular and border management computer systems, as well as on criminal history record computer systems. In addition, to identify individuals with greater certainty, several biometric systems have been developed in parallel with these systems. It is notable that most of these systems were developed separately and for different purposes that reflect agency-specific missions and legal authorities.

The U.S. government's principal terrorist watch list system has been the DOS's TIPOFF system, which is classified. While the other members of the Intelligence Community have begun culling through their intelligence reports and producing additional lookout records, prior to September 11, 2001, the staff of INR's TIPOFF produced by far the lion's share of terrorist lookout records. For the purposes of visa issuance and border inspections, TIPOFF lookout records are loaded into two unclassified systems: CA's CLASS and DHS's IBIS.

CLASS is a computerized system used to manage visa applications, among other consular-related activities. Border inspectors use the IBIS system to process travelers entering the United States at international ports of entry.[507] Many

[507] In most cases, the U.S. Border Patrol — formerly part of the INS — does not have access to IBIS, since Border Patrol agents were and are responsible principally for monitoring territory between land border ports of entry, rather than screening travelers at ports of entry, as customs and immigration inspectors do. As a consequence, some apprehended aliens who are paroled, or

agencies compile watch lists for law enforcement and other purposes, which are also loaded into IBIS. Hence, inspectors act as agents of these agencies when processing travelers. As an integrated system, IBIS allows inspectors to seamlessly and simultaneously search several law enforcement and border management databases.

While data sharing between some of these systems is routine, with others it is not. For example, declassified lookout records are downloaded from TIPOFF and uploaded into the DOS CLASS system and the NAILS II, a legacy INS system that is currently maintained by DHS's ICE. Prior to TIPOFF's transfer, this was done weekly, but priority cases could be uploaded into IBIS within minutes if needed. At the TSC, it will be done daily, if not more often. In turn, NAILS II records are uploaded into TIPOFF, since immigration officers produce terrorist-related lookout records as well. It is likely that these practices will be continued at the TSC, but it is unknown how frequently or in what manner they will be accomplished. Until required to by the USA PATRIOT Act, the DOJ was unwilling to share criminal history records with the DOS, including terrorist lookout records contained in NCIC.

Merging watch lists will not likely require integrating entire systems. Nonetheless, there are likely to be other technological impediments. For example, from system to system, and watch list to watch list, there remains no standardization of data elements, such as, name, date of birth, place of birth, or nationality. In the past decade, digitized biometrics (principally fingerprints) have been used increasingly to identify individuals with greater certainty, but most biometric systems have been developed separately from other systems. Integrating data from biometric systems, such as IAFIS and IDENT, into either the TID or the TSDB could be technologically difficult and costly. Under HSPD-6, the TTIC director has been charged with the responsibility for setting uniform system standards for watch list records.

At the same time, while elevating and expanding the terrorist watch list function under HSPD-6 is an important step in the wider war on terrorism, specialists in the area of national security have observed that homeland (border) security could be improved by upgrading and integrating existing consular/immigration and border management systems, criminal record history systems, and biometric systems.[508]

---

released on their own recognizance, into the United States, are not checked against watch lists or criminal history record systems. Initiatives are underway to provide agents with lap top computers, which include access watch lists and other data in a SBU format, but most Border Patrol stations do not have access to IBIS for reasons of cost and logistics.

[508] Lee S. Strickland, J.D., and Jennifer Willard, M.L.S., "Reengineering the Immigration System: As Case for Data Mining and Information Assurance to Enhance Homeland Security," Homeland Security Journal, Oct. 2002, p. 9.

GAO Watch List Recommendations

In April 2003, the General Accounting Office (GAO) issued a report that included findings and several recommendations regarding terrorist watch lists. GAO found that at least nine agencies maintained 12 terrorist and criminal watch lists that were used principally for border security or law enforcement purposes. GAO reported that data sharing was hampered by incompatible system architectures — computer hardware, software, and networking. Therefore, GAO recommended that a central authority (leadership), spanning several departments and agencies, be made responsible for standardizing and consolidating watch lists. According to GAO, the new system should be developed to allow agencies to effectively carry out their missions by enforcing all relevant laws in their unique operational environments.[509] At a minimum, lookout records from at least some of these systems (described below) would likely be incorporated into the TSDB.

Of the 12 systems listed by GAO that include watch lists, nine are described below. Table 1 below lists these nine systems and the departments and agencies responsible for maintaining them. The systems that GAO listed, which are not described below, include the U.S. Marshals' "wants and warrants" file, the U.S. Air Force Office of Special Investigations' Top 10 Fugitive List, and U.S. Central Bureau for Interpol's terrorism watch list. These lists were not included in the treatment below because: the Marshals' wants and warrants file is incorporated into NCIC; the Air Force list is small by comparison to the rest; and Interpol records were reviewed by the FBI and INR for inclusion in NCIC and TIPOFF. At the TTIC, it is likely that Interpol records will continue to be reviewed for inclusion in the TID and, by extension, in the TSDB.

While not included in the GAO study, the Regional Information Sharing System/Law Enforcement Online (RISS/LEO) is described below, because state and local investigators support this system. Not only could RISS/LEO be used to share lookout records with state and local law enforcement, but investigative files could also be shared in some cases. In terms of biometric technology, two systems figure prominently, IAFIS and IDENT. Furthermore, Justice has recently built a biometric capability into NCIC. Brief mention is also given to State's Consolidated Consular Database, which serves as a central repository for all visa applications, including digitized visa photos and, in some cases, fingerprints.

TIPOFF[510]

---

[509] For further information, see GAO Report GAO-03-322, Information Technology: Terrorist Watch Lists Should Be Consolidated to Promote Better Integration and Sharing (Washington, Apr. 2003), p. 28.

[510] Briefing with DOS's Bureau of Intelligence and Research, Oct. 23, 2003.

TIPOFF is a classified computer lookout system, which was maintained by the DOS's INR to identify and watch-list known and suspected terrorists.[511] Created in 1987, it originally consisted of 3x5 index cards in a shoe box. TIPOFF staff used specialized computer search engines to systematically cull through all-source data, from highly classified central intelligence reports to intelligence products based on open sources, to identify known and suspected terrorists. These classified records are scrubbed to protect intelligence sources and methods, and biographic identifiers are declassified, and exported into lookout systems (CLASS and IBIS). Consular officers can query these records electronically in CLASS to deny visas to terrorists and their supporters. Immigration and customs inspectors query these records in IBIS to deny terrorists entry into the United States at international ports of entry.

Following the 1993 World Trade Center bombing, the Visa Viper process was established, as a dedicated/secure telegraphic channel that allows consular and intelligence officers to report known and suspected terrorists to INR for inclusion in TIPOFF. There are more than 120,000 records of terrorists and other criminals in TIPOFF, nearly double the number on September 11, 2001. Due to the use of aliases among terrorists, some of these records involve the same individuals. There are nearly 81,000 distinct individual terrorist names in TIPOFF.

Until recently, all subjects of TIPOFF records were non-U.S. persons — roughly speaking those persons who are not legal permanent residents (immigrants) or citizens of the United States. Under HSPD-6, the terrorist identification process currently performed by INR will be expanded and transferred to TTIC. A mirror image of INR's TIPOFF system has been built at TTIC to feed terrorist lookout records into a terrorist identities database (TID). Since September 11, 2001, other members of the Intelligence Community have combed through their products and case files to identify additional terrorists who should be excluded from entering the United States. As part of these efforts, records on U.S. persons (citizens and legal permanent residents) who are the subject of ongoing criminal or national security investigations will be entered into the TID as well. The process performed by INR of declassifying lookout records and exporting them to the appropriate consular, border security, and law enforcement agencies has been transferred to TSC.

Consular Lookout and Support System (CLASS)[512]

---

[511] For several years past, the INR was expanding TIPOFF to include records on known and suspected international criminals and drug traffickers as well. Under HSPD-6, this function will remain at INR.

[512] Briefing with DOS's Bureau of Consular Affairs, Oct. 23, 2003.

The CLASS system is the DOS's principal unclassified lookout database that is used by consular officers abroad to check the names of visa and passport applicants against several watch lists that are maintained for various purposes, including screening known and suspected terrorists. While the DOS has maintained an automated visa lookout system since 1970, the development of CLASS was accelerated after the first World Trade Center bombing and the conspiracy to blow up the Holland and Lincoln Tunnels, and the United Nations Headquarters, in New York City.[513]

In terms of name recognition, the CLASS system is the most advanced lookout system currently maintained by the federal government. It includes a compressed name search capability, as well as sophisticated Arabic, Russian/Slavic, East Asian, Hispanic, date of birth, and country of birth algorithms. The language algorithms, for example, search for variations in name spelling based on the phonetic transliteration of names from other languages into the Roman alphabet. The algorithm scores the searches to arrange them in order of likelihood of a match. All consular posts can directly access CLASS online. There are about 15.4 million records in CLASS, including 90,000 records on suspected or known terrorists and their supporters.[514]

National Automated Immigration Lookout System II (NAILS II)[515]

The NAILS II system is the lookout system formerly maintained by INS, until that agency was dismantled and its constituent parts were transferred to DHS. Today, NAILS II is maintained by the DHS's ICE. NAILS II contains about 3.8 million files, including biographical and case data on persons who may be inadmissible or are being sought by immigration officers for other reasons related to immigration enforcement. Of these files, 58,000 files concern suspected or known terrorists and their supporters. The NAILS II system can be searched by name, variations on the name, alien registration number, and date of birth. The name recognition technology in NAILS II is Soundex, a technology that

[513] The case of Sheikh Omar Abdel Rahman is illustrative. He had been implicated in the assassination of Egyptian President Anwar Sadat in 1981 and watch-listed, yet he was issued a visa in Khartoum, Sudan. At the time, the Khartoum consulate lookout records were on microfiche and there were several variations of Rahman's name. He was convicted for his part in the conspiracy to blow up the Holland and Lincoln Tunnels, and the United Nations Headquarters, in New York City.

[514] CLASS data on immigrant and nonimmigrant visa holders are downloaded several times daily into IBIS through NAILS II and the Treasury Enforcement Communications System II (TECS II), which are both maintained currently by DHS.

[515] Mark T. Kenmore, "Update on U.S. Ports of Entry," Immigration & Nationality Law Handbook, 2002-2003 Edition, vol. 1 (Washington, 2002), p. 257.

was patented some 100 years ago.[516] Lookout records are downloaded from TIPOFF and uploaded into NAILS II on an hourly basis, and from NAILS II into CLASS on a weekly basis, or as needed. At the TSC, this process will be performed daily.

Interagency Border Inspection System (IBIS)[517]

The IBIS system, an unclassified system, was maintained by the Department of the Treasury's U.S. Customs Service, until Customs was transferred to DHS. INS was also a major stakeholder in this system, since both Customs and Immigration inspectors screen aliens for admission into the United States at ports of entry.

The IBIS system was congressionally mandated by the Omnibus Drug Initiative Act of 1988[518] in order to share lookout records maintained separately by INS, State, and Customs. The Customs Service supported about 17 different watch lists by downloading lookout records from other agencies into the IBIS. IBIS provides inspectors with the ability to perform a single, all purpose query in the primary inspection lanes.[519] If the system generates a hit, the inspector diverts the traveler to secondary inspection for additional clearance procedures. Developed by the Customs Service, IBIS utilizes the pre-existing TECS II. Today, TECS II and IBIS are maintained by the CBP at DHS.[520]

IBIS exchanges data with CLASS and several immigration systems, including the NAILS II (described above) and the Deportable Alien Control System (DACS), among others. It also allows inspectors to access the FBI's NCIC and National Law Enforcement Telecommunications System (NLETS), as well as the Drug Enforcement Administration's Narcotics and Dangerous Drugs Identification System (NADDIS). The Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), U.S. Secret Service, Internal Revenue Service, and the Royal Canadian Mounted Police (RCMP) also provide lookout records for inclusion in IBIS. Law enforcement and regulatory personnel from 20 other federal agencies use IBIS.

---

[516] Dr. John C. Hermansen, Name-Recognition Technology Aids the Fight Against Terrorism, Journal of Counterterrorism & Homeland Security International (winter 2003), p. 2.

[517] Briefing with the U.S. Customs Service, Nov. 16, 2001.

[518] §4604 of P.L. 100-690, 102 Stat. 4289.

[519] In is notable that at land border ports of entry during primary inspections, the border inspectors do not enter the names and other pertinent biographic identifiers of border crossers who arrive in private conveyance into IBIS. Instead, the inspectors enter vehicle license plate numbers into IBIS and visually scan the border crossers' travel documents.

[520] Under an administrative reorganization within the DHS, INS enforcement programs were merged with Customs, and reconstituted as the CBP and the ICE. Both Customs and Immigration Inspectors are now part of CBP.

In addition, the Advanced Passenger Inspection System (APIS) was grafted onto IBIS to establish alien entry/exit control in the airport environment (as opposed to land border and sea ports). As required by the Border Security Act (P.L. 107-173), the DHS has rolled out the U.S. VISIT program, a newly developed automated entry/exit control system that includes scanners and readers to verify and collect biometric information on foreign travelers.[521] Under the U.S. VISIT program, IBIS and the APIS interface with two systems with biometric capabilities, IDENT and the Consular Consolidated Database.

As in NAILS II, the name search capability in IBIS is Soundex. While IBIS is considered superior to NAILS II in terms of systems performance and name recognition, it is not considered as robust as the CLASS system in terms of certain search functions. There are about 16 million records in IBIS, including nearly 80,000 records on known and suspected terrorists. In regard to IBIS another key issue for Congress is systems availability. There have been press accounts that IBIS has been inaccessible at certain ports of entry for extended periods of time, during which allegedly foreign travelers were not screened against watch lists.[522]

Computer Assisted Passenger Profiling System (CAPPS)[523]

TSA administers the CAPPS system, a classified system, which includes a "selectee" process and a "no fly" list. The operational concept underlying CAPPS is to select "high-risk" travelers based on ticket purchasing patterns, among other things, for greater scrutiny in terms of body and baggage searches, while expediting processing for "low-risk" travelers. The "selectee" process is the core of CAPPS. It was authorized in the 1996 Federal Aviation Administration Act.[524] The system was mandated in 1999 by the Federal Aviation Administration, prior to the establishment of TSA, to promote aviation security following several aircraft bombings. In addition, the Aviation and Transportation Security Act[525] authorized the development of a "no fly" list, which is essentially a list of persons who are prohibited from boarding a commercial aircraft for a host of reasons. The actual system, however, was developed and is managed by the airline industry.

---

[521] For further information, see CRS Report RL32234, U.S. Visitor and Immigrant Status Indicator Technology Program (U.S.-VISIT), by Lisa Seghetti and Stephen Vina.

[522] Alfonso Chardy, "Airport Terrorist Database Often Offline; Official Says Backups Are In Place to Prevent Disaster," Miami Herald, Mar. 8, 2002, p. B1.

[523] Federal Register, Aug. 1, 2003, p. 45265.

[524] P.L. 104-848.

[525] See 49 U.S.C. §114(h)(3), or §101 of P.L. 107-71, 115 Stat. 597.

More recently, TSA has been testing a second generation system, CAPPS-II, that, among other things, uses sophisticated algorithms to data mine (search) government and proprietary (commercial) databases to acquire limited background information on air travelers to authenticate their identity. Critics point out that terrorists could "beat" the system by adopting another person's identity. They point to the increasing frequency and ease with which criminals engage in identity fraud. In addition, the system will assign travelers a color coded categorical risk assessment.[526]

- Green-coded passengers would not be considered a risk and would only be subject to basic screening procedures — metal detectors and baggage x-rays.
- Yellow-coded passengers would be deemed either unknown or possible risk, and would be subject to extra screening procedures — bag and body searches.
- Red-coded passengers would be considered high risk and would not be allowed to travel, and law enforcement officials would be notified of their attempts to board commercial aircraft.

Critics, however, decry the cloak of secrecy under which TSA is developing CAPPS II. They assert that identity-based profiling under CAPPS II would result in a loss of privacy that would not be counterbalanced by a corresponding increase in security. Because of these fears, others maintain that transparency is vital to the system's further development and success.[527] Some legal scholars also question whether it would be permissible to prevent a person from boarding an aircraft on a mere suspicion of organizational affiliation.[528]

Congress, meanwhile, included Section 519 in the FY2004 Homeland Security Appropriations Act,[529] which prohibits the expenditure of any funding provided under that act to deploy or implement this new system until it has been evaluated by GAO. Since then, GAO has reported that the development of this system is behind schedule, and TSA has encountered major impediments in testing CAPPS II. In particular, the European Union and commercial airlines have been reluctant to hand over crucial data because of privacy concerns. Moreover, GAO underscored that the CAPPS II, as designed, would be vulnerable to terrorists

---

[526] Federal Register, Aug. 1, 2003, p. 45266.

[527] Jill D. Rhodes, "CAPPS II: Red Light, Green Light, or 'Mother, May I?,'" The Homeland Security Journal, Mar. 2004, p. 1.

[528] Ibid., p. 7.

[529] P.L. 108-90, 117 Stat. 1137.

who adopted (stole) another person's identity.[530] TSA anticipates that CAPPS-II will be integrated with USVISIT, DHS's newly developed automated entry/exit control program.[531] Such a measure would introduce a biometric component into the CAPPS-II process for noncitizens, so that their identities could be confirmed with greater certainty.

National Crime Information Center (NCIC)[532]

The FBI maintains the NCIC, a national computer database for criminal justice records. NCIC is linked to an index system — the Interstate Identification Index (III), which points authorized law enforcement authorities to federal, state, and local criminal records. In 1999, NCIC 2000 was brought online by the FBI. Major improvements built into NCIC 2000 include an improved name search capability, digitized right index finger prints and mug shots, other digitized images (tatoos, scars, or stolen vehicles), a sexual offenders file, an incarcerated persons file, a convicted person on supervised release (probation or parole) file, user manuals on line, information linking capabilities, online system support, and other improvements.

Another major enhancement associated with NCIC 2000 is the ability for patrol officers to receive and send data to the system from their patrol cars or other temporary locations with laptop computers, hand-held fingerprint scanners, or digital cameras. The total budget to develop NCIC 2000 was about $183 million.[533] For FY2003, about $36 million was allocated by the FBI to administer and maintain NCIC 2000.

NCIC 2000 gives law enforcement officers access to over 43 million records: 41 million criminal history records and 2.5 million hot files. Hot files would include lookouts on suspected and known terrorists, which are included in the Violent Gang and Terrorist Organization File (VGTOF). As in IBIS and NAILS II, however, the name recognition technology in NCIC 2000 is Soundex, which is not nearly as robust as the name recognition technologies built into CLASS. For example, the length of the name field in NCIC is only 28 characters, while it is over 80 in CLASS.[534]

---

[530] U.S. General Accounting Office, Aviation Security: Computer-Assisted Passenger Prescreening System Faces Significant Implementation Challenges, GAO-04-385, Feb. 2004, p. 4.

[531] Federal Register, Aug. 1, 2003, p. 45266.

[532] For further information, click on [http://www.fbi.gov/hq/cjisd/ncic.htm].

[533] U.S. Department of Justice, Federal Bureau of Investigation, National Crime Information Center 2000 (Washington, July 15, 1999), p. 3 at [http://www.fbi.gov/pressrel/pressre199/ncic2000.htm].

[534] Briefing with DOS's Bureau of Intelligence and Research, Oct. 23, 2003.

For years, Justice denied the DOS access to NCIC on the grounds that CA was not a law enforcement agency, but State was given authority to access NCIC in the USA PATRIOT Act.[535]

As of August 2002, between 7 to 8 million files on non-U.S. persons with FBI criminal records were added to CLASS from NCIC.[536] When Customs and Immigration inspectors query IBIS in the primary inspection lanes, the system queries NCIC's hot files like the U.S. Marshal Service's want and warrants file and the VGTOF, but full criminal background history checks are only performed when travelers are diverted into secondary inspections for certain irregularities or suspicious behavior. Under HSPD-6, NCIC is the platform on which additional terrorist screening records from the TSC's TSDB have been disseminated to duly authorized state, local, territorial, and tribal law enforcement agencies.[537]

Regional Information Sharing System/Law Enforcement Online[538]

The Regional Information Sharing System (RISS) is an unclassified, but secured web-accessible system of six regional computer networks that were established to share state and local investigative data involving criminal gangs and drug trafficking.[539] RISS is funded through the DOJ Office of Justice Programs, but is administered and operated jointly by several state agencies.

Section 701 of the USA PATRIOT Act[540] amends the Omnibus Crime Control and Safe Streets Act of 1968 to authorize the use of RISS to share investigative data that might involve potential terrorist conspiracies and activities. As required by law, criminal files included in RISS must be based on "probable cause" that the subjects of the file have committed, or are about to commit, a crime.[541] While a

---

[535] See §403(a) of P.L. 107-56, 115 Stat. 343.

[536] U.S. Department of State, Testimony to the Joint Congressional Intelligence Committee Inquiry by Ambassador Francis X. Taylor, Coordinator for Counterterrorism (Washington, Oct. 1, 2002), p. 2.

[537] Memorandum of Understanding accompanying HSPD-6, item 18, p. 5.

[538] For further information, click on [http://www.iir.com/RISS/].

[539] Wilson P. Dizard III, "All Points Bulletin: FBI and Justice Link, Get the Word Out," Post-Newsweek Business Information, Inc. (Lexus/Nexus: Oct. 7, 2003), p. 1. (Hereafter cited as Dizzard, "All Points Bulletin: FBI and Justice Link.").

[540] P.L. 107-56, 115 Stat. 374.

[541] 28 Code of Federal Regulations, § 23.3(b)(3). "Criminal intelligence information means data which has been evaluated to determine that it is relevant to the identification of and the criminal

cigarette bootlegging conspiracy, for example, may appear to have no terrorism nexus, by analyzing investigative data in RISS, other patterns of criminal or terrorist activity may emerge.

Law Enforcement Online (LEO) is a secured web-accessible portfolio of applications and information sources made available by the FBI to state and local law enforcement agencies. More recently, RISS has been merged with the FBI's LEO system. The RISS/LEO merger will facilitate federal/state communications on a secured/web accessible system, as opposed to older teletype systems like the NLETS.[542]

Through RISS/LEO, the FBI will distribute to state and local law enforcement agencies selected open source (unclassified) reports, as well as sensitive but unclassified law enforcement reports. RISS/LEO enjoys considerable support among state and local law enforcement agencies as a user-friendly and web-accessible system.

Biometric Systems for Identity Verification

"Biometrics" are physical characteristics or personal traits of an individual used to identify him, or verify his claim to a certain identity. Examples of biometrics include fingerprints, facial and hand geometry, iris and retina scans, voice recognition, and handwritten signatures. While most biometric technologies have only been developed in the past 10 to 15 years, fingerprints have been used by law enforcement to verify identity for the past century. For these purposes, the FBI maintains the Integrated Automated Fingerprint Identification System (IAFIS), an automated 10-fingerprint matching system that captures rolled prints. All 50 states are connected to IAFIS. With over 47 million sets of fingerprints, it is the largest biometric database in the world.[543]

In 1995, the INS piloted the Automated Biometric Fingerprint Identification System (IDENT) in California. In the following year, IDENT was deployed to over 34 sites on the Southwest border, and over 3,000 criminal aliens were identified attempting to enter the United States. IDENT is a two flat fingerprint system that includes prints of 4.5 million aliens who have been (1) apprehended while attempting to enter the United States illegally between ports of entry or allowed to withdraw their application for admission at a port of entry (4 million records), (2) previously apprehended (300,000 records), or (3) convicted of aggravated felonies (240,000).

---

activity engaged in by an individual who or organization which is reasonably suspected of involvement in criminal activity."

[542] Dizard, "All-Points Bulletin: FBI and Justice Link," p. 1.

[543] U.S. General Accounting Office, Technology Assessment: Using Biometrics for Border Security, GAO-03-174, Nov. 2002, p. 149.

Some Members of Congress, particularly those serving on the Appropriations Committees, were concerned that two incompatible fingerprint identification systems were being developed within the DOJ. This issue became heated following revelations that the INS had apprehended a suspected murderer, Rafael Resendez-Ramirez, but allowed him to voluntarily return to Mexico. Resendez-Ramirez subsequently reentered the United States and committed four additional murders. Language in the FY2000 Commerce-Justice-State appropriations act expressed dismay that other federal, state and local law enforcement officers did not have access to IDENT data. In response, the Attorney General put the IDENT/IAFIS migration project under the supervision of Justice Management Division (JMD).

JMD conducted several pilot programs, which examined the feasibility of interchanging data between the two systems.[544] For example, IAFIS data for individuals in the "wants and warrants" file was downloaded into IDENT. JMD also developed an IDENT/IAFIS workstation that allowed Border Patrol agents and immigration inspectors to run IDENT prints against IAFIS. This system had a 10 minute response time and required agents to process each apprehended person twice, once under IDENT and again through the IDENT/IAFIS work station.

In addition, JMD conducted a criminality study, which examined IDENT records from the 1998 through mid-2000 time frame and found that about 8.5 % of those individuals had some notable charge placed against them.[545] The transfer of the components of the former INS to the DHS, however, has hampered this project. According to the DOJ Office of the Inspector General, despite a delay of two years, a partially integrated version of the IDENT/IAFIS system was available for deployment in December 2003. Full integration and deployment of the system,

---

[544] IDENT is instrumental in identifying how many times an alien has been apprehended. According to the DOJ, however, there are legal concerns, about entering such data into criminal databases like IAFIS for aliens who may have attempted to enter the United States illegally, but were not convicted of a criminal violation. Indeed, most aliens attempting to enter the United States illegally between ports of entry are apprehended up to five to seven times before they are charged with misdemeanor illegal entry. If they are subsequently apprehended, they are charged with felony reentry.

[545] U.S. Department of Justice, Federal Bureau of Investigation, Criminal Justice Information Services (CJIS) Division, "DOJ Agencies Team Up To Improve The Security At U.S. Borders," The CJIS Link (Clarksburg, WV, spring 2002), p. 2.

however, may extend past FY2008.[546] Meanwhile, about 4,500 FBI fingerprint files of known or suspected terrorists have been entered into IDENT.[547]

The DOS, meanwhile, has established the capacity at consular posts abroad to capture electronic records of nonimmigrant visas, including digitized visa photos, which are transmitted and replicated in State's Consolidated Consular Database. In FY2001, DOS and INS conducted a pilot nonimmigrant visa data-sharing program at the Newark International Airport. As part of this program, nonimmigrant visa records were transmitted to IBIS, including digitized photos. These visa photos are useful for identity verification, and reportedly this capability has been deployed at all air ports of entry.

In addition, the DOS has begun testing facial recognition (biometric) technologies with nonimmigrant visa photos as a means to verify identity as well, but these technologies are less mature than those using fingerprint. As a biometric measurement for nonimmigrant visa applicants, however, the DOS strongly favors facial recognition to fingerprints, because it does not require the applicant to submit to an active measurement procedure. In addition, facial recognition biometric measurements can be derived from photos and videotape gathered by the intelligence community in order to identify known terrorists and other persons who may be excludable from the United States for national security reasons.

HSPD-6 directs that the TTIC's TID and the FBI domestic terrorist database incorporate all available biometric data, to the extent permitted by law, including data on persons yet to be identified (e.g., latent prints gathered at a crime scene or the caves of Afghanistan). In addition, these systems are to be designed so that new advancements in biometrics technology can be incorporated into them.

Possible Issues for Congress

While watch lists have long been maintained by law enforcement and border security agencies, the Administration's plans to expand these lists and widen their dissemination raises issues related to individual privacy and the security of the nation. For Congress, several immediate issues have emerged or may emerge, including the following:

- Has the transfer of the TIPOFF terrorist identification function to TTIC and TIPOFF terrorist watch list function to the TSC been accomplished without degrading the capabilities of other governmental entities charged

---

[546] U.S. Department of Justice, Office of the Inspector General, Report No. 1-2003-005, Status of IDENT/IAFIS Integration, (Washington, Feb. 2004), p. 11.

[547] Ibid., 18.

with identifying, screening, and tracking known and suspected terrorists? If not, how and in what way has the system been improved?

- How operational is the TSC at this time? Will the TSDB be fully integrated ("dynamically linked") with the visa issuance, border inspection, commercial aviation security systems by the end of CY2004? Has the Administration committed enough resources to create a single, fully integrated TSDB?
- With the bulk of the Nation's terrorism-related lookout records in a single, integrated TSDB, what measures have and will be taken to insure the security of the TSDB?
- Will the TSC Director have a role in evaluating the security and adequacy of the systems used by screening agencies?
- What measures have been or will be taken to improve the name search capabilities of NCIC and IBIS?
- How expeditiously will the TSC be able to respond to terrorist-related NCIC hits made by state and local law enforcement officers? Is there a bench mark for how long such persons can be stopped for questioning?
- If persons identified as known or suspected terrorists, or their supporters, are not arrested or detained, what governmental entities will be notified of their presence in the United States? What measures will be taken to monitor their whereabouts and activities while in the United States? What other actions might be taken by those to whom the information is disseminated?
- What is the criteria for including persons in the TSDB as suspected or known terrorists, or their supporters? Will sufficient safeguards be put in place to protect constitutional rights? Should policies and guidelines regarding the inclusion of such persons in the TSDB be made public?
- What redress is or will be available to an individual wrongly placed on a watch list? Will there be a formal appeals process? If so, what agency will handle this process?
- What mechanisms will be put in place to audit system users to determine whether they are abusing the system? Should there be associated civil or criminal penalties for such abuse?
- Should Congress consider requiring a statutory authorization for the TSC, the consolidated TSDB, and related activities as a means of assuring greater accountability?
- Are there cultural or tradecraft issues related to information sharing that the FBI and other agencies will need to overcome in order to more effectively share information and properly manage lookout records for other agencies?
- Would the database and watch list functions be better located and consolidated in a single Executive Branch agency with clearer lines of authority and responsibility?
- Finally, are the TSC and TSDB, and by extension the TTIC, temporary or permanent solutions?

Conclusion

There is an emerging consensus that the U.S. intelligence and law enforcement community missed several vital opportunities to watch-list and screen several conspirators involved in the September 11, 2001 terrorist attacks. Under HSPD-6, the Bush Administration has taken steps to elevate and expand terrorist identification and watch-list functions. These measures, if effectively implemented, will better equip the U.S. government to screen and monitor the whereabouts of known and suspected terrorists, and their supporters. Furthermore, working from common terrorist identities and watch list databases could be an effective mechanism to break down institutional and cultural firewalls and promote greater interagency cooperation and data sharing.

Conversely, as the U.S. government pursues a more aggressive policy in identifying and watch-listing known and suspected terrorists, and their supporters, there is significant potential for a corresponding loss of privacy and an erosion of civil liberties. While the Administration asserts that such information will be collected according to preexisting authorities and individual agency policies and procedures, it is inevitable that individuals will be misidentified. In such cases, most would agree that it will be incumbent upon the U.S. government to act swiftly to correct such mistakes, and perhaps compensate those individuals for their inconveniences or possible damages.

Establishing a TSDB by merging watch lists will not likely require integrating entire systems. Nonetheless, there are likely to be technological impediments to merging watch list records. From system to system, and watch list to watch list, there remains no standardization of data elements, such as, name, date of birth, place of birth, or nationality. In the past decade, moreover, digitized biometrics (principally fingerprints) have been developed to identify individuals with greater certainty, but most biometric systems have been developed separately from other systems. Integrating data from biometric systems into either the TID or the TSDB could be technologically difficult and costly.

Under HSPD-6, the Administration has established the TSC as a "multi-agency effort." At the same time, establishing a consolidated TSDB and effectively disseminating lookout records to screening agencies, including state and local law enforcement, is not likely to be a small or short-term endeavor. At this time, congressional input into this process is confined to oversight by several congressional committees and appropriating funding to several participating agencies.

Appendix A. Frequently Used Abbreviations

To aid the reader, the following list of abbreviations is provided.

APIS - Advanced Passenger Information System
CA - Bureau of Consular Affairs
CAPPS - Computer Assisted Passenger Profiling System

CIA - Central Intelligence Agency
CBP - Bureau of Customs and Border Protection
CLASS - Consular Lookout and Support System
CT Watch - Counterterrorism Watch
CTC - CIA's Counterterrorism Center
CTD - FBI's Counterterrorism Division
DCI - Director of Central Intelligence
DHS - Department of Homeland Security
DIA - Defense Intelligence Agency
DOD - Department of Defense
DOJ = Department of Justice
DOL - Department of Labor
DOS - Department of State
FBI - Federal Bureau of Investigation
FOIA - Freedom of Information Act
FTTTF - Foreign Terrorist Tracking Task Force
HSPD-6 - Homeland Security Presidential Directive 6
IAFIS - Integrated Automated Fingerprint Inspection System
IAIP - Information Analysis and Infrastructure Protection Directorate
IBIS - Interagency Border Inspection System
ICE - Bureau of Immigration and Customs Enforcement
IDENT - Automated Biometric Fingerprint Identification System
INA - Immigration and Nationality Act
INR - Bureau of Intelligence and Research
INS - Immigration and Naturalization Service
JMD - Justice Management Division
JTTF - Joint Terrorism Task Force
LEO - Law Enforcement Online
MOU - Memorandum of Understanding
NAILS II - National Automated Border Inspection System II
NSA - National Security Agency
NCIC - National Crime Information Center
NJTTF - National Joint Terrorist Task Force
NTC - National Targeting Center
RISS - Regional Information Sharing System
TID - Terrorist Identities Database
TSA - Transportation Security Administration
TSC - Terrorist Screening Center
TSDB - Terrorist Screening Database
TTIC - Terrorism Threat Integration Center
U.S.-VISIT - U.S. Visitor and Immigrant Status Indicator Technology Program
VGTOF - Violent Crime and Terrorist Organization Fil

Terrorist Watchlist Checks and Air Passenger Prescreening, RL33645 (December 30, 2009).

WILLIAM J. KROUSE, CONGRESSIONAL RESEARCH SERV., TERRORIST WATCHLIST CHECKS AND AIR PASSENGER PRESCREENING (2009), *available at* http://www.intelligencelaw.com/library/secondary/crs/pdf/RL33645_12-30-2009.pdf.

William J. Krouse
Specialist in Domestic Security and Crime Policy
wkrouse@crs.loc.gov, 7-2225

Bart Elias
Specialist in Aviation Policy
belias@crs.loc.gov, 7-7771

December 30, 2009

Congressional Research Service

7-5700
www.crs.gov
RL33645

Summary

Considerable controversy continues to surround U.S. air passenger prescreening and terrorist watchlist checks. In the past, such controversy centered around diverted international flights and misidentified passengers. Another issue surfaced on Christmas Day 2009, when an air passenger attempted to ignite an explosive device on a Detroit-bound flight from Amsterdam. Although U.S. counterterrorism officials reportedly had created a record on the air passenger in the Terrorist Identities Datamart Environment (TIDE), which is maintained at the National Counterterrorism Center (NCTC), it does not appear that the NCTC ever nominated him for entry into the U.S. government's consolidated Terrorist Screening Database, which is maintained at the Terrorist Screening Center. Therefore, he would not have been placed on watchlists used by front-line, air passenger prescreening agencies, principally the Department of Homeland Security (DHS), Transportation Security Administration (TSA), and Customs and Border Protection (CBP).

Under Homeland Security Presidential Directive 6, the Terrorist Screening Center (TSC) was established as a multiagency collaborative effort administered by the Federal Bureau of Investigation (FBI). The TSC maintains a consolidated Terrorist Screening Database (TSDB). The TSC distributes TSDB-generated

terrorist watch lists to frontline screening agencies that conform with the missions and legal authorities under which those agencies operate. In addition, the TSC has developed comprehensive procedures for handling encounters with known and suspected terrorists and their supporters, and provides terrorist screening agencies with aroundthe-clock operational support in the event of possible terrorist encounters.

CBP uses the Advanced Passenger Information System (APIS) to capture personal identity and travel information on international travelers (both citizens and noncitizens) from passenger manifests provided by air carriers and vessel operators. For the purposes of both border and transportation security, CBP vets that information in most cases prior to departure against several terrorist watchlists that are subsets of the TSDB. More recently, TSA has positioned itself through the Secure Flight program to receive similar data through the DHS APIS portal to vet domestic aircraft and vessel passengers against terrorist watch lists, also prior to departure. In time, TSA will assume from CBP transportation security-related terrorist watch list vetting for international aircraft and vessel passengers as well.

In addition, both CBP and TSA capture selected elements of passenger name record (PNR) information that is used to focus inspection and screening resources more efficiently on high-risk individuals at either international ports of entries upon arrival at a U.S. port of entry or at airport security checkpoints prior U.S. air carrier flights. For these purposes, CBP administers the Automated Targeting System-Passenger and TSA administers the Computer-Assisted Passenger Prescreening System. Furthermore, to handle and resolve the complaints of passengers and meet these statutory requirements, the DHS has established the DHS Traveler Redress Inquiry Program (TRIP) as a mechanism for addressing watchlist misidentification issues and other situations where passengers feel that they have been unfairly or incorrectly delayed or denied boarding.

Congress addressed related terrorist watch-listing and screening issues in the Implementing Recommendations of the 9/11 Commission Act of 2007 (P.L. 110-53) and the Intelligence Reform and Terrorism Prevention Act (P.L. 108-458). In the 111th Congress, the House passed the FAST Redress Act of 2009 (H.R. 559), a bill that addresses air passenger watch list misidentifications.

Introduction

Considerable controversy surrounds U.S. air passenger prescreening processes and terrorist watchlist checks. On Christmas Day 2009, an air passenger, Umar Farouk Abdulmutallab, allegedly attempted to ignite an explosive device while traveling from Amsterdam on board a Detroit-bound commercial airliner (Northwest Airlines Flight 253). Based on a tip provided by Abdulmutallab's father, U.S. counterterrorism officials reportedly had created a record on Abdulmutallab in mid-November in the Terrorist Identities Datamart

Enviornment (TIDE), which is maintained at the National Counterterrorism Center (NCTC).[548] It does not appear, however, that the NCTC ever nominated Abdulmutallab for entry into the U.S. government's consolidated Terrorist Screening Database, which is maintained by the Federal Bureau of Investigation (FBI) at the Terrorist Screening Center. Therefore, he would not have been placed on the Transportation Security Administration (TSA) "No Fly" list or any other watchlist used by other front-line screening agencies. Consequently, this incident has generated questions about "watch-list" procedures. Although those procedures are largely classified, this report provides an overview of recent efforts to improve terrorist watchlist checks and air passenger prescreening.

The incident also raises a new policy issues regarding the interaction between these broader terrorist databases and systems and the "No-Fly" and selectee lists maintained by the Transportation Security Administration (TSA) for prescreening airline passengers, as well as the relationship between passenger prescreening processes and screening procedures to detect explosives and other threat items at airport checkpoints.[549]

Background: HSPD-6 and Terrorist Screening

In September 2003, then-President George W. Bush issued Homeland Security Presidential Directive 6 (HSPD-6), establishing a Terrorist Screening Center to consolidate the U.S. government's approach to terrorist watch-listing and screening.[550] To this end, certain terrorist identification and watchlist functions, which were previously performed by the Department of State's (DOS's) Bureau of Intelligence and Research (INR), were transferred to the newly established Terrorist Screening Center and the Terrorist Threat Integration Center (TTIC)—today the National Counterterrorism Center (NCTC).

NCTC and Terrorist Identification

The NCTC serves as the central hub for the fusion and analysis of information collected from all foreign and domestic sources on international terrorist threats. Under the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458), the NCTC was placed under the newly created Office of the Director of National Intelligence (ODNI). Prior to this legislation and HSPD-6, however, the nation's principal international terrorist watchlist, known as TIPOFF, was

---

[548] Dan Eggen, Karen DeYoung, and Spencer S. Hsu, "Plane Suspect Was Listed in Terror Database After Father Alerted U.S. Officials," Washington Post, December 27, 2009, p. A01.

[549] For further information, see CRS Report R40543, Airport Passenger Screening: Background and Issues for Congress, by Bart Elias.

[550] The White House, Homeland Security Presidential Directive/HSPD-6, Subject: Integration and Use of Screening Information (Washington, September 16, 2003).

maintained by DOS's INR.[551] Under HSPD-6, TIPOFF was officially transferred to the TTIC on September 16, 2003. Nearly a year later, the President established the NCTC by executive order on the foundations of the TTIC.[552] The NCTC continued TTIC's efforts to establish a much more expansive database on international terrorists.

Based partly on TIPOFF, the NCTC currently maintains a Terrorist Identities Datamart Environment (TIDE)—designated under HSPD-6 to be the single repository into which all international terrorist-related data available to the U.S. government are stored. In February 2006, TIDE included over 325,000 terrorist-related records.[553] By August 2008, TIDE had grown to "more than 540,000 names, but only 450,000 separate identities because of the use of aliases and name variants."[554] Less than 5% of those records purportedly pertain to U.S. persons (i.e., citizens or legal permanent residents of the United States).[555]

An effective watchlist process is contingent on Intelligence Community[556] agencies sharing information on known and suspected international terrorists and their supporters with NCTC and, in turn, the NCTC nominating those persons for inclusion in the U.S. government's consolidated terrorist screening database (see Figure 1 above).

---

[551] Prior to HSPD-6, INR-generated TIPOFF records were distributed to DOS's Bureau of Consular Affairs (CA), as well as to border screening agencies, for inclusion in the Consular Lookout and Support System (CLASS), the Interagency Border Inspection System (IBIS), and the National Automated Immigration Lookout System (NAILS). For further information, see CRS Report RL31019, Terrorism: Automated Lookout Systems and Border Security Options and Issues, by William J. Krouse and Raphael Perl. See also CRS Report RL32366, Terrorist Identification, Screening, and Tracking Under Homeland Security Presidential Directive 6, by William J. Krouse.

[552] Executive Order 13354, "National Counterterrorism Center," 69 Federal Register 53589, Sept. 1, 2004.

[553] Walter Pincus and Dan Eggen, "325,000 Names on Terrorism List: Rights Groups Say Database May Include Innocent People," Washington Post, February 15, 2006, p. A01.

[554] National Counterterrorism Center, Terrorist Identities Datamart Environment (TIDE), August 2008.

[555] Ibid.

[556] The Intelligence Community includes the Central Intelligence Agency (CIA); the National Security Agency (NSA); the Defense Intelligence Agency (DIA); the National Geospatial-Intelligence Agency (GIA); the National Reconnaissance Office (NRO); the other DOD offices that specialize in national intelligence through reconnaissance programs; the intelligence components of the Army, Navy, Air Force, and Marine Corps, the FBI, the Department of Energy, and the Coast Guard; the INR at the DOS, the Office of Intelligence and Analysis at Department of the Treasury, and elements of the DHS that are concerned with the analyses of foreign intelligence information (50 U.S.C. §401a(4)).

TSC and Terrorist Watch-Listing and Screening

For the purposes of watch-listing, the FBI-administered Terrorist Screening Center (TSC) maintains the consolidated Terrorist Screening Database (TSDB). The NCTC provides international terrorism data and the FBI provides domestic terrorism data for inclusion in the TSDB. Both sets of data are merged in the consolidated TSDB maintained by the TSC. According to the FBI, international terrorists include those persons who carry out terrorist activities under foreign direction. For this purpose, they may include citizens or noncitizens, under the rationale that citizens could be recruited by foreign terrorist groups. Or noncitizens (aliens) could immigrate to the United States and naturalize (become citizens), having been unidentified terrorists before entry, or having been recruited as terrorists sometime after their entry into the United States.

By comparison, domestic terrorists are not under foreign direction and operate entirely within the United States. According to the Administration, both sets of data (on international and domestic terrorists) will include, when appropriate, information on "United States persons."[557] Criteria for the inclusion of U.S. persons in the database was developed by an interagency working group. The term "United States persons" includes U.S. citizens and legal permanent residents (immigrants). In June 2005, DOJ OIG issued an audit, reporting that the TSC had established a single consolidated TSDB, as recommended by GAO,[558] but with some difficulties.[559] Among other things, the TSDB had not been completely audited to ensure that its records were complete and accurate.

As of September 2008, the TSDB contained 400,000 individual identities, of which 3% are U.S. persons.[560] Due to aliases and name variants, however, the TSDB includes over one million records on those individuals.[561] The TSC

---

[557] The definition of "United States person" is found at 50 U.S.C. §1801(i): a citizen of the United States, an alien lawfully admitted for permanent residence (as defined §1101(a)(2) of Title 8), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation that is incorporated in the United States, but does not include a corporation or an association that is a foreign power, as defined in subsection (a)(1), (2), or (3) of this section.

[558] U.S. General Accounting Office, Information Technology: Terrorist Watch Lists Should Be Consolidated to Promote Better Integration and Sharing, GAO Report GAO-03-322 (April 2003).

[559] U.S. Department of Justice, Office of the Inspector General, Audit Division, Review of the Terrorist Screening Center, Audit Report 05-27, (Washington, June 2005), 160 pp.

[560] Written Statement of Rick Kopel, Principal Deputy Director, Terrorist Screening Center, Before the House Committee on Homeland Security, Subcommittee on Transportation Security and Infrastructure Protection, September 9, 2008, p. 4.

[561] Ibid.

distributes TSDB-generated terrorist watchlists to frontline screening agencies that conform with the missions and legal authorities under which those agencies operate. Consequently, these watchlists (e.g., the TSA's No Fly and Automatic Selectee lists) are in some cases only subsets of the TSDB.

In addition, the TSC has developed comprehensive procedures for handling encounters with known and suspected terrorists and their supporters, and provides terrorist screening agencies with around-the-clock operational support in the event of possible terrorist encounters. For example, TSDB-generated lookout records were and are currently being disseminated to state, local and tribal law enforcement officers through the National Crime Information Center (NCIC, see Figure 1 above). The unclassified portion of some, but not all, TSDB-generated lookout records (name, date of birth, passport number, and country of origin) are loaded into the NCIC's Violent Gang and Terrorist Offender File (VGTOF). Similar look out records are also shared with the Department of Defense and selected foreign governments. In addition, the TSC supports the terrorist screening activities of TSA and U.S. Customs and Border Protection (CBP), as well as the Department of State's Bureau of Consular Affairs (CA).

9/11 Commission and Integrated Terrorist Travel Strategy

In July 2004, the National Commission on Terrorist Attacks upon the United States (9/11 Commission) made air passenger prescreening- and terrorist travel-related findings and recommendations in its final report. Shortly thereafter, the TSA unveiled the "Secure Flight" domestic air passenger prescreening program (described below),[562] and the Administration issued Homeland Security Presidential Directive 11 (HSPD-11), calling for "comprehensive terrorist-related screening procedures."[563]

Among other things, the 9/11 Commission concluded that disrupting terrorist travel was as powerful a weapon as targeting their money.[564] The 9/11 Commission found, however, that prior to the 9/11 attacks, the intelligence community did not view watch-listing as integral to intelligence work.[565] To prevent future terrorist attacks, the 9/11 Commission recommended that the

---

[562] U.S. Department of Homeland Security, Transportation Security Administration, "TSA To Test New Passenger Pre-Screening System" (Washington, August 26, 2004), 2 pp.

[563] The White House, Homeland Security Presidential Directive/HSPD-11, Subject: Comprehensive Terrorist-Related Screening Procedures (Washington, August 27, 2004).

[564] National Commission on Terrorist Attacks upon the United States, The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States, (Washington, 2004), p. 385.

[565] National Commission on Terrorist Attacks upon the United States, "Three 9/11 Hijackers: Identification, Watchlisting, and Tracking," Staff Statement no. 2, (Washington, 2004), p. 1.

United States expand terrorist travel intelligence and countermeasures,[566] and that the U.S. border security systems be integrated with other systems to expand the network of screening points to include the nation's transportation systems and access to vital facilities.[567]

To increase aviation security, the 9/11 Commission recommended that Congress and TSA give priority to screening passengers for explosives.[568] At a minimum, the 9/11 Commission recommended that all passengers referred to secondary screening be thoroughly checked for explosives.[569] Arguably, this necessitates a robust process to carefully select only those passengers believed to pose the greatest risk to aviation security, while minimizing false positives. To improve air passenger prescreening, the 9/11 Commission recommended that

- the "no-fly" and "automatic selectee" watchlists used to screen air passengers be improved without delay;
- the actual screening process be transferred from U.S. air carriers to TSA;
- air passengers be screened against the larger set of U.S. government watchlists (principally the TSDB); and
- air carriers be required to supply the needed information to test and implement air passenger prescreening.[570]

As described below, both the Administration and Congress acted to implement the 9/11 Commission's recommendations and establish an integrated strategy to disrupt terrorist travel, but the results to date have been mixed.[571]

CBP and TSA and International Air Passenger Prescreening

At air and sea ports of entry, CBP uses the Advanced Passenger Information System (APIS) to capture personal identity and travel information on international travelers (both citizens and noncitizens) from passenger manifests provided by air carriers and vessel operators. For the purposes of both border and transportation security, CBP vets that information in most cases prior to

---

[566] The 9/11 Commission Final Report, p. 385.

[567] Ibid., p. 387.

[568] Ibid., p. 393. Also, for further information, see CRS Report RS21920, Detection of Explosives on Airline Passengers: Recommendation of the 9/11 Commission and Related Issues, by Dana A. Shea and Daniel Morgan.

[569] Ibid., p. 393.

[570] Ibid.

[571] Jonathan Alter, "Plugging Holes in the Skies: The Terrorists Used Airplanes as Weapons in 9/11. So Why Haven't We Made Travel Safer by Now?" Newsweek, August 21-28, 2006, p. 50.

departure against several terrorist watchlists that are subsets of the TSDB. In addition, both CBP and TSA capture selected elements of passenger name record (PNR) information that is used to focus inspection and screening resources more efficiently on high-risk individuals at either international ports of entries upon arrival at a U.S. port of entry or at airport security checkpoints prior U.S. air carrier flights. For these purposes, CBP administers the Automated Targeting System-Passenger and TSA administers the Computer-Assisted Passenger Prescreening System.

Under current practice, airlines transfer manifest data through CBP's APIS several times prior to departure as it becomes available; however, final advanced passenger information (API) data were sometimes not transferred until after the flight has departed (wheels up). In several cases, known and suspected terrorists have been allowed to board aircraft at airports abroad and, subsequently, this led to costly diversions when air carriers were prevented from entering U.S. airspace or continuing to their destinations. Several of these incidents generated significant press coverage in 2004.[572] As described below, CBP issued new regulations (effective February 18, 2008) that require all international air carriers and vessel operators to provide CBP with API data in advance of an aircraft's departure.

More recently, TSA has positioned itself through the Secure Flight program to receive similar data through the DHS APIS portal to vet domestic aircraft and vessel passengers against terrorist and other watchlists, also prior to departure. As originally conceived, the Secure Flight program included an element to select passengers for greater screening at passenger checkpoints based on certain characteristics gleaned from API and PNR data. This element of Secure Flight was modeled to some extent on a controversial program known as the Computer-Assisted Passenger Prescreening System (CAPPS), but is similar to CBP's Automated Targeting System (ATS). Both systems are described below. Although TSA has scrapped this element from its Secure Flight plan, there are no plans to discontinue CAPPS. In addition, under the Secure Flight program, TSA will assume from CBP in time transportation security-related terrorist watchlist vetting for international aircraft and vessel passengers as well.

CBP's National Targeting Center (NTC) confers with TSC representatives to resolve potential watchlist matches. Despite close cooperation between CBP's NTC and the FBI-administered TSC, as has been the case for TSA and domestic flights, CBP misidentifications on international flights have also generated some

---

[572] See David Leppard, "Terror Plot To Attack US with BA Jets," Sunday Times (London), January 4, 2004, p. 1; Sara Kehaulani Goo, "Cat Stevens Held After DC Flight Diverted," Washington Post, September 22, 2004, p. A10; and "US-Bound Air France Flight Diverted Due to Passenger," Agence France Presse, November 21, 2004.

controversy.[573] Despite these difficulties, the 9/11 Commission made several recommendations to increase such data sharing and strengthen air passenger prescreening against TSC-maintained watchlists. Some of these were reflected in provisions that Congress included in the Intelligence Reform and Terrorism Prevention Act (P.L. 108-458). The air passenger prescreening provisions in this law are discussed generally below.

CBP and Advanced Passenger Information System (APIS)

CBP administers APIS to allow international air carriers and vessel operators to transmit data collected from aircraft and ship manifests on passengers and crew members in an electronic format to the CBP Data Center. API data includes both personal identity information and other travel information. Personal identity information is usually collected electronically by air carriers and vessel operators, as well as travel agents, from the Machine Readable Zone (MRZ) on a person's passport or other travel document. It includes, but is not limited to, a person's full name, date of birth, gender, country of residence, and country of citizenship. Additional travel data elements are also collected from passenger and crew manifests. Those travel data elements include carrier code, port of first arrival, status on board an aircraft or vessel, data and time of arrival, and foreign port code. For a complete list of API data elements, see Appendix A.

Through the Treasury Enforcement Communications System (TECS),[574] CBP cross-references API data against law enforcement, customs, and immigration screening systems/databases, as well as terrorist watchlists that have been exported from the U.S. government's consolidated TSDB.

Terrorist Watchlist Checks and Post 9/11 Statutory Mandates

Prior to the 9/11 attacks, API data were collected voluntarily to streamline and expedite the clearance process for law-abiding passengers at international ports of entry.[575] Following those attacks, however, the collection and transmission of API data was mandated under both the Aviation Transportation Security Act of

---

[573] Niraj Warikoo, "Doctor Says He's Profiled At Airports: Beverly Hills Man Joins Class Action vs. Government," Detroit Free Press, June 20, 2006. Jeff Coen, "ACLU Expands Profiling Lawsuit," Chicago Tribune, June 20, 2006, p. C6.

[574] In the APIS System of Records Notification (SORN), DHS described TECS as an "Information Technology platform." See U.S. Department of Homeland Security, Privacy Office, "Privacy Act of 1974; Customs and Border Protection Advanced Passenger Information System Systems of Record," 73 Federal Register, pp. 68435-68439, November 18, 2008.

[575] In 1988, the legacy U.S. Customs Service developed APIS as a module of TECS, in cooperation with the legacy Immigration and Naturalization Service.

2001 (ATSA)[576] for commercial passenger flights arriving in the United States and the Enhanced Border Security and Visa Entry Reform Act of 2002 (EBSVERA) for flights and vessels arriving in and departing from the United States.[577] In line with the recommendations of the 9/11 Commission, Congress included in the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) several provisions related to terrorist watchlist screening. Those provisions require

- DHS to perform preflight terrorist watchlist screening for all passengers and crew onboard aircraft bound for or departing from the United States (Section 4012(a)(6));
- TSA to screen preflight all passengers and crew on domestic flights (Section 4012(a)(1)); and
- DHS to conduct watchlist screening for passengers and crew on cruise ships and other ocean-going vessels (Section 4071).[578]

APIS Pre-departure/Pre-arrival Final Rule

Effective on February 18, 2008, all international air carriers and vessel operators are required to provide CBP with API data in advance of an aircraft's departure or vessel's departure/arrival, depending on the vessel's port of origin (U.S. or foreign).[579] Air carriers have two methods for providing this information: (1) "APIS 30" allows operators to submit passenger and crew manifests in batch form by an interactive or non-interactive method no later than 30 minutes prior to securing aircraft doors for departure; (2) "APIS Interactive Quick Query" allows transmission of manifest information as each passenger checks in, up to, but no later than, the time aircraft doors are secured. In line with best practices, air carriers are also encouraged to transmit available APIS data 72 hours prior to a flight. For sea-and ocean-going vessels departing the United States, vessel operators are required to transmit API data 60 minutes prior to departure. For vessels departing foreign ports that are destined for U.S. ports, vessel operators are required to transmit API data no less than 24 hours before arrival and no greater than 96 hours before arrival.

[576] P.L. 107-71; November 19, 2001; 115 Stat. 597; Section 115.

[577] P.L. 107-173; May 14, 2002; 116 Stat. 543; Section 402.

[578] P.L. 108-458; December 17, 2004; 118 Stat. 3638.

[579] U.S. Department of Homeland Security, Bureau of Customs and Border Protection, "Advance Electronic Transmission of Passenger and Crew Member Manifests for Commercial Aircraft and Vessels," Final rule, 72 Federal Register, pp. 48320-48353, August 23, 2007.

DHS issued a privacy impact assessment for APIS on August 8, 2007.[580] API data for all persons are copied to the Border Crossing Information System (BCIS). For noncitizens, API data are copied to the Arrival and Departure Information System (ADIS) as part of the US-VISIT requirements.[581] Both systems are modules that reside on TECS.

CBP and the Automated Targeting System (ATS)

Given the volume of people and goods seeking entry into the United States every year, it is impractical to physically inspect every person or shipment that arrives at a U.S. port or entry.[582] Therefore, in the mid-1990s, the legacy U.S. Customs Service developed a decision support tool known as the Automated Targeting System (ATS) to assist border inspectors with interdicting illegal drugs and other contraband.[583] Prior to the 9/11 attacks, the scope of ATS was reportedly limited to parties (custom brokers, freight forwarders, and trucking/shipping companies) and cargoes that were associated with past criminality that raised the suspicions of customs authorities.[584] After the 9/11 attacks, ATS was reconfigured and its scope widened to target known and suspected terrorists and terrorist activities as well, by assigning risk assessments to conveyances and cargo, and selecting passengers for enhanced screening.[585]

ATS Modules

[580] U.S. Department of Homeland Security, Privacy Impact Assessment for the Advance Passenger Information System (APIS), August 8, 2007, 23 pp.

[581] DHS has developed the US-VISIT program to more accurately identify and screen non-citizen border-crossers. Congress first mandated that the former Immigration and Naturalization Service (INS) implement an automated entry and exit data system that would track the arrival and departure of every alien in §110 of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (IIRIRA; P.L. 104-208). The objective for an automated entry and exit data system was, in part, to develop a mechanism that would be able to track nonimmigrants who overstayed their visas as part of a broader emphasis on immigration control. Following the September 11, 2001 terrorist attacks, however, there was a marked shift in priority for implementing an automated entry and exit data system. While the tracking of nonimmigrants who overstayed their visas remained an important goal of the system, border security and the identification of potential terrorists have become the paramount concerns with respect to implementing the system.

[582] In FY2008, at 327 ports of entry, CBP processed 409 million pedestrians and passengers, 121 million conveyances, and 29 trade entries. CBP also collected approximately $34.5 billion in revenue, apprehended 723,825 aliens attempting to enter the United States illegally, and seized nearly 3.1 million pounds of illegal narcotics. Source: CBP, Performance and Accountability Report, FY2008, December 4, 2008, p. 6.

[583] CBP briefing provided to CRS on November 24, 2008.

[584] Ibid.

[585] Ibid.

Today, CBP's NTC uses ATS to analyze trade data and cargo, crew, and passenger manifest information to "target" its inspection resources toward persons and cargo shipments that potentially pose the highest risk. The NTC was established in November 2001 with the primary mission of providing "round-the-clock tactical targeting and analytical support for CBP's counterterrorism efforts."[586] At the NTC, intelligence from other federal agencies, in the form of "lookouts," and other law enforcement and intelligence reporting are also reviewed. ATS consists of six modules that include

- ATS-Inbound for importers, cargoes, and conveyances (rail, truck, ship, and air);
- ATS-Outbound for exporters, cargoes, and conveyances (rail, truck, ship, and air);
- ATS-Passenger for passengers and crew entering and departing the United States (air, ship, and rail);
- ATS-Land for vehicles and persons entering the United States at land border ports of entry;
- ATS-International for information sharing and cargo targeting with foreign customs authorities; and
- ATS-Trend Analysis and Analytical Selectivity for selective targeting based on trend analysis.[587]

With the exception of ATS-Passenger, these modules employ weighted rule sets to assign scores, identifying high-risk conveyances and cargo shipments.[588] Above a certain threshold risk score, conveyances and cargo are subject to further inspection at international ports of entry.[589]

Passenger Name Records and ATS-P

In the air and sea passenger environment, CBP requires international air carriers and vessel operators to transmit passenger name record (PNR) data to the NTC. Like API data, PNR data are collected by air carriers and vessel operators in their automated reservation or departure control systems. Although there is some overlap between the API and PNR data, most PNR data would not be included typically on a passenger or crew manifest. While PNR data have been submitted

[586] National Counterterrorism Center, National Strategy to Combat Terrorist Travel, May 2, 2006, p. 28.

[587] U.S. Department of Homeland Security, Privacy Impact Assessment for the Automated Targeting System, August 3, 2007, p. 7.

[588] Ibid.

[589] National targeting thresholds are set by the NTC and are constantly evaluated and adjusted in response to intelligence and analysis.

voluntarily by air carriers since 1997, CBP reports that it collects these data currently as part of its border enforcement mission and pursuant to the Aviation and Transportation Security Act of 2001 (P.L. 107-71).[590] PNR data includes, but is not limited to, date of reservation/ticket issuance, dates of intended travel, payment and billing information, travel agency/travel agent, baggage information, and PNR specific travel itinerary. On July 26, 2007, after considerable negotiations, the European Union and the United States reached a permanent agreement, under which 19 types of PNR data are being collected.[591] PNR data is to be maintained by CBP for seven years in an active file and eight years thereafter in a dormant file.[592] According to then-Secretary Michael Chertoff, DHS has agreed to data protections that meet the privacy standards of both the European Union and United States.[593] For a complete list of PNR data elements under the EU-U.S. agreement, see Appendix B. For an overview of the events leading up to this agreement, see Appendix C.

Through the ATS-Passenger, CBP compares and analyzes PNR data by comparing it to several law enforcement, customs, and immigration systems/databases that include, but are not limited, to the following:

- Advanced Passenger Information System (APIS),
- Nonimmigrant Information System (NIIS),
- Suspect and Violater Indices (SAVI),
- Border Crossing Information System (BCIS),
- Department of State visa databases,
- TECS seizure data, and
- terrorist watchlists that are subsets of the U.S. government's Terrorist Screening Database.[594]

In DHS's ATS Privacy Impact Assessment, the department underscored that ATS-Passenger uses the same methodology for all individuals, a practice that arguably precludes the possibility of disparate treatment of individuals or

---

[590] U.S. Department of Homeland Security, Privacy Impact Assessment for the Automated Targeting System, August 3, 2007, p. 3.

[591] U.S. Department of Homeland Security, Statement By Homeland Security Secretary Michael Chertoff On A New Agreement With The European Union for Passenger Name Record Data Sharing, July 26, 2007.

[592] Ibid.

[593] Ibid.

[594] U.S. Department of Homeland Security, Privacy Impact Assessment for the Automated Targeting System, August 3, 2007, p. 5.

groups.[595] ATS-Passenger, moreover, does not assign a score to determine an individual's risk. Rather, it compares PNR data for all travelers against the systems/databases listed above to identify matches with law enforcement lookouts as well as patterns of suspicious activity that have been discerned through past investigations and intelligence.[596]

In conclusion, ATS-Passenger enables DHS to distinguish those passengers who may pose a risk earlier and in ways that would be impossible during primary inspection at a port of entry.[597] DHS claims that these efforts have had measurable success, resulting in the identification of known and suspected terrorists in addition to other criminals such as narcotics smugglers, travelers with fraudulent documents, and lost/stolen passports, all of whom would have otherwise gone undetected.[598] As described below, the FAA also developed a similar decision support tool in the mid-1990s known as CAPPS, which has been inherited by TSA.

TSA "No Fly" and "Automatic Selectee" Watchlists

The TSA provides the airlines with the "No Fly" and "Automatic Selectee" watchlists for use in identifying passengers who are to be denied boarding or who require additional scrutiny prior to boarding. The "No Fly" watchlist is a list of persons who are considered a direct threat to U.S. civil aviation. Aircraft bombings in the late 1980s prompted the U.S. government to adopt this list in 1990. It was initially administered jointly by the FBI and Federal Aviation Administration (FAA), but the FAA assumed sole administrative responsibility for this list in November 2001. At that time, the FAA instituted the "Automatic Selectee" list as well. As the names of these lists imply, prospective passengers found to be on the "No Fly" list are denied boarding and referred to law enforcement, whereas those on the "Automatic Selectee" list are selected for secondary security screening before being cleared to board.

Under the Aviation Transportation Security Act,[599] TSA was established and assumed the administrative responsibility for these lists. As the FAA did before it, the TSA distributes these watchlists to U.S. air carriers. In turn, the air carriers screen passengers against these watchlists before boarding. In general, these lists are downloaded into a handful of computer reservations systems used by most

---

[595] Ibid, p. 4.

[596] Ibid, p. 5.

[597] CBP briefing provided to CRS on November 14, 2008.

[598] Ibid.

[599] Public 107-71, Nov. 19, 2001, 115 Stat. 597.

U.S. air carriers; however, a few smaller carriers still manually compare passenger data against these lists. As intelligence and law enforcement officials were concerned about the security of the "No Fly" list, only a handful of names were listed prior to the 9/11 attacks (fewer than 20).[600] Since then, the lists have been expanded almost daily.[601] Within TSA, the Office of Intelligence is responsible for resolving potential watchlist matches.

According to the FBI, the "No Fly" and "Automatic Selectee" lists were consolidated into the TSC's TSDB sometime in the latter half of FY2004.[602] While much larger, these watchlists still appear to be a relatively small subset of the TSDB. It has been reported that by the end of FY2004, there were more than 20,000 names on the "No Fly" list and TSA was being contacted by air carriers as often as 30 times per day with potential name matches.[603] During 2004, the "No Fly" and "Automatic Selectee" lists were the subject of increased media scrutiny for misidentifications. In some cases, these misidentifications included Members of Congress (e.g., Senator Edward Kennedy and Representatives John Lewis and Don Young).[604]

It is notable that because not all known and suspected terrorists are considered "threats to civil aviation," there could be legal and investigative policy considerations that would bear upon placing all such persons, who are included in the TSDB, on the "No Fly" list and possibly the "Automatic Selectee" list. The TSC, moreover, may be reluctant to release the full list of known and suspected terrorists to the airlines because of data security concerns. Although data security remains a concern, a much larger terrorist watchlist is provided by the TSC to CBP. This watchlist, however, remains under government control.

The Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458) included two reporting requirements related to air passenger prescreening and

---

[600] National Commission on Terrorist Attacks Upon the United States, The Aviation Security System and the 9/11 Attacks, Staff Statement no. 3, January 27, 2004, p. 6.

[601] Electronic Privacy Information Center, "'Documents Show Errors in TSA's 'No Fly' Watchlist," April 2003, at http://www.epic.org/privacy/airtravel/foia/watchlist_foia_analysis.html.

[602] U.S. Department of Justice, Federal Bureau of Investigation, Criminal Justice Information Services (CJIS) Division, "Terrorist Screening Center Consolidates Data for Law Enforcement Needs," The CJIS LINK, vol. 7, no. 4, October 2004, pp. 1-2.

[603] Sara Kehaulani Goo, "Faulty 'No Fly' System Detailed," Washington Post, October 9, 2004, p. A01.

[604] Sara Kehaulani Goo, "Committee Chairman Runs Into Watch-List Problem: Name Similarity Led to Questioning at Anchorage and Seattle Airports, Alaska Congressman Says," Washington Post, Sept. 30, 2004, p. A17; and "Hundreds Report Watch-List Trials: Some Ended Hassles at Airports by Making Slight Change to Name," Washington Post, August 21, 2004, p. A08.

terrorist watchlists. Section 4012(b) required the DHS Privacy Officer to report to Congress,[605] within 180 days of enactment (June 15, 2005), on the impact of the "No Fly" and "Automatic Selectee" lists on privacy and civil liberties. Section 4012(c) required the National Intelligence Director, in consultation with the Secretary of Homeland Security, the Secretary of State, and the Attorney General, to report to Congress, within a 180 days of enactment, on the criteria for placing individuals in the consolidated TSDB watchlists maintained by the TSC, including minimum standards for reliability and accuracy of identifying information, the threat levels posed by listed persons, and the appropriate responses to be taken if those persons were encountered.

In April 2006, the DHS Privacy Office issued its report assessing the impact of the "No Fly" and "Automatic Selectee" lists on privacy and civil liberties.[606] The report cited concerns about the quality of the information of those lists, as well as the underlying intelligence.[607] The report also noted allegations about profiling on the basis of race, religion, or national origin, but reported that it could not substantiate those allegations.[608] Furthermore, the report assessed existing DHS redress mechanisms, which are described briefly below.

In regard to the criteria used to place individuals on terrorist watchlists consolidated in the TSDB, it is unknown whether the National Intelligence Director reported to Congress on this matter. Nevertheless, the Privacy Office report stressed that those criteria could not be made public without (1) compromising intelligence and security or (2) allowing persons wishing to avoid detection to subvert those lists.[609] In October 2007, the GAO reported that the FBI and Intelligence Community were using reasonable standards for watchlisting persons who are suspected of having possible links to terrorism.[610]

---

[605] Section 4012(b) of P.L. 108-458 required that the report be submitted to the Committee on the Judiciary, the Committee on Governmental Affairs and Homeland Security, and the Committee on Commerce, Science, and Transportation in the Senate; and to the Committee on the Judiciary, the Committee on Government Reform, the Committee on Transportation and Infrastructure, and the Committee on Homeland Security in the House of Representatives.

[606] U.S. Department of Homeland Security, DHS Privacy Office Report on Assessing the Impact of the Automatic Selectee and No Fly Lists on Privacy and Civil Liberties, April 27, 2006, 22 pp.

[607] Ibid., p. 8.

[608] Ibid., p. 9.

[609] Ibid.

[610] U.S. Government Accountability Office, Terrorist Watch List Screening, Opportunities Exist to Enhance Management Oversight, Reduce Vulnerabilities in Agency Screening Processes, and Expand the Use of the List, GAO08-110, October 2007, p. 19.

On January 17, 2007, the head of TSA, Assistant Secretary Edmund "Kip" Hawley, testified before the Senate Committee on Commerce, Science and Transportation about aviation security and related recommendations made by the National Commission on Terrorist Attacks upon the United States (9/11 Commission).[611] With regard to terrorist watchlist screening of air passengers, Assistant Secretary Hawley informed the committee that TSA and the Terrorist Screening Center were reviewing the "No Fly" list in an effort to reduce the number of individuals on that list by as much as 50%.[612] According to a press account, the "No Fly" list includes 4,000 names of individual persons and the "Selectee" lists includes about 14,000 names.[613]

Computer-Assisted Passenger Prescreening System (CAPPS)

The 1996 Federal Aviation Reauthorization Act authorized the development of the Computer-Assisted Aviation Prescreening System (CAPS) system.[614] At the time this bill was enacted, however, the Federal Aviation Administration (FAA) had already begun to develop the system that became CAPS.[615] The FAA, together with Northwest Airlines, developed the CAPS interface with the airline's computer reservation system in 1996 and 1997. Additional field testing continued through 1997 and 1998. The FAA issued a proposed rule directing all major U.S. air carriers to maintain CAPS on their computer reservation systems in April 1999.[616] However, this rule was never made final, reflecting in part the controversy generated by this system.

CAPS and Checked Baggage Screening

---

[611] U.S. Department of Homeland Security, Testimony of Assistant Secretary Edmund S. Hawley before the Senate Committee on Commerce, Science and Transportation, "Aviation Security and 9/11 Commission Recommendations," January 17, 2007.

[612] Ibid.

[613] Carrie Johnson, "Explosive Could Have Blown Hole in Plane: President Orders Review of Watch Lists as Criticism Intensifies," Washington Post, December 29, 2009, p. A4.

[614] P.L. 104-264; 110 Stat. 3253. Section 307 of the act reads: "The Administrator of the Federal Aviation Administration, the Secretary of Transportation, the intelligence community, and the law enforcement community should continue to assist air carriers in developing computer-assisted passenger profiling programs and other appropriate passenger profiling programs which should be used in conjunction with other security measures and technologies."

[615] Also, during this time, the White House Commission on Aviation Safety and Security (Gore Commission) recommended that an automated profiling system for commercial aviation be developed. See White House Commission on Aviation Safety and Security: Final Report to President Clinton, February 12, 1997.

[616] 64 Federal Register, pp. 19219-19240, April 19, 1999.

The operational concept behind the CAPS system is to select "high-risk" travelers based on certain characteristics found in passenger name record (PNR) data elements—like ticket purchasing patterns and the details of their travel itineraries for greater scrutiny in terms of baggage screening, while expediting baggage screening for "low-risk"passengers. In other words, the CAPS system was designed to determine which passengers were unlikely to have an explosive device in their checked baggage, so that limited explosive detection capabilities could be focused on a smaller number of passengers and bags.[617] The CAPS system was reviewed by the Department of Justice's Civil Rights and Criminal Divisions, along with the FBI, and was found not to be based on characteristics related to ethnicity, gender, or religious faith.[618] The CAPS system was later renamed CAPPS (Computer-Assisted Passenger Presceening System). Like the "No Fly" and "Automatic Selectee" watchlists, the CAPPS system is largely invisible to the public as the system itself resides on airline reservations systems (for example, Sabre and Amadeus).[619] The federal government, moreover, does not control or collect data utilized by CAPPS.

CAPPS and Passenger Screening at Airport Security Checkpoints

It is significant to note that, on September 11, 2001, nine of the 19 hijackers were selected by CAPPS for additional baggage screening; however, CAPPS was not used to select passengers for greater screening at passenger checkpoints.[620] Since the 9/11 attacks, CAPPS has been expanded, and TSA uses the system to identify persons based on certain characteristics gleaned from the PNR data who are selected for not only additional passenger-checked baggage screening, but additional passenger checkpoint screening as well.

9/11 Commission Recommendations and CAPPS II

The 9/11 Commission formally recommended that the "no fly" and "automatic selectee" lists should be improved, and that air passengers should be screened not only against these lists, but the "larger set of watchlists maintained by the federal government."[621] Moreover, the TSA should perform this function, as

---

[617] Statement of Jane Garvey to the National Commission on Terrorist Attacks Upon the United States, May 22, 2003, p. 11.

[618] Anthony Fainberg, "Aviation Security in the United States: Current and Future Trends," Transportation Law Journal, vol 25, spring 1998, p. 200.

[619] Ibid., p. 200.

[620] Statement of Cathal L. Flynn to the National Commission on Terrorist Attacks Upon the United States, January 27, 2004, p. 4.

[621] National Commission on Terrorist Attacks Upon the United States, The 9/11 Commission Report, Authorized ed. (New York: W.W Norton & Co., 2004), p. 393.

opposed to the air carriers, and the air carriers should be required to supply the information needed to test a new air passenger prescreening system.[622]

When the 9/11 Commission report was released in July 2004, the TSA had already been working for almost two years on a new passenger prescreening system called CAPPS II. This system was intended to replace the airline-operated systems for checking passenger names against the government-issued "no-fly" watchlist (those individuals to be denied boarding) and the "automatic selectee" watchlist (those individuals designated for additional or secondary screening at airport security checkpoints). In addition, in lieu of a biometric, CAPPS II was designed to include sophisticated algorithms that would query both government and commercial databases to authenticate the identity of passengers and crew, as well as assess their risk.

Critics argued, however, that the TSA's ever-expanding vision for prescreening constituted an unprecedented government-sponsored invasion of privacy. This and other controversies ultimately led TSA to scrap CAPPS II in August 2004, soon after the release of the 9/11 Commission final report, and pursue enhanced prescreening capabilities under a new system called Secure Flight. As described below, TSA planned to begin implementing Secure Flight in December 2008, but actual implementation did not begin until March 2009. Although, the original scope of the Secure Flight has also been scaled back so that it no longer includes an identity authentication component or a rule for more intensive searching, TSA has not announced any plans to discontinue the use of CAPPS.

TSA Secure Flight Program

Reflecting the recommendations of the 9/11 Commission, Congress included several provisions related to preflight screening of airline passengers against terrorist watchlists in the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458). In particular, section 4012 of that act requires the TSA to assume from U.S. air carriers the passenger watchlist screening function after it establishes an advanced (pre-departure) air passenger prescreening system that utilizes the greater set of watchlists integrated and consolidated in the FBI-administered Terrorist Screening Database (TSDB). It also required the DHS to screen passengers on international flights against the TSDB prior to departure, a requirement currently met by CBP through its APIS pre-departure process (described above). Following the demise of CAPPS II (described above), TSA has sought to address the mandate for domestic passenger prescreening though the development of the Secure Flight system and plans to eventually incorporate international passenger prescreening under this system as well, following its successful implementation domestically.

---

[622] Ibid.

Initial Program Design, Development, and Related Legislation

As initially conceived by TSA, the Secure Flight program was designed to improve passenger prescreening and deter, detect, and prevent known or suspected terrorists from boarding commercial flights. The TSA endeavored to meet this objective by using Secure Flight as a means to focus its limited screening resources on individuals and their baggage who are perceived to pose an elevated or unknown risk to commercial aviation, while reducing the number of passengers screened and wait times at passenger screening checkpoints. According to TSA, Secure Flight consisted of four elements:

- a streamlined rule for more intensive screening,
- a scaled-back identity authentication process,
- a passenger name check against the Terrorist Screening Database, and
- an appeals process for passengers who may have been misidentified.

In addition to the appeals process, the Secure Flight program is an amalgam of features taken from existing screening systems, CAPPS II, and the 9/11 Commission's recommendations that passengers be screened against the wider set of terrorist watchlists maintained by the U.S. government. Within TSA, the Office of National Risk Assessment had responsibility for establishing policy for the Secure Flight program.

To reduce redundant or overlapping passenger processing systems, TSA initially planned to design Secure Flight so that the system would be used only for prescreening passengers on domestic flights. As described above, DHS's CBP would continue to be responsible for checking passenger identities against watchlists and prescreening passengers on inbound and outbound international flights. It was unclear, however, whether responsibility for screening domestic and international flights could clearly be divided between TSA and CBP, because many international flights have domestic legs and international passengers sometimes make connections to domestic flights.

It was also unclear, moreover, whether the development of Secure Flight for domestic flight would impair TSA's responsibility for screening international air passengers who may be threats to civil aviation. At issue is TSA's authority and responsibility over all aspects of aviation security versus CBP's authority and responsibility for border management and security. It remained an open policy question whether the CBP pre-departure screening of air passengers on all in-bound international flights through APIS would be sufficient. In the case of international air travel, the distinction between aviation and border security functions has become increasingly blurred.

Problems Developing Secure Flight

Like its predecessor, CAPPS II, the Secure Flight program initially proved controversial. In March 2005, the DHS OIG reported that TSA had mishandled

some passenger data while testing CAPPS II, but since that time, the agency's approach to privacy issues had improved markedly.[623] In the same month, the GAO reported that TSA had begun developing and testing Secure Flight; however, TSA had not determined fully "data needs and system functions," despite ambitious timelines for program implementation.[624] Consequently, the GAO reported that it was uncertain whether TSA would meet its August 2005 Secure Flight operational deployment date.[625] The TSA, in fact, did not meet the deadline and in February 2006 announced that it was restructuring ("rebaselining") the Secure Flight program.

In addition, in July 2005, GAO reported that TSA had not fully disclosed its use of passenger data during the testing for Secure Flight.[626] In August 2005, the DOJ OIG reported that there were numerous problems coordinating the development of the Secure Flight program with the efforts of the FBI-administered TSC.[627] In September 2005, the identity authentication element of the Secure Flight program, under which TSA planned to compare PNR data (for domestic flights) with databases maintained by commercial data aggregators to verify passenger identities, was reportedly dropped.[628] In December 2006, moreover, the DHS's Privacy Office issued a report, finding that the TSA had not accurately described its use of personal data as part of the Secure Flight program in notifications required under the Privacy Act.[629]

Furthermore, in the FY2005 DHS Appropriations Act (P.L. 108-334), Congress prohibited TSA (or any other component of DHS) from spending any

---

[623] U.S. Department of Homeland Security, Office of Inspector General, Review of the Transportation Security Administration's Role in the Use and Dissemination of Airline Passenger Data (Redacted), OIG-05-12, March 2005, p. 8.

[624] U.S. Government Accountability Office, Aviation Security: Secure Flight Development and Testing Under Way, but Risks Should Be Managed as System Is Further Developed, GAO-05-356, March 28, 2005, p. 17.

[625] Ibid.

[626] U.S. Government Accountability Office, Aviation Security: Transportation Security Administration Did Not Fully Disclose Uses of Personal Information during Secure Flight Program Testing in Initial Privacy Notices, but Has Recently Taken Steps to More Fully Inform the Public, GAO-05-864R, July 22, 2005, p. 9.

[627] U.S. Department of Justice, Office of the Inspector General, Review of the Terrorist Screening Center's Efforts to Support the Secure Flight Program, Audit Report 05-34, August 2005, 41 pp.

[628] John Bacon, "TSA: 'Data Mining' Deleted from Plan," USA Today, September 23, 2005, p. 3A.

[629] U.S. Department of Homeland Security, Privacy Office, Secure Flight Report: DHS Privacy Office Report to the Public on the Transportation Security Administration's Secure Flight Program and Privacy Recommendations, December 2006, 15 pp.

appropriated funds on the deployment of Secure Flight, or any successor system used to screen aviation passengers, until the GAO reports that certain conditions have been met, including the establishment of an appeals process.[630] Similar provisions have been included in subsequent departmental appropriations, including the FY2009 DHS Appropriations Act (P.L. 111-5).[631] As noted above, TSA began implementing Secure Flight domestically in March 2009. In the FY2010 DHS Appropriations Act (P.L. 111-83), Congress did not include a similar spending prohibition; however, report language requires TSA to report within 90 days on its progress in addressing GAO's Secure Flight-related recommendations.

Secure Flight Final Rule

On October 28, 2008, TSA published a final rule detailing the operational implementation of Secure Flight, effective December 29, 2008.[632] TSA is implementing Secure Flight in two phases. The first phase encompasses only *domestic* flights, while the second phase will include *international* departures and arrivals as well as commercial international flights overflying any of the 48 contiguous states. TSA began operational testing in May 2009 to test the reliability of data transmission connections to receive passenger data from the airlines and transmit screening results back to the airlines, and to assess the performance of the watch list screening process under operational conditions. Operational testing and phased-in implementation of Secure Flight for vetting domestic passengers is currently underway. Effective August 15, 2009, airlines were required to begin collecting full name, date of birth, gender, and redress number (if available) for domestic passengers. The airlines were required to begin collecting such information for international passengers effective October 31, 2009. The TSA has stated that its goal is to fully implement Secure Flight for domestic flights by early 2010, and for all international flights by the end of 2010.[633]

During the time operational testing of Secure Flight is ongoing, airlines will be required to continue the process of checking passengers against the "no fly" and "automatic selectee" lists provided by TSA. As a result, TSA will continue to distribute these lists to airlines until all airlines have completed operational testing of the domestic portion of Secure Flight and TSA assumes full responsibility for comparing passenger data against the terrorist watch list.

---

[630] Sec. 522, 118 Stat. 1319.

[631] Sec. 513, 121 Stat. 2072.

[632] U.S. Department of Homeland Security, Transportation Security Administration, "Secure Flight Program; Final Rule," 72 Federal Register, pp. 64018-64066, October 28, 2008.

[633] Transportation Security Administration, "TSA's Secure Flight Enters First Public Phase," May 12, 2009.

For international flights, CBP will continue to check passenger names against terrorist watch lists under the APIS pre-departure protocols until Secure Flight in fully implemented for international flights. However, airlines will transmit data using a single transmission DHS portal, although the two systems have slightly different data requirements and different timetables for the delivery of data, as explained in the Secure Flight final rule.

Overflights[634] represent a new category of covered operations that will require transmission of passenger data for screening against the terrorist watch list and will encompass operators that may not operate flights to and from the United States. According to the final rule, the phase in of overflights in the Secure Flight system will coincide with the phase in of international flights.

Secure Flight and Terrorist Watchlist Checks

Initially, the TSA will begin implementing the use of Secure Flight to compare passenger data (Secure Flight Passenger Data) provided by the airlines against the TSDB. This will replace the process of providing these "automatic selectee" and "no fly" lists to the airlines. The program will apply to passenger airlines offering scheduled passenger service and public charter flights that operate to and from about 450 commercial passenger airports throughout the United States. These airlines will be required to submit passenger data to the TSA beginning 72 hours prior to the flight and thereafter continue to provide passenger data as soon as it becomes available. The airlines must also submit this required information for any non-employee seeking access to the sterile area beyond the security screening checkpoint, such as an individual assisting a special needs traveler or escorting an unaccompanied minor to or from an aircraft. The airlines will be required to collect from all passengers and individuals seeking access to the airport sterile area their full name, date of birth, and gender data. The airline must also request from travelers any known traveler[635] or passenger redress number provided by the TSA and, if these numbers are provided by the passengers, then the airline must transmit them to the TSA. The airline must also

---

[634] Overflights refer to flights that transit through the airspace above a geographic area but do not originate or land at a destination in that area. As noted previously, Secure Flight requirements will only be applied to those overflights transiting through airspace over the contiguous 48 states and will not include aircraft overflying Alaska or Hawaii.

[635] The TSA Secure Flight final rule explains that this Known Traveler Number would be a unique number assigned to a traveler for whom the federal government has already conducted a threat assessment and was found to not pose a security threat. Since the TSA eliminated the requirement for security threat assessments for passengers participating in the voluntary Registered Traveler (RT) program effective July 30, 2008, it does not appear that the Known Traveler Number field will be propagated with RT number data at this point, and it is not believed that RT participation will, at present, have any impact on the name based threat assessment process to be conducted under the Secure Flight program.

transmit passport numbers, itinerary information, record locator data, and various other reference numbers if these data are available. For a complete list of Secure Flight Passenger Data (SFPD), see Appendix D.

Once received, the TSA will use an automated process to compare this passenger data against the consolidated TSDB. The TSA does not maintain its own watch list, but rather the TSA is a customer of the TSC. In consultation with the TSA, the TSC compiles the "no fly" and "automatic selectee" lists from the consolidated TSDB. Under the Secure Flight system, TSA will similarly continue to rely on the TSDB to determine whether to deny a passenger boarding or subject the passenger and his or her property to additional physical screening.

When the Secure Flight process returns an indication of an exact or reasonably similar match, a TSA intelligence analyst will review additional available information in an effort to reduce the number of false positive matches. If the TSA determines that a probable match exists, it will forward these results along with the passenger information to the TSC to provide confirmation of the match. According to the procedures set forth in the Secure Flight final rule, if the TSA or the TSC cannot make a definitive determination, notification would be sent to the airline to require the passenger to present a verifying identity document (VID), such as an unexpired driver's license or a passport, when checking in at the airport. If the TSA determines that the passenger data provided is a match to the Secure Flight selectee list, it will inform the airline which, in turn, will be required to identify the passenger and his or her baggage for enhanced screening. The TSA may also inform an airline that a passenger is to be placed in "inhibited status," meaning that he or she may not be issued a boarding pass or enter the sterile area of an airport.

Passengers who believe that they have been wrongly delayed, denied boarding, or subject to additional screening as a result of the Secure Flight system and the process it applies to screening passenger data against terrorist watch list information may seek redress from the DHS. The procedures for redress apply to all DHS-operated systems for screening individuals against terrorist watch list data and are described in further detail below.

Misidentifications and Related Procedures

Misidentifications have been a recurring issue for Congress. Initially, such problems were frequently associated with TSA's administration of the "No Fly" and "Automatic Selectee" lists. More recently, however, this may be an emerging problem for CBP as well in light of the American Civil Liberties Union (ACLU) class-action suit against that agency.[636]

---

[636] According to the ACLU, U.S. citizens have been subjected to repeated and lengthy stops, questioning, body searches, handcuffing, excessive force, and separation from family while being detained by CBP officers because of possible watchlist matches. Nine of these U.S. citizens have

Under HSPD-6, the TSC Director has been made responsible for developing policies and procedures related to the criteria for including terrorist identities data in the consolidated TSDB and for measures to be taken in regard to misidentifications, erroneous entries, outdated data, and privacy concerns. The Bush Administration maintained further that because the TSC does not collect intelligence, and has no authority to do so, all intelligence or data entered into the TSDB are actually being collected by other agencies in accordance with applicable, pre-existing authorities.

At the same time, however, the TSC is limited in its ability to address certain issues related to misidentifications because it is restricted from divulging classified or law enforcement-sensitive information to the public under certain circumstances (discussed below). The same could be said for many frontline-screening agencies as well (e.g., TSA and CBP), because many terrorist lookout records, while possibly declassified, are based on classified intelligence collected by other agencies. Such records would probably be considered security sensitive information. Hence, questions could arise as to which agencies, if any, are in a position to handle matters pertaining to misidentifications.

Moreover, if procedures are not properly coordinated, inconvenienced travelers who have been misidentified as terrorists or their supporters could face a bureaucratic maze if they attempt to seek redress and remedy. The DOJ OIG audit on TSC operations (described above) included a recommendation that the TSC strengthen procedures for handling misidentifications and articulate those procedures formally in written documents (operational guidelines).[637] Congress later required reports from the Administration and GAO regarding the use of terrorist watchlists.

Disclosure Under FOIA and Privacy Act

In regard to TSC, Members of Congress and other outside observers have questioned whether there should be new policy and procedures at different levels (such as visa issuance, border inspections, commercial aviation security, domestic law enforcement, and security of public events) for the inclusion of persons in the TSDB.[638] Also, Members have asked how a person could find out if they were in the Terrorist Screening Database and, if so, how they got there. In congressional testimony, then-TSC Director Bucella surmised that a person would learn of being in the TSDB when a screening agency encountered them

---

filed a class action suit against DHS. See Rahman v. Chertoff, Case No. 05 C 3761 (E.D. Ill. filed June 19, 2006).

[637] Ibid., p. 76.

[638] For further information, see CRS Report RL31730, Privacy: Total Information Awareness Programs and Related Information Access, Collection, and Protection Laws, by Gina Stevens.

and, perhaps, denied them a visa or entry into the United States, or arrested them. Bucella suggested that the TSC would probably be unable to confirm or deny whether the person was in the TSDB under current law.[639]

Consequently, persons who have been identified or misidentified as terrorists or their supporters would have to pursue such matters through the screening agency. The screening agency, however, might not have been the originating source of the record, in which case a lengthy process of referrals may have to be initiated. Under such conditions, persons identified as terrorists or their supporters may turn to the Freedom of Information Act (FOIA) or the Privacy Act as a last alternative. Under FOIA,[640] any person, including a noncitizen or nonpermanent resident, may file a request with any executive branch agency or department, such as the State Department or DHS, for records indicating he or she is on a watchlist. However, under national security and law enforcement FOIA exemptions, the departments may withhold records on whether an individual is on a watchlist.[641] Consequently, a FOIA inquiry is unlikely to shed any light on these areas.

In addition, a citizen or legal permanent resident may file a Privacy Act[642] request with DHS and/or DOJ to discern whether a screening agency or the FBI has records on them. However, the law enforcement exemption under the Privacy Act may permit the departments to withhold such records. Under the Privacy Act, a citizen or legal permanent resident may request an amendment of their record if information in the record is inaccurate, untimely, irrelevant, or incomplete. Under both FOIA and the Privacy Act, there are provisions for administrative and judicial appeal. If a request is denied, the citizen or legal permanent resident is required to exhaust his or her administrative remedies prior to bringing an action in U.S. District Court to challenge the agency's action.[643]

Other Possible Legal Questions

---

[639] Donna Bucella, Terrorist Screening Center Director, Testimony Before the National Commission on Terrorist Attacks upon the United States, January 26, 2004, p. 1.

[640] 5 U.S.C. §522.

[641] 5 U.S.C. §§522(b), (c), 522a(j).

[642] 5 U.S.C. §522a.

[643] One recent legal analysis examined several U.S. court decisions addressing the use of terrorist watchlists for aviation security purposes. According to that analysis, it appears that the presiding judges in those cases were willing to defer to TSA regarding determinations that watchlist records were security sensitive information, even though those records were essential to the maintenance of the plaintiffs' claims. See Linda L. Lane, "The Discoverability of Sensitive Security Information in Aviation Litigation," Journal of Air Law and Commerce, vol. 71, Summer 2006, p. 434.

The Bush Administration pledged that terrorist screening information would be gathered and employed within constitutional and other legal parameters. CRS is unaware of any official statement by the Obama Administration regarding these matters. Nevertheless, although the Privacy Act generally does not restrict information sharing related to known and suspected terrorists who are not U.S. persons for the purposes of visa issuance and border inspections, it does restrict the sharing of information on U.S. persons (citizens and legal permanent residents) for purely intelligence purposes, who are not the subject of ongoing foreign intelligence or criminal investigations.[644] Consequently, legal questions concerning the inclusion of U.S. persons on various watchlists under criminal or national security predicates may arise. In addition, questions of compensation for persons damaged by mistaken inclusion in these databases will likely be an issue.

DHS Redress Mechanisms

Both the DHS Privacy Office and GAO reported to Congress on existing DHS redress mechanisms, by which an individual who felt he or she had been unfairly denied boarding on a commercial aircraft or singled out for screening could contact several DHS offices and initiate a redress inquiry.

Early Mechanisms

According to the DHS Privacy Office, individuals who believed they had been misidentified as a terrorist while being screened by TSA could have contacted either the TSA Ombudsman's Contact Center or Office of Civil Rights.[645] Information was also available on the TSA website regarding the redress process.[646] Individuals seeking redress were issued a Privacy Act Notice and Passenger Identity Verification Form, which was processed by the TSA Office for Transportation Security Redress (OSTR).[647] If OSTR concluded an individual had been misidentified, it would place him or her on a "cleared" list.[648] However, GAO reported that individuals who had been placed on the cleared lists could have continued to encounter inconveniences. For example, "they may be forced to obtain a boarding pass at the ticket counter as opposed to the using the Internet, curbside, or airport kiosk check-in options."[649]

---

[644] Department of State, Testimony to the Joint Congressional Intelligence Committee, p. 5.

[645] U.S. Department of Homeland Security, DHS Privacy Office Report on Assessing the Impact of the Automatic Selectee and No Fly Lists on Privacy and Civil Liberties, April 27, 2006, p. 17.

[646] Ibid.

[647] Ibid.

[648] Ibid.

[649] U.S. Government Accountability Office, Terrorist Watch List Screening, GAO-06-1031, Sept. 2006, p. 34.

Meanwhile, individuals who believe they have been misidentified while being screened by CBP could contact that agency's Customer Service Satisfaction Unit.[650] In addition to contacting either TSA or CBP, individuals who had possibly been misidentified could have also contacted either the DHS Privacy Office or Office of Civil Rights and Civil Liberties.[651] As described above, frontline-screening agencies referred matters concerning individuals who believe they have been mistakenly watchlisted to the TSC, as is the case today.

At a Senate hearing, the former head of TSA, Assistant Secretary Hawley, conceded that the redress processes at TSA had been "too cumbersome and expensive," prompting the agency to introduce a new streamlined process and automated redress management system.[652] Hawley also testified that then-DHS Secretary Chertoff had developed a program envisioned by then-Secretary of State Condoleezza Rice that is designed to provide travelers with a single, simple process for addressing watchlist-related complaints.[653] Hawley also testified that the advance air passenger prescreening program known as Secure Flight would reduce misidentifications—the largest source of complaints.[654] He reported that TSA had processed more than 20,000 redress requests in 2006, and the average processing times of those requests had been reduced from two months to 10 days.[655]

Traveler Redress and Inquiry Program (TRIP)

The Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458) required the TSA and DHS to establish appeals procedures by which persons who are identified as security threats based on records in the TSDB may appeal such determinations and have such records, if warranted, modified to alleviate such occurrences in the future. Also, provisions in the Implementing Recommendations of the 9/11 Commission Act of 2007 (P.L. 110-53) required the DHS to establish an Office of Appeals and Redress to establish a timely and fair process for individuals who believe they have been delayed or prohibited from

---

[650] U.S. Department of Homeland Security, DHS Privacy Office Report on Assessing the Impact of the Automatic Selectee and No Fly Lists on Privacy and Civil Liberties, April 27, 2006, p. 17.

[651] Ibid.

[652] U.S. Department of Homeland Security, Testimony of Assistant Secretary Edmund S. Hawley before the Senate Committee on Commerce, Science and Transportation, "Aviation Security and 9/11 Commission Recommendations," January 17, 2007.

[653] Ibid.

[654] Ibid.

[655] Ibid.

boarding a commercial aircraft because they were wrongly identified as a threat. The provisions further establish a requirement to maintain records of those passengers and individuals who have been misidentified and have corrected erroneous information.

To handle and resolve the complaints of passengers and meet these statutory requirements, the DHS has established the DHS Traveler Redress Inquiry Program (DHS TRIP) as a mechanism for addressing watchlist misidentification issues and other situations where passengers feel that they have been unfairly or incorrectly delayed or denied boarding or identified for additional security screening at airport screening checkpoints, ports of entry or border checkpoints, or when seeking to access other modes of transportation.

The DHS TRIP program allows passengers seeking redress, or their lawyers or other representatives, to file complaints either by using an online system or by completing and mailing a complaint form.[656] After completing the online questionnaire or mailing the complaint form, the DHS will request supporting information within 30 days. Filers are given a control number that allows them to track the status of their inquiry using the Internet. The DHS will make a final determination and respond to the filer. If the investigation finds that the traveler has been delayed due to a misidentification or similar name-matching issue, the response will describe the steps required to resolve this issue. Often, the traveler may be required to retain a copy of the DHS response letter and present it during the check-in process when traveling on airline flights. The DHS cautions, however, that the steps taken may not resolve all future travel-related concerns. For example, the traveler may be selected for additional screening based on a variety of factors or at random. If a passenger disagrees with the resolution decision made by the DHS, he or she may take further steps to appeal the decision.

Fair, Accurate, Secure, and Timely (FAST) Redress Act of 2009 (H.R. 559)

In the 111th Congress, the House passed the FAST Redress Act (H.R. 559) under suspension of the rules on February 3, 2009, a bill introduced by Representative Yvette D. Clarke. This bill is similar to a proposal (H.R. 4179) passed in the 110th Congress, also introduced by Representative Clarke. The House Committee on the Judiciary reported H.R. 4179 (H.Rept. 110-686) on June 5, 2008. The House passed H.R. 4179 on June 18, 2008. Senator Amy Klobuchar introduced an identical proposal (S. 3392). The FAST Redress Act would amend the Homeland Security Act of 2002 (P.L. 107-296) to direct the Secretary of Homeland Security to establish a timely and fair process for individuals who believe they were delayed or prohibited from boarding a commercial aircraft because they were

[656] Complete instructions for filing complaints under the DHS TRIP program can be found at: http://www.dhs.gov/files/programs/gc_1169676919316.shtm.

wrongly identified as a threat when screened against any terrorist watchlist or database used by TSA or any component of DHS. It would also authorize an Office of Appeals and Redress within DHS to implement, coordinate, and execute this process.

Possible Issues for Congress

Three issues loom large in terms of the U.S. government's capabilities to identify, screen, and track terrorists and their supporters. For example, how reliable is the intelligence that is the basis for lookout records? When will the TSA and CBP be able to prescreen effectively air passengers prior to departure? Will the TSC in cooperation with screening agencies be able to establish viable redress and remedy processes for persons misidentified as terrorists or their supporters given certain limitations placed on those agencies in regard to the public divulgence of national security and law enforcement sensitive information?

Reliability of Intelligence Underlying Lookout Records

Because the Terrorist Identities Datamart Environment (TIDE) maintained by the National Counterterrorism Center (NCTC) is the principal source of lookout records on international terrorists placed in the TSC's consolidated terrorist screening database, a key oversight issue for Congress is ensuring that intelligence community agencies are sharing the appropriate information necessary to identify terrorists and their supporters with the NCTC. Is the TSC receiving timely terrorist identities data updates that reflect the best and most reliable intelligence available to intelligence and law enforcement agencies?

Preflight Passenger Screening by TSA and CBP

While largely related to implementation, a number of unresolved questions remain with regard to prescreening air passengers prior to departure (wheels up). How quickly can TSA develop and deploy an advanced air passenger prescreening system that, among other things, will assume the day-to-day administration of the "No Fly" and "Automatic Selectee" watchlists from the airlines?

Viable Processes of Redress and Remedy for Misidentifications

Concerning misidentifications, under HSPD-6, the TSC Director is responsible for developing policies and procedures related to the criteria for inclusion into the consolidated TSDB, and for taking measures to address misidentifications, erroneous entries, outdated data, and privacy concerns. An issue for Congress may be the extent to which the TSC is working with screening agencies to develop appropriate and effective redress and remedy processes for persons misidentified as terrorists or their supporters. Given certain limitations placed on the TSC and screening agencies with regard to releasing national security and law enforcement sensitive information, will sufficient information channels be available and remedial processes established to provide for accurate and expeditious determinations in misidentification cases?

Appendix A. APIS Data Elements

APIS data elements include the following:

- Full Name.
- Date of Birth.
- Gender.
- Passport Number.
- Passport Country of Issuance.
- Passport Expiration Date.
- Passenger Name Record Locator.
- Foreign Airport Code—place of origination.
- Port of First Arrival.
- Final Foreign Port for In-transit Passengers.
- Airline Carrier Code.
- Flight Number.
- Date of Aircraft Departure.
- Time of Aircraft Departure.
- Date of Aircraft Arrival.
- Scheduled time of Aircraft Arrival.
- Citizenship.
- Country of Residence.
- Status on Board Aircraft.
- Travel Document Type.
- Alien Registration Number.
- Address in the United States (except for outbound flights, U.S. citizens, lawful permanent residents, and crew and in-transit passengers).[657]

Appendix B. PNR Data Elements

PNR data elements include the following:

- PNR record locator code.
- Date of reservation/issue of ticket.
- Date(s) on intended travel.
- Name(s).
- Available frequent flier and benefit information (i.e., free tickets, upgrades, etc.).
- Other names on PNR, including number of travelers on PNR.
- All available contact information (including originator of reservation).
- All available payment/bill information.
- Travel itinerary for specific PNR.
- Travel agency/travel agent.
- Code share information.

---

[657] 73 Federal Register, pp. 64023-64024, October 28, 2008.

- Split/divided information.
- Travel status of passenger (including confirmations and check-in status) and relevant travel history.
- Ticketing information, including ticket number, one way tickets, and Automated Fare Quote (ATFQ) fields.
- Baggage information.
- Seat information.
- Open text fields.
- Any collected APIS information.
- All historical changes to the PNR listed above.[658]

Appendix C. EU-U.S. Data Sharing

In Summer 2006, the issue of PNR data sharing emerged as a problem for the United States. Although the European Court of Justice had ruled an EU-U.S. PNR data sharing agreement to be illegal and ordered a cessation of such data sharing on September 30, 2006, then-DHS Secretary Chertoff proposed that the United States should acquire greater amounts of PNR data to improve passenger prescreening for known and suspected terrorists following the foiled plot to bomb airliners flying from the UK to the United States in August 2006.[659] An interim EU-U.S. agreement was reached on October 19, 2006, and a permanent agreement in late July 2007.

European Court of Justice Ruling

In May 2006, the European Court of Justice ruled in favor of an "action of annulment" requested by the European Parliament with regard to the legality of an agreement made by the European Commission and CBP to exchange PNR data to improve passenger prescreening for terrorists, attempting to board transatlantic flights.[660] The court ordered the cessation of PNR data sharing on September 30, 2006.[661] If it had not been resolved, this impasse between the U.S. and EU authorities with regard to PNR data sharing might have significantly affected travel from EU countries to the United States. While the European Commission and CBP renegotiated an interim agreement in terms that were not objectionable to the European Court of Justice, that agreement was temporary.

---

[658] U.S. Department of Homeland Security, "Letter from the United States to the Council of the European Union," July 26, 2007, p. 2.

[659] Michael Chertoff, "A Tool We Need to Stop the Next Airliner Plot," Washington Post, August 29, 2006, p. A15.

[660] "EU Court Rules Illegal EU-U.S. Air Passenger Data Deal," Associate Press Worldstream, May 30, 2006.

[661] "EU, US Officials: New Agreement Will Be Reached on Passenger Data," Agence France Presse, May 30, 2006.

Some European authorities, including Members of the European Parliament, continued to express concern about adequate data protections under the agreement.

CBP Proposed Rule Requires Additional PNR Data Preflight

In July 2006, CBP published a notice of proposed rulemaking, in which the agency sought to acquire PNR data (complete manifests) 60 minutes prior to departure, with a mechanism that would allow for individual, real-time transactions up to 15 minutes prior to a flight's departure for last-minute ticket buyers and other manifest changes.[662] In part, U.S. authorities maintain that such advanced information is necessary for prescreening noncitizens traveling to the United States under the visa waiver program, as well as long-term, multiple-entry visa holders, because they are not screened at a U.S. consulate abroad as part of a visa issuance process.[663]

Following the foiled conspiracy to bomb several airliners flying from Britain to the United States in August 2006, observers noted that the suspected conspirators could have boarded the aircraft bound for the United States without having been screened against the international terrorist watchlists maintained by the TSC in the TSDB prior to a flight's departure, because the UK is a participant in the visa waiver program. In response to the plot, DHS reportedly issued a temporary order requiring that passenger name records be provided preflight to CBP for transatlantic flights originating in the UK,[664] as opposed to 15 minutes after a flight's departure as normally required under current CBP regulations (for arrival manifests).[665] Furthermore, CBP reportedly announced that it would seek to obtain greater amounts of air passenger data preflight from all air carriers and retain that data longer.[666] Reportedly, some Europeans strongly opposed such

---

[662] Federal Register, vol. 71, no. 135, July 14, 2006, pp. 40035-40048.

[663] It is noteworthy that in the Enhanced Border Security and Visa Entry Reform Act of 2002 (P.L. 107-173), Congress included a requirement that countries participating in the visa waiver program issue their nationals machine-readable, tamper-resistant, biometric passports by October 26, 2004. In a subsequent law (P.L. 108-299), the machine-readable and tamper-resistant requirements were extended to October 26, 2005, and the biometric requirement was modified so that it only applied to passports issued after that date. In the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458), Congress required that visa waiver countries certify that they are developing a machine-readable, tamper-resistant, biometric passport by October 26, 2006. For further information, see CRS Report RL32221, Visa Waiver Program, by Alison Siskin.

[664] Mark Skertic, "Passenger List Review May Add To Flight Time," Chicago Tribune, August 17, 2006, p. 1.

[665] 19 Code of Federal Regulations (CFR), Parts 4 and 122.

[666] Ellen Nakashima, "U.S. Seeks to Expand Data Sharing: Retention of Airline Passenger Details Raises Privacy Concerns in E.U.," Washington Post, August 23, 2006, p. A5.

data sharing and see U.S. demands for such data, without stronger data privacy safeguards, as an infringement on their national and collective sovereignties.[667]

EU-U.S. Interim Agreement

Despite lingering concerns about data protection and privacy, on October 19, 2006, the EU and U.S. concluded an interim agreement on PNR that allows PNR data in air carrier reservations systems to continue to be transferred to CBP in the same manner as previously. It also reportedly addressed other privacy issues. For example, the agreement anticipated the development of a new screening system, under which air carriers would send (push) PNR data to CBP, rather than the air carriers allowing CBP access (pull) the data from their reservations systems, as is the case today.[668] This issue is often referred to as the "push/pull issue" and involves systems access and data control. There were additional data protection/privacy issues for the European Union and the United States to resolve in regard to TSA's Secure Flight program and CBP's Automated Targeting System. Particularly troubling for some Europeans and privacy advocates were the following proposed elements of the agreement: (1) retention of PNR data for up to 40 years; (2) collection of increased amounts and types of data; and (3) distribution of that data, along with risk assessments and possibly other analyses, to other law enforcement agencies, where control of those data would be beyond the reach of the agencies whose missions necessitated that such data be collected. The interim agreement would have expired on July 31, 2007.

EU-U.S. Permanent Agreement

On July 26, 2007, then-DHS Secretary Michael Chertoff announced a new agreement between the European Union and the United States on PNR data sharing.[669] Chertoff underscored that PNR data were an essential screening transatlantic travelers against watchlists. Under the permanent agreement, DHS would collect 19 types of PNR data, which would be maintained for seven years in an active file and eight years in a dormant file. On August 23, 2007, DHS issued a final rule that requires all international air carriers and vessel operators to provide CBP with advanced passenger information, including PNR data, in advance of an aircraft's departure or vessel's departure/arrival, depending on the

---

[667] Ibid.

[668] "Council Adopts Decision on Signature of Agreement with U.S. on Continued Use of PNR Data," US Fed News, October 16, 2006.

[669] Department of Homeland Security, Statement of Homeland Secretary Michael Chertoff On A New Agreement With The European Union For Passenger Name Record Data Sharing, Press Release, July 26, 2007.

vessel's port of origin (U.S. or foreign).[670] This rule became effective on February 18, 2008.

Appendix D. Secure Flight Data Elements

Secure Flight Passenger Data (SFPD) elements include the following:

- Full Name.
- Date of Birth.
- Gender.
- Redress Number or Known Traveler Number (if available).
- Passport Number (if available).
- Passport Country of Issuance (if available).
- Passport Expiration Data (if available).
- Foreign Airport Code—place of origination.
- Port of First Arrival.
- Flight Number.
- Date of Aircraft Departure.
- Time of Aircraft Departure.
- Date of Aircraft Arrival.
- Scheduled time of Aircraft Arrival.[671]

[670] U.S. Department of Homeland Security, Bureau of Customs and Border Protection, "Advance Electronic Transmission of Passenger and Crew Member Manifests for Commercial Aircraft and Vessels," Final rule, 72 Federal Register, pp. 48320-48353, August 23, 2007.

[671] 73 Federal Register, pp. 64023-64024, October 28, 2008.

General Management Laws: A Compendium

CONGRESSIONAL RESEARCH SERV., GENERAL MANAGEMENT LAWS: A COMPENDIUM, RL30795 (MAY 19, 2004), *available at* http://www.intelligencelaw.com/library/secondary/crs/pdf/RL30795_5-19-2004.pdf.

Order Code RL30795

Updated May 19, 2004

Clinton T. Brass
Coordinator Analyst in American National Government
Government and Finance Division

Summary

This report (hereafter "compendium") is a companion to CRS Report RL32388, General Management Laws: Major Themes and Management Policy Options. In combination, these reports have three main objectives: (1) to identify and describe the major management laws under which the executive branch of the federal government is required to operate, including their rationale, design, and scope; (2) to assist Members of Congress and their staff in oversight of executive branch management; and (3) to help Congress when considering potential changes to the management laws themselves, as well as other legislation, including authorization statutes and appropriations.

The compendium contains profiles of selected "general management laws" — broad statutes designed to regulate the activities, procedures, and administration of all or most executive branch agencies. The quality of the general management laws, as well as their implementation, are considered crucial to maintaining the accountability of the executive branch to Congress, the President, and the public. Moreover, these laws influence the effectiveness of federal agencies when they implement, evaluate, and help formulate public policies.

The compendium includes more than 90 separate entries that describe general management laws for the executive branch of the federal government. The entries in the compendium are organized into the following seven functional categories: (1) Information and Regulatory Management; (2) Strategic Planning, Performance Measurement, and Program Evaluation; (3) Financial Management, Budget, and Accounting; (4) Organization; (5) Procurement and Real Property Management; (6) Intergovernmental Relations Management; and (7) Human Resources Management and Ethics. These categories include many laws and

topics, including the Freedom of Information Act (FOIA, section I.E.), Privacy Act (I.F.), Federal Advisory Committee Act (FACA, I.G.), National Environmental Policy Act (NEPA, I.L.), Data Quality Act (I.O.; increasingly known as the Information Quality Act (IQA)), Inspector General Act (II.A.), Government Performance and Results Act (II.B.), Balanced Budget and Emergency Deficit Control Act (III.D.), Budget Enforcement Act (III.E.), Government Corporation Control Act (IV.A.), Davis-Bacon Act (V.F.), Unfunded Mandates Reform Act (UMRA, VI.C.), Hatch Act (VII.A.(5) and VII.A.(29)), Ethics in Government Act (VII.B.), Federal Tort Claims Act (VII.E.), and issues like information security (section I), improper payments (section III), services acquisition and contracting (section V), and federal employees and civil service laws (e.g., the National Security Personnel System at the Department of Defense, and the Department of Homeland Security personnel system (section VII.A)).

For each entry in the compendium, one or more CRS analysts present a brief history of the general management law, describe the law's major provisions, discuss key developments and issues, and provide source readings for readers who want more information. The compendium reflects the status of general management laws at the end of the first session of the 108th Congress, and will be updated along with the companion report to reflect actions taken through the close of the 108th Congress.

Introduction

Purposes

This report, General Management Laws: A Compendium (hereafter "compendium"), is a companion to CRS Report RL32388, General Management Laws: Major Themes and Management Policy Options, by Clinton T. Brass. In combination, these reports have three main objectives:

- to identify and describe the major general management laws under which the executive branch is required to operate, including their rationale, design, and scope;
- to assist Members of Congress and their staff in overseeing management of the executive branch; and
- to help Congress when considering potential changes to the management laws, as well as other legislation, including authorizing statutes and appropriations.[672]

[672] A related report, CRS Report RL30240, Congressional Oversight Manual, describes the major purposes, processes, techniques, and information sources for congressional oversight of the executive branch.

The compendium contains profiles of selected "general management laws" — broad statutes designed to regulate the activities, procedures, and administration of all or most executive branch agencies.[673] The quality of the general management laws, as well as their implementation, are considered crucial to maintaining the accountability of the executive branch to Congress, the President, and the public. Moreover, these laws influence the effectiveness of federal agencies when they implement, evaluate, and help formulate public policies.

As a complement to this compendium, the General Management Laws: Major Themes and Management Policy Options report ("companion report") focuses on major themes and possible management policy options for Congress that emerge when the general management laws are viewed together, as a whole. The compendium reflects the status of general management laws at the end of the first session of the 108th Congress, and will be updated along with the companion report to reflect actions taken through the close of the 108th Congress.[674]

How the Compendium and Companion Report Are Organized

Compendium

This compendium includes more than 90 separate entries that describe general management laws for the executive branch. The entries are organized into the following seven functional categories:[675]

- Information and Regulatory Management;
- Strategic Planning, Performance Measurement, and Program
- Evaluation;
- Financial Management, Budget, and Accounting;
- Organization;
- Procurement and Real Property Management;
- Intergovernmental Relations Management; and
- Human Resources Management and Ethics.

---

[673] Agencies are sometimes exempted from the coverage of specific general management laws due to a category into which they fall (e.g., department, government corporation, etc.), specific provisions in an agency's authorizing statute or appropriations, or provisions in the general management law itself.

[674] Previous versions of this compendium, coordinated by Ronald C. Moe, reflected the status of general management laws at the close of the 104th, 105th, and 106th Congresses, respectively. This compendium stands on the shoulders of these efforts.

[675] The listed functions are not necessarily the only way to categorize the report's entries into sections, which could have been aggregated differently or further broken down.

Within the management field, functions typically refer to "business areas that require related bundles of skill" or "groups of people with similar skills and performing similar tasks."[676] (In the private sector, by way of comparison, functions often include marketing, finance, production, and human resources.) This functional orientation is a major theme that the companion report addresses.

Most of the compendium's entries discuss a specific law, or in some cases, several related laws. The "Human Resources Management and Ethics" section, however, presents most civil service laws according to their codification in Title 5 of the United States Code — the way that practitioners and specialists typically discuss these laws. For each entry in this compendium, one or more CRS analysts present a brief history of the general management law in a section entitled Statutory Intent and History, describe the law itself in a section entitled Major Provisions, and close with a summary of key developments and issues in a Discussion section. Finally, for readers interested in more detail, each entry cites Selected Source Reading.

All the entries in the compendium conform to the overall structure described above; but because the laws have different audiences, levels of complexity, and histories, the entries sometimes differ in extent, level of detail, or emphasis.

Companion Report

In turn, as a complement to this compendium, the companion report identifies potential management policy options for Congress.[677] First, the companion report

[676] For more discussion of functional structures and perspectives within a management context, see John R. Schermerhorn Jr., Core Concepts of Management (Hoboken, NJ: John Wiley & Sons, 2004), pp. 119-120, and Peter F. Drucker, Management (New York: Harper & Row, 1974), pp. 558-563. This usage of the term function differs from usages found in Title 5 of the United States Code and in budgetary accounting. In Title 5, the term function is used in several contexts, including agency strategic plans (5 U.S.C. § 306, requiring agencies to specify goals and objectives for major functions and operations of the agency), transfer of functions (5 U.S.C. § 3503), and reductions in force (5 U.S.C. § 3502). Title 5 does not define the term, but the implementing regulations for transfer of functions and reductions in force define function as "all or a clearly identifiable segment of an agency's mission (including all integral parts of that mission), regardless of how it is performed" (5 C.F.R. § 351.203). With regard to budgetary accounting, the term function refers to categories of federal spending, organized according to the purpose or mission of government (e.g., income security, energy, and international affairs). The Congressional Budget and Impoundment Control Act of 1974 established the first statutory foundation for budget function classifications (see 2 U.S.C. § 632(a)(4) and 31 U.S.C. § 1104(c)). For background on budget function classifications, see CRS Report 98-280, Functional Categories of the Federal Budget, by Bill Heniff Jr.; and U.S. General Accounting Office, Budget Function Classifications: Origins, Trends, and Implications for Current Uses, GAO/AIMD-98-67, Feb. 1998.

[677] CRS Report RL32388, General Management Laws: Major Themes and Management Policy Options, by Clinton T. Brass.

provides historical context on the roles that Congress and the President play in managing the executive branch. Next, the companion report briefly discusses the extent to which management in the public and private sectors can be compared. Finally, the largest share of the companion report analyzes major themes that run through the general management laws and identifies potential management policy options for Congress. The themes include:

- Discretion for the Executive Branch. Congress frequently faces the issue of how much discretion to give the executive branch. Congress has several management policy options to address delegation situations and help balance agency flexibility with accountability.
- Standardization vs. Customization. Should the management laws under which agencies operate be standardized, with rules that apply uniformly to many different agencies? Or should some agencies have agency-specific laws that are customized to each agency's internal and external environments? Or should there be a mix of the two approaches? The report discusses advantages and disadvantages of the different approaches and analyzes two options for Congress when making these decisions.
- Functional Silos vs. Integrated General Management. A functional perspective (e.g., looking at agency operations from the perspective of a budget officer or human resources officer) is important, because it can boost efficiency through specialization and ensure centralized control over strategic decisions. However, if functional orientations become inward-looking, various functions can operate as "silos" — in isolation from one another — resulting in coordination problems or missed opportunities. The report analyzes policy options for Congress to bring an integrated general management perspective to solve agency management problems.
- Making and Measuring Progress. For over two decades, many executive branch agencies have suffered from persistent, major management problems. Often these problems relate to areas the general management laws were intended to address. The report analyzes potential options for measuring and motivating agency progress in improving management practices.
- Agency "Chief Officers" and Interagency Councils. Statutorily created "chief officers" (e.g., chief financial officers and chief acquisition officers) have increased in number and importance in federal agencies, as in the private sector. Congress also established interagency councils of these officers. The report analyzes options for Congress in considering whether additional chief officers and councils should be established, and how Congress might make the councils more accountable.

I. Information and Regulatory Management

A. Federal Register Act

Statutory Intent and History

The Federal Register Act was originally legislated in 1935 (49 Stat. 500) to establish accountability and publication arrangements for presidential proclamations and executive orders and for federal agency rules and regulations. The centerpiece of the resulting system is the Federal Register, an executive gazette produced by the Office of the Federal Register of the National Archives and Records Administration. It is printed by the Government Printing Office and lately has been available, as well, in electronic formats (online and via CD-ROM).[678]

In many respects, the Federal Register Act of 1935 was a response to the increasing number of regulations, rules, and related administrative actions of the New Deal era, and the fugitive status of these instruments. The expansion of the federal government during World War I had resulted in the presidential and agency issuance of a growing quantity of administrative requirements. Brief experience with a gazette — The Official Bulletin — had been beneficial, but of temporary, wartime, duration.[679] Its disappearance made a difficult situation worse. A contemporary observer characterized the operative situation in 1920 as one of "confusion,"[680] and another described the deteriorating conditions in 1934 as "chaos."[681] During the early days of the New Deal, administrative law pronouncements were in such disarray that, on one occasion, government attorneys arguing a lawsuit before the Supreme Court were embarrassed to find their case was based upon a nonexistent regulation,[682] and on another occasion, discovered they were pursuing litigation under a revoked executive order.

The response was the mandating of the Federal Register. Produced in a magazine format, it is now published each business day. Soon after enacting the Federal Register Act, Congress, in 1937, amended it and inaugurated the Code of Federal Regulations, a useful supplement to the Register (50 Stat. 304). This cumulation of the instruments and authorities appearing in the gazette contains almost all operative agency regulations, and is now updated annually.

---

[678] Commercially produced electronic versions of the Federal Register are available for purchase from private sector vendors who have introduced value-added features, such as search capability or annotations, to the basic GPO text.

[679] John Walters, "The Official Bulletin of the United States: America's First Official Gazette," Government Publications Review, vol. 19, May-June 1992, pp. 243-256.

[680] John A. Fairlie, "Administrative Legislation," Michigan Law Review, vol. 18 (Jan. 1920), p. 199.

[681] Erwin N. Griswold, "Government in Ignorance of the Law — A Plea for Better Publication of Executive Legislation," Harvard Law Review, vol. 48 (Dec. 1934), p. 199.

[682] United States v. Smith, 292 U.S. 633 (1934), appeal dismissed on the motion of the appellant without consideration by the Court.

Later, the general statutory authority underlying the Federal Register was relied upon for the creation of other series of publications — the United States Government Manual, which has been available for public purchase since 1939; the Public Papers of the Presidents, which were first published in 1960; and the Weekly Compilation of Presidential Documents, which was begun in the summer of 1965.

Major Provisions

The cumulative and operative authority of the Federal Register Act may be found in Chapter 15 of Title 44, United States Code. The Office of the Federal Register (OFR) is mandated and the appointment of its director by the Archivist of the United States is authorized. Responsibility for the production of the Federal Register and the preservation of the original copies of documents published in it are vested in the Archivist.

The original and two duplicate originals or certified copies of a document required or authorized to be published in the Federal Register must be filed with the OFR. Materials so filed are marked with a notation as to the date and hour of receipt. One copy of filed materials is immediately available for public inspection at the OFR.

Filed materials are transmitted to the Government Printing Office (GPO), which is responsible for the production and distribution of the Federal Register. The GPO also prepares, produces, and distributes periodic cumulative indices of the daily issues of the Register.

Documents which must be published in the Federal Register include:

- presidential proclamations and executive orders, except those not having general applicability and legal effect or effective only against federal agencies or persons in their capacity as officers, agents, or employees thereof;[683]
- documents or classes of documents that the President may determine from time to time have general applicability and legal effect;
- documents or classes of documents that may be required to be so published by act of Congress; and
- other documents or classes of documents authorized to be published by regulations prescribed with the approval of the President.

Conversely, the act declares that "comments or news items of any character may not be published in the Federal Register" (44 U.S.C. § 1505(b)).

---

[683] The Federal Register Act states that "every document or order which prescribes a penalty has general applicability and legal effect" (44 U.S.C. § 1505).

The requirements for filing documents for publication in the Federal Register may be suspended by the President during "an attack or threatened attack upon the continental United States." Such a suspension remains in effect "until revoked by the President, or by concurrent resolution of the Congress" (44 U.S.C. § 1505(c)).

Federal Register operations are supervised by the Administrative Committee of the Federal Register, which is chaired by the Archivist of the United States and includes a Department of Justice officer designated by the Attorney General, and the Public Printer. The director of the Office of the Federal Register serves as committee secretary. This panel, with the approval of the President, prescribes the regulations governing the Federal Register, including such matters as the documents to be authorized by regulation for publication in the gazette, the manner and form in which the Register is produced, and certain distribution matters and charges concerning it.

The Administrative Committee, with the approval of the President, also supervises and manages the production of the Code of Federal Regulations. The Code is a "complete codification of the documents of each agency of the Government having general applicability and legal effect, issued or promulgated by the agency by publication in the Federal Register or by filing with the Administrative Committee, and are relied upon by the agency as authority for, or are invoked or used by it in the discharge of, its activities or functions" (44 U.S.C. § 1510(a)). The Office of the Federal Register prepares and publishes the codifications appearing in the Code.

The Federal Register, the Code of Federal Regulations, and other series of publications produced pursuant to the general authority of the Federal Register Act are available to the public through sales, OFR and other websites ([http://www.archives.gov/federal_register/index.htm]), and distribution to federal depository libraries.

Discussion

While most major federal administrative law instruments — such as executive orders, presidential proclamations, and agency rules and regulations — are published in the Federal Register and Code of Federal Regulations, not all such authorities are so produced. During the past few years, concern has been expressed from time to time in Congress about certain national security directives of the President not being subject to accountability or publication under the Federal Register Act. They have been variously denominated as National Security Decision Memoranda during the Nixon-Ford Administrations, as Presidential Directives during the Carter Administration, as National Security Decision Directives during the Reagan Administration, as National Security Directives during the George H. W. Bush Administration, and as Presidential Decision Directives by the Clinton Administration. In 1988, a House

subcommittee held hearings on a proposal to amend the Federal Register Act to provide accountability in the use of these presidential directives. A complication in so legislating is that these instruments are usually all security classified. Another type — Homeland Security Presidential Directives — was launched by President George W. Bush in late October 2002. This development sparked renewed congressional concern about accountability for these presidential directives.

Selected Source Reading

U.S. Congress. House. Committee on Government Operations. Executive Orders and Proclamations: A Study of a Use of Presidential Powers. Committee print. 85th Congress, 1st session. Washington: GPO, 1957.

——. Presidential Directives and Records Accountability Act. Hearing on H.R. 5092. 100th Congress, 2nd session. Washington: GPO, 1989.

CRS Report 98-611. Presidential Directives: Background and Overview, by Harold
C. Relyea.

U.S. National Archives and Records Administration. Office of the Federal Register. Code of Federal Regulations: Title 1 — General Provisions. Washington: GPO, 1997.

Harold C. Relyea

B. Administrative Procedure Act

Statutory Intent and History

With the advent of the New Deal, greater expectations and reliance were placed upon the federal government for the achievement of certain political and social objectives. This required the development of both an expanded administrative law process and new regulatory agencies. Unlike a number of European states at that time, the United States did not have in place a sophisticated administrative system and had to build one. The first step was the passage of the Federal Register Act (described elsewhere in this compendium) in 1935, which required all federal agencies to publish notice of their rules, proposed rules, and legal notices in a single, readily available source, later to be known as the Federal Register.

Although substantial progress was made in uniform public notice and publication processes for regulation making by the agencies, a single general management law covering all the agencies was not passed until after World War II. The Administrative Procedure Act (APA; 60 Stat. 237; 5 U.S.C. § 551 et seq.), enacted in 1946, is considered the seminal federal administrative legislation of the modern era. The major contribution of the act was to establish for the first time minimum procedural requirements for certain types of agency decision making processes. Its general purposes were to (1) require agencies to keep the public currently informed of agency organization, procedures, and rules; (2) provide for public participation in the rulemaking process; (3) prescribe uniform standards for the conduct of formal rulemaking and adjudicatory proceedings (i.e., proceedings required by statute to be made on the record after opportunity for agency hearing); and (4) restate the law of judicial review of agency action.

The act imposes on agencies certain requirements for two modes of agency decision making: rulemaking and adjudication. In general, the term agency refers to any authority of the government of the United States, whether or not it is within, or subject to review by, another agency. Congress, the courts, and the governments of territories, possessions, and the District of Columbia are excluded.

Major Provisions

The APA has two major subdivisions: Sections 551-559, dealing with general agency procedures, and Sections 701-706, dealing with judicial review. In addition, several sections dealing with administrative law judges are scattered throughout Title 5 (Sections 1305, 3105, 3344, 5372, and 7521).

The structure of the APA is shaped around the distinction between rulemaking and adjudication, with different schemes of procedural requirements prescribed for each. Rulemaking is agency action that formulates the future conduct of persons, through the development and issuance of an agency statement designed to implement, interpret, or prescribe law or policy. It is essentially legislative in

nature because of its future general applicability and its concern for policy considerations. Adjudication, on the other hand, is concerned with determination of past and present rights and liabilities. The result of an adjudicative proceeding is the issuance of an order.

Beyond the distinction between rulemaking and adjudication, the APA subdivides each of these categories of agency action into formal and informal proceedings. Whether a particular rulemaking or adjudicatory proceeding is considered to be "formal" depends on whether the proceeding is required by statute to be "on the record after opportunity for an agency hearing" (5 U.S.C. § 553(c), § 554(a)). The act prescribes elaborate procedures for both formal rulemaking and formal adjudication, and relatively minimal procedures for informal rulemaking. Virtually no procedures are prescribed by the APA for the remaining category of informal adjudication, which is by far the most prevalent form of governmental action.

Rulemaking

Section 553 sets the requirements for informal rulemaking (also known as notice and comment rulemaking). An agency must publish a notice of proposed rulemaking in the Federal Register, afford interested persons an opportunity to participate in the proceeding through the submission of written comments or, at the discretion of the agency, by oral presentation, and when consideration of the matter is completed, incorporate in the rules adopted "a concise general statement of their basis and purpose" (5 U.S.C. § 553(c)). A final rule must be published in the Federal Register "not less than 30 days before its effective date" (5 U.S.C. § 553(d)). Interested persons have a right to petition for the issuance, amendment or repeal of a rule (5 U.S.C. § 553(e)). Although the APA does not specify a minimum period for public comment, at least 30 days have been traditionally allotted. More recently, Executive Order 12866[684] has prescribed that covered agencies allow at least 60 days. Agencies are free to grant additional procedural rights, and Congress has at times particularized requirements for certain agencies or programs.

The APA also provides for formal rulemaking, a procedure employed when rules are required by statute to be made on the record after an opportunity for agency hearing. Essentially, this procedure requires that the agency issue its rule after the kind of trial-type hearings procedures normally reserved for adjudicatory orders (discussed below).

Adjudication

[684] 3 C.F.R., 1993 Comp., pp. 638-649.

Sections 554, 556, and 557 apply to formal adjudications (i.e., cases for which an adjudicatory proceeding is required by statute to be determined on the record after an agency proceeding). Sections 556 and 557 spell out the specific procedures to be utilized in formal adjudication. In brief, a trial type hearing must be held, presided over by members of the agency or an administrative law judge (ALJ). Section 556 prescribes the duties of ALJs, the allocation of burden of proof, and parties' rights to cross-examination. Section 557 provides that an ALJ must issue an initial decision, which becomes the agency's final decision if not appealed. The record must show the ruling on each finding, conclusion, or exception raised. Ex parte communications relevant to the merits of a pending formal agency proceeding are prohibited.

Judicial Review of Agency Action

Sections 701-706 constitute a general restatement of the principles of judicial review embodied in many statutes and judicial decisions; however, they leave the mechanics regarding judicial review to be governed by other statutes or court rules.

Section 701 establishes a presumption of reviewability of agency actions by providing that the action "of each authority of the Government of the United States" is subject to judicial review except where "statutes preclude judicial review," or "where agency action is committed to agency discretion by law" (Section 701(a)(1),(2)). The Supreme Court has consistently supported the strong presumption of reviewability, requiring a "showing of 'clear and convincing' evidence of a ... legislative intent to restrict access to judicial review." (Citizens to Protect Overton Park v. Volpe, 401 U.S. 402, 410 (1971); Abbott Laboratories v. Gardner, 387 U.S. 136, 141 (1967); Bowen v. Michigan Academy of Family Physicians, 476 U.S. 667, 681 (1986)). Moreover, the exception for actions "committed to agency discretion" is narrowly construed and is applicable only in "rare instances where statutes are drawn in such broad terms that in a given case, there is no law to apply" (Volpe, supra, 401 U.S. at 410).

A challenge may be brought by any person who is "adversely affected or aggrieved" by the action "within the meaning of the relevant statute" (5 U.S.C. § 702). Courts deciding the standing of a person challenging a rule also must comply with the limitations on federal court jurisdiction imposed by the "case or controversy" requirement of Article III of the Constitution, which has been interpreted to require that a party bringing an action in federal court demonstrate an "injury in fact," caused by the violation of a legally protected interest, that is concrete and particularized, and actual or imminent, as opposed to conjectural or hypothetical (see Valley Forge Christian College v. Americans United for Separation of Church and State, 454 U.S. 473 (1982); see also Lujan v. Defenders of Wildlife, 504 U.S. 555 (1992)). In addition, parties seeking to establish constitutional standing are required to show that their injury "fairly can be traced to the challenged action" and that the injury is likely to be redressed by a favorable judicial decision (Allen v. Wright, 468 U.S. 737 (1984); Valley Forge,

supra, at 472). A person challenging an agency rule who satisfies Section 702*s test is also likely to satisfy the injury requirement for constitutional standing. Indeed, courts typically merge their discussions of Section 702*s "adversely affected or aggrieved" language with the constitutional injury requirement (see, e.g., Wilderness Society v. Griles, 824 F.2d 4, 11 (D.C. Cir. 1987)).

In addition to constitutional requirements, the judiciary has developed prudential rules to constrain the instances in which review may be obtained. Like their constitutional counterparts, these judicially imposed limits on the exercise of federal jurisdiction are "founded in concern about the proper — and properly limited — role of the courts in a democratic society" (see Warth v. Seldin, 422 U.S. 490, 498 (1974)). However, unlike their constitutional counterparts, they may be modified or abrogated by Congress. The prudential components of the standing doctrine require that (1) a plaintiff assert his own legal rights and interests rather than those of third parties; (2) a plaintiff's complaint be encompassed by the "zone of interests" protected or regulated by the constitutional or statutory guarantee at issue; and (3) courts decline to adjudicate "'abstract questions of wide public significance' which amount to 'generalized grievances' pervasively shared and most appropriately addressed in the representative branches" (Valley Forge, supra, at 472).

Any standing inquiry is further complicated in instances when an organization seeks to challenge agency action. An organization may have standing to sue if it has been injured as an entity, and may likewise possess standing to sue on behalf of its members, so long as the members would otherwise have standing to sue in their own right; the interests the organization seeks to protect are germane to its purpose; and neither the claim asserted nor the relief requested requires the participation of individual members (see Hunt v. Washington State Apple Advertising Commission, 432 U.S. 333, 343 (1977)).

The forum for judicial review of agency rules is determined by statute. Statutes containing judicial review provisions applicable to rulemaking generally call for direct, pre-enforcement review in the courts of appeals, and usually specify requirements as to venue, timing of review, and scope of review. If there is no specifically applicable judicial review provision governing the agency's rule, a challenge to the rule will normally be through an action for an injunction or declaratory relief in a district court. Jurisdiction must be obtained through one of the general jurisdictional statutes, the most frequently asserted being 28 U.S.C. § 1331, the so-called "federal question" provision, which gives district courts "original jurisdiction of all civil actions wherever the matter in controversy ... arises under the Constitution, laws, or treaties of the United States." Other jurisdictional provisions that may be used are 28 U.S.C. § 1337 (actions arising under commerce-related statutes) and 28 U.S.C. § 1361 (mandamus jurisdiction).

Section 706 sets forth the scope of review of agency actions. In general, the scope of review depends on the nature of the agency determination under challenge. Agency conclusions on questions of law are reviewed de novo. When a court

reviews an agency's construction of a statute it administers, the court is required to uphold Congress's intent where Congress has directly spoken to the precise statutory question at issue. If the statute is silent or ambiguous with respect to the specific issue, however, the agency's interpretation of the statute must be upheld if the agency's construction of the statute is permissible (see Chevron U.S.A. v. NRDC, 467 U.S. 837 (1984)). The Supreme Court has clarified the limits of this standard, ruling that Chevron deference applies only in instances when Congress has delegated authority to an agency to make rules carrying the force of law, and when the agency interpretation claiming deference was promulgated pursuant to that authority (see United States v. Mead Corp., 533 U.S. 218, 229 (2001)).

Agency exercises of judgment or discretion, such as in informal rulemaking or informal adjudication, are reviewed under the "arbitrary, capricious, abuse of discretion" standard. Under this standard, an agency determination will be upheld if it is rational, based on a consideration of the relevant factors, and within the scope of the authority delegated to the agency by Congress. The agency must examine the relevant data and articulate a satisfactory explanation for its action, including a rational connection between the facts found and the choices made. A court is not to substitute its judgment for that of the agency (see Motor Vehicle Mfr's Assoc. v. State Farm Mut. Auto Ins. Co., 463, U.S. 29, 42-43 (1983)).

Agency determinations of fact, typically in challenges of agency adjudications, are reviewed under the "substantial evidence" test when the agency determination is reviewed on the record of an agency proceeding required by statute (see Consolo v. FMC, 383 U.S. 607, 618-21 (1966)), citing (Universal Camera v. NLRB, 340 U.S. 474 (1951)).

Discussion

The APA retains its preeminence as the general management law governing agency decisionmaking by means of rulemaking and adjudication. Essentially unamended by Congress since 1946, it has maintained its vitality in the face of vast and fundamental changes in the nature and scope of federal government responsibilities. In great measure this accommodation has come about because of judicial rulings that have effected important transformations of the meaning and scope of its otherwise neutral and spare terminology. The hallmark of our modern administrative state — agency rulemaking through the process of informal rulemaking — is a creative judicial cultivation. With the encouragement of the courts, rulemaking replaced adjudication as the dominant formal decision making process. Administrative lawmaking was "democratized" in a series of decisions between 1965 and 1983 that expanded both the obligations of agencies and the role of reviewing courts. The result has been the transformation, without benefit of legislative amendment, of informal rulemaking into a new, on-the-record proceeding that has fostered widespread public participation in the process.

To be sure, Congress has not simply silently acquiesced in this revolutionary transformation. Although Congress has never undertaken a comprehensive revision of the APA, it has always recognized that it could do so, and with increasing frequency, it has supplanted the APA's requirements with more explicit directives for particular agencies and programs mirroring the above-described judicial innovations. Often this legislation has been aimed at formalizing the procedural protections ensuring effective and meaningful public participation in agency policymaking. Thus, certain health, environmental, and consumer protection statutes, for example, contain detailed "hybrid-rulemaking" requirements and procedural as well as substantive changes.[685]

Moreover, the deregulation movement of the 1970s and 1980s successfully focused attention on the economic consequences of regulation and the need for a broader analytic approach to regulatory decision making that assessed the impacts of costs and new technologies. The executive branch took the lead by adding new layers of clearances for rules by executive order that included requirements for consideration and evaluation of their costs and benefits. (See Executive Orders 12291, 12498, and 12866).[686] Proposed regulatory reform legislation in recent Congresses has included bills that not only would have codified the judicially created procedural requirements of the last two decades, but also would have required all agencies engaged in rulemaking to utilize methodologies requiring detailed risk assessment and cost benefit analysis for major regulations which would have been subjected to intense judicial review. While these particular reform efforts have been unsuccessful, Congress has passed several notable measures, including a mechanism that subjects all agency rules to congressional review and possible veto; a procedure to require the General Accounting Office to conduct an independent evaluation of an agency's cost-benefit analysis of a proposed or final rule when requested by a chair or ranking member of a committee of jurisdiction; a process designed to restrict regulations imposing unfunded costs on state and local governments and the private sector; and a process designed to ensure that federal agencies use and disseminate accurate information. There is also an emerging and controversial trend on the part of agencies to attempt to enhance public participation in the administrative process by accepting electronically submitted comments.

---

[685] See, e.g., 42 U.S.C. § 300g-1(d) (requiring public hearing prior to the promulgation of regulations pursuant to the Safe Drinking Water Act); 15 U.S.C. § 2605 (providing for public hearing and opportunity for cross-examination of witnesses prior to promulgation of regulations under the Toxic Substances Control Act); and 15 U.S.C. § 2058 (providing for a public hearing before promulgation of rules under the Consumer Product Safety Act).

[686] See 3 C.F.R., 1981 Comp., pp. 127-134; 3 C.F.R., 1985 Comp., pp. 323-325; and 3 C.F.R., 1993 Comp., pp. 638-649, respectively.

While the APA's basic rulemaking model is relatively straightforward, it has been argued that the additional requirements that have been imposed by Congress, the executive branch, and the courts have made the rulemaking process rigid and burdensome upon agencies. In turn, this has led to the argument that rulemaking has become "ossified," with agencies either undertaking resource and time intensive steps to ensure that a rule will withstand increased scrutiny, or simply circumventing the traditional rulemaking process by issuing policy statements and interpretive rules to effectuate compliance with a regulatory agenda. Ultimately, however, it would appear that the current APA scheme is likely to continue to be the key vehicle for formulating and implementing agency policy directives.

Selected Source Reading

Aman, Alfred C. Jr., and William T. Mayton. Administrative Law and Process. New York: Matthew Bender, 1993.

Johnson, Stephen M. "The Internet Changes Everything: Revolutionizing Public Participation and Access to Government Information Through the Internet." Administrative Law Review, vol. 50 (spring 1998), pp. 277-337.

Kerwin, Cornelius M. Rulemaking: How Government Agencies Write Law and Make Policy, 2nd ed. Washington: CQ Press, 1999.

Koch, Charles H. Administrative Law and Practice, 2nd ed., 3 vols. St. Paul, MN: West Publishing Co., 1997.

Lubbers, Jeffrey S. A Guide to Federal Rulemaking, 3rd ed. Washington: American Bar Association, 1998.

McGarity, Thomas O. "Some Thoughts on 'Deossifying' the Rulemaking Process." Duke Law Journal, vol. 41, 1992, pp. 1385-1462.

O'Reilly, James T. "The 411 on 515: How OIRA's Expanded Information Roles in 2002 Will Impact Rulemaking and Agency Publicity Actions." Administrative Law Review, vol. 54 (spring 2002), pp. 835-851.

Pierce, Richard J. Jr. "Seven Ways to Deossify Agency Rulemaking." Administrative Law Review, vol. 47 (winter 1995), pp. 59-95.

Shepherd, George B. "Fierce Compromise: The Administrative Procedure Act Emerges From New Deal Politics." Northwestern University Law Review, vol. 90 (1996), pp. 1557-1683.

Verkuil, Paul R. "Comment: Rulemaking Ossification — A Modest Proposal." Administrative Law Review, vol. 47 (summer 1995), pp. 453-459.

CRS Report RL32339, Federal Regulations: Efforts to Estimate Total Costs and Benefits of Rules, by Curtis W. Copeland.

CRS Report RL32356, Federal Regulatory Reform: An Overview, by Curtis W. Copeland.

CRS Report RL32240, The Federal Rulemaking Process: An Overview, by Curtis W. Copeland.

Morton Rosenberg
T. J. Halstead

C. Federal Records Act and Related Chapters of Title 44

Statutory Intent and History

Proper maintenance of federal records within the departments and agencies has been legislatively addressed by Congress since the earliest days of the republic. When chartering the initial departments, for example, Congress authorized the heads of these entities to issue regulations for, among other matters, the custody, use, and preservation of the records, papers, and property.[687] It was also the responsibility of these officials to ensure that these regulations were observed in practice.

Through the years, Congress from time to time legislated additional requirements and administrative arrangements concerning federal records. In 1934, for instance, a major step was taken with the mandating of the National Archives (48 Stat. 1122).[688] The head of this entity, the Archivist of the United States, has subsequently become a major policy leader regarding the entire life cycle of federal records, including their (1) creation or collection; (2) processing; (3) transmittal, including access and dissemination; (4) use; (5) active storage; (6) inactive storage; and (7) final disposition.[689]

The Federal Records Act of 1950 (64 Stat. 583) was another milestone. While it is most often remembered for its placement of the Archivist and the National Archives under the authority of the Administrator of the General Services Administration,[690] among the statute's important innovations were:

- creation of the National Historical Publications Commission to "make plans, estimates, and recommendations for such historical works and collections of sources as it deems appropriate for printing or otherwise recording at the public expense ... [and to] cooperate with and encourage both governmental and nongovernmental institutions, societies, and individuals in collecting and preserving and, when it deems such action to be desirable, in editing and publishing the papers of outstanding citizens of the United States and such other documents as may be important for an

---

[687] See, for example, 1 Stat. 28, 49, and 65; these and similar provisions were consolidated in the Revised Statutes of the United States (1878) at Section 161, which is presently located in the United States Code at 5 U.S.C. § 301.

[688] The National Archives was rechartered in the National Archives and Records Administration Act of 1984 (98 Stat. 2280), which largely constitutes Chapter 21 of Title 44 of the United States Code.

[689] Peter Hernon, "Information Life Cycle: Its Place in the Management of U.S. Government Information Resources," Government Information Quarterly, vol. 11, 1994, pp. 143-170.

[690] This relationship ended in 1984 when the National Archives was restored to the status of an independent agency within the executive branch.

understanding and appreciation of the history of the United States" (44 U.S.C. §§ 2501-2506);
- authorizing the analysis, development, promotion, and coordination of standards, procedures, and techniques "designed to improve the management of records, to insure the maintenance and security of records deemed appropriate for preservation, and to facilitate the segregation and disposal of records of temporary value," and other related actions (44 U.S.C. §§ 2904-2906);
- authorizing the establishment, maintenance, and operation of records centers "for the storage, processing, and servicing of records for Federal agencies pending their deposit with the National Archives of the United States or their disposition in any other manner authorized by law" (44 U.S.C. § 2907);
- prescribing the records management responsibilities of agency heads (44 U.S.C. §§ 3101-3107); and
- prescribing archival administration responsibilities for the deposit of federal agency and congressional records "determined by the Archivist to have sufficient historical or other value to warrant their continued preservation by the United States Government" in the National Archives, and other related actions (44 U.S.C. §§ 21072111).

The provisions of the Federal Records Act and those of subsequent records management statutes are largely codified in chapters of Title 44 of the United States Code.

Major Provisions

Within Title 44 of the United States Code, Chapters 21, 22, 29, 31, and 33 contain major provisions of records management law. The first of these, Chapter 21, after prescribing the establishment, organization, and principal leadership of the National Archives and Records Administration, specifies certain general authority, duties, and responsibilities of the Archivist. These include procedures and conditions for the acceptance of records for historical preservation; responsibility for the custody, use, and withdrawal of records transferred to the Archives; responsibilities for the preservation, arrangement, duplication, and exhibition of records by the Archivist; and the procedures and conditions governing the establishment of a presidential archival depository or presidential library to be accepted and maintained by the Archivist.[691]

Chapter 22 contains the provisions of the Presidential Records Act of 1978 (92 Stat. 2523), which marked a major change in federal policy on the custody and

[691] Concerning the acceptance and maintenance of presidential archival depositories by the Archivist, see CRS Report RS20825, Presidential Libraries: The Federal System and Related Legislation, by Harold C. Relyea.

preservation of presidential records. As a consequence of the Watergate incident and related matters, the official papers and records of President Richard Nixon were placed under federal custody by specially legislated arrangements — the Presidential Recordings and Materials Preservation Act of 1974 (88 Stat. 1695). This statute requires that these materials remain in Washington, DC, where they are maintained under the supervision of the Archivist. Thus, Nixon neither could take his presidential records and documents with him when he left office, nor could place them in a presidential library outside the nation's capital.

This 1974 statute also created the temporary National Study Commission on Records and Documents of Federal Officials (88 Stat. 1698). The panel was tasked "to study problems and questions with respect to the control, disposition, and preservation of records and documents produced by on behalf of Federal officials, with a view toward the development of appropriate legislative recommendations and other recommendations regarding appropriate rules and procedures with respect to such control, disposition, and preservation." Its final report was issued in March 1977.[692]

Responding partly to some of the commission's recommendations, Congress legislated the Presidential Records Act in 1978. After defining "presidential records," the statute specifies that all such materials created on or after January 20, 1981, are subject to its provisions. It effectively made presidential records federal property, to remain under the custody and control of the Archivist when each incumbent President left the White House. Jimmy Carter was the last occupant of the Oval Office who could freely take away his records and papers.

Chapter 29, setting out the records management authority and responsibilities of the Archivist and the Administrator of General Services, contains core provisions from the Federal Records Act of 1950. Specified here are the objectives of federal records management, the two officials' general responsibilities for records management, and the Archivist's authority to establish standards for the selective retention of records, inspect agency records, and establish, maintain, and operate records centers.

Chapter 31, also containing core provisions from the Federal Records Act, prescribes the records management responsibilities of the federal agencies, including the general duties of agency heads, the requirement to establish and maintain "an active, continuing program for the economical and efficient management of the records of the agency," and certain related procedural matters.

---

[692] U.S. National Study Commission on Records and Documents of Federal Officials, Final Report of the National Study Commission on Records and Documents of Federal Officials (Washington: GPO, 1977). Also see Anna Kasten Nelson, "The Public Documents Commission: Politics and Presidential Records," Government Publications Review, vol. 9, Sept./Oct. 1982, pp. 431-451.

Chapter 33 is devoted to the disposal of federal records. It authorizes the Archivist to issue regulations and utilize a system of records lists and disposition schedules to eliminate non-current agency records lacking preservation value.

Discussion

Most of the existing statutory law concerning records management was developed when paper formats dominated federal recordkeeping and production. During the past few decades, the adequacy of this authority has come into question as electronic forms and formats have become more prevalent. The many challenges of the electronic record phenomenon continue to be discussed and evaluated. General Records Schedule (GRS) 20, a primary, government-wide, records management directive, has been revised recently, and efforts are underway to develop an electronic records archive at the National Archives.

Selected Source Reading

National Research Council. Building an Electronic Records Archive at the National
Archives and Records Administration: Recommendations for Initial
Development. Washington: National Academies Press, 2003.

U.S. National Archives and Records Administration. Disposition of Federal Records. Washington: GPO, 1992.

——. Guide to Record Retention Requirements in the Code of Federal Regulations. Washington: GPO, 1986.
Harold C. Relyea

D. Congressional Review of Regulations Act

Statutory Intent and History

The Supreme Court's acceptance in 1937 of the New Deal's rejection of passive, minimalist governance, and its replacement by a more activist governmental philosophy, signaled the beginning of the era of the administrative state that has seen the emergence of a pattern of pervasive governmental economic and social regulation. Since 1937, an unbroken line of Supreme Court and lower court decisions has provided legitimacy for broad delegations of congressional power to the executive, and has fostered and nurtured the hallmark of the modern administrative state, agency lawmaking through the process of informal rulemaking. With the encouragement of the courts, rulemaking has replaced adjudication as the dominant formal administrative decision making process.

The necessity to delegate increasing amounts of legislative power to administrative agencies to accomplish the expanded objective of government, while at the same time maintaining congressional control and responsibility over the exercise of the delegated authority, created a constitutional tension, however. This tension has been manifested over the years by a variety of legislative attempts to develop a review mechanism that would allow Congress to exercise its oversight responsibility to assure agency accountability in the exercise of delegated authority. Initially, Congress increasingly relied on the legislative veto, a device that allowed it to delegate power conditionally and to retrieve it, or block agency exercise of its delegated authority, by the action of both houses, one house, a committee, or, at times, by a committee chairman alone. In 1983, in INS v. Chadha (462 U.S. 919 (1983)), the Supreme Court found all such veto mechanisms to be an unconstitutional exercise of legislative power because of their failure to follow the Constitution's exclusive prescription for lawmaking: bicameral passage and presentment to the President for his signature or veto.

The immediate consequence of the Supreme Court's ruling was to force Congress to rely more heavily on its traditional mechanisms of control of administrative action, such as the authorization and appropriations process, committee oversight and investigations, and the confirmation process as means of restraining perceived regulatory excesses. In addition, regulatory reform proposals throughout the 1980s and 1990s consistently contained requirements that agencies perform cost-benefit, cost-effectiveness and risk assessment analyses as integral parts of their rulemaking processes.

None of these government-wide reforms succeeded until the enactment of the Small Business Regulatory Enforcement Fairness Act of 1996 (SBREFA; 110 Stat. 857-874). Subtitle E of the act for the first time established a mechanism by which Congress can disapprove, on a fast-track, virtually all federal agency rules. Failure to report a covered rule for congressional review will prevent the rule from becoming effective. The effectiveness of major rules is stayed for 60 days to allow for congressional scrutiny. A rule vetoed by the passage of a joint resolution of disapproval is deemed never to have been effective and an agency

may not propose to issue a substantially similar rule without further congressional authorization.

However, a number of unresolved interpretive issues, as well as certain structural problems, have limited the effectiveness of this review mechanism.

Major Provisions

The congressional review mechanism, codified at 5 U.S.C. §§ 801-808, requires that all agencies promulgating a covered rule must submit a report to each house of Congress and to the Comptroller General (CG) that contains a copy of the rule, a concise general statement describing the rule (including whether it is deemed to be a major rule), and the proposed effective date of the rule. A rule cannot take effect if the report is not submitted (Section 801(a)(1)(A)). Each house must send a copy of the report to the chairman and ranking minority member of each jurisdictional committee (Section 801(a)(1)(C)). In addition, the promulgating agency must submit to the CG (1) a complete copy of any cost-benefit analysis; (2) a description of the agency*s actions pursuant to the requirements of the Regulatory Flexibility Act and the Unfunded Mandates Reform Act of 1995; and (3) any other relevant information required under any other act or executive order. Such information must also be made "available" to each house (Section 801(a)(1)(B)).

Section 804(3) adopts the definition of rule found at 5 U.S.C. § 551(4) which provides that the term "means the whole or part of an agency statement of general ... applicability and future effect designed to implement, interpret, or prescribe law or policy."[693] The legislative history of Section 551 (4) indicates that the term is to be broadly construed: "The definition of rule is not limited to substantive rules, but embraces interpretive, organizational and procedural rules as well."[694] The courts have recognized the breadth of the term, indicating that it encompasses "virtually every statement an agency may make,"[695] including interpretive and substantive rules, guidelines, formal and informal statements, policy proclamations, and memoranda of understanding, among other types of

[693] Section 804(3) excludes from the definition "(A) any rule of particular applicability, including a rule that approves or prescribes for the future rates, wages, prices, services, or allowance therefore, corporate or financial structures, reorganizations, mergers, or acquisitions thereof, or accounting practices or disclosures bearing on any of the foregoing; (B) any rule relating to agency management or personnel; or (C) any rule of agency organization, or practice that does not substantially affect the rights or obligations of non-agency parties."

[694] U.S. Attorney General, Manual on the Administrative Procedure Act, 13 (1948).

[695] Avoyelles Sportsmen's League, Inc., v. Marsh, 715 F.2d 897 (5th Cir. 1983).

actions.[696] Thus a broad range of agency action is potentially subject to congressional review.

The Comptroller General and the administrator of the Office of Information and Regulatory Affairs (OIRA) of the Office of Management and Budget have particular responsibilities with respect to a "major rule," defined as a rule that will likely have an annual effect on the economy of $100 million or more, increase costs of processing for consumers, industries, or state and governments, or have significant adverse effects on the economy. The determination of whether a rule is major is assigned exclusively to the OIRA administrator (Section 804(2)). If a rule is deemed major by the OIRA administrator, the CG must prepare a report for each jurisdictional committee within 15 calendar days of the submission of the agency report required by Section 801 (a)(1) or its publication in the Federal Register, whichever is later. The statute requires that the CG's report "shall include an assessment of the agency's compliance with the procedural steps required by Section 801(a)(1)(B)." However, the CG has interpreted his duty under this provision narrowly as requiring that he simply determine whether the prescribed action has been taken, i.e., whether a required cost-benefit analysis has been provided, and whether the required actions under the Regulatory Flexibility Act, the Unfunded Mandates Reform Act of 1995, and any other relevant requirements under any other legislation or executive orders were taken, not whether the action was properly done or was in accord with congressional intent.

The designation of a rule as major also affects its effective date. A major rule may become effective on the latest of the following scenarios: (1) 60 days after Congress receives the report submitted pursuant to Section 801(a)(1) or after the rule is published in the Federal Register; (2) if Congress passes a joint resolution of disapproval and the President vetoes it, the earlier of when one house votes and fails to override the veto, or 30 days after Congress receives the message; or (3) the date the rules would otherwise have taken effect (unless a joint resolution is enacted) (Section 801(a)(3)).

Thus, the earliest a major rule can become effective is 60 days after the submission of the report required by Section 801(a)(1) or its publication in the Federal Register, unless some other provision of the law provides an exception for an earlier date. Three possibilities exist. Under Section 808(2) an agency may determine that a rule should become effective notwithstanding Section 801(a)(3) where it finds "good cause in that notice and public procedure thereon

---

[696] See, for example, Chem Service, Inc. v. EPA, 12 F.3d 1256 (3rd Cir. 1993)(memorandum of understanding); Caudill v. Blue Cross and Blue Shield of North Carolina, 999 F.2d 74 (4th Cir. 1993)(interpretative rules); National Treasury Employees Union v. Reagan, 685 F.Supp 1346 (E.D. La 1988)(federal personnel manual letter issued by the Office of Personnel Management); New York City Employment Retirement Board v. SEC, 45 F.3d 7 (2nd Cir. 1995)(affirming lower court's ruling that SEC "no action" letter was a rule within Section 551(4)).

are impracticable, unnecessary, or contrary to the public interest." Second, the President may determine that a rule should take effect earlier because of an imminent threat to health or safety or other emergency; to insure the enforcement of the criminal laws; for national security purposes; or to implement an international trade agreement (Section 801(c)). Finally, a third route is available under Section 801(a)(5), which provides that "the effective date of a rule shall not be delayed by operation of this chapter beyond the date on which either House of Congress votes to reject a joint resolution of disapproval under Section 802." All other rules take effect "as otherwise allowed by law," after having been submitted to Congress under Section 801(a)(1) (Section 801(a)(4)).

All covered rules are subject to disapproval even if they have gone into effect. Congress has reserved to itself a review period of at least 60 days. Moreover, if a rule is reported within 60 session days of the Senate or 60 legislative days of the House prior to the date Congress adjourns a session of Congress, the period during which Congress may consider and pass a joint resolution of disapproval is extended to the next succeeding session of Congress (Section 801(d)(1)). Such held-over rules are treated as if they were published on the 15th session day of the Senate and the 15th legislative day of the House in the succeeding session, and as though a report under Section 801(a)(1) was submitted on that date (Section 801(d)(2)(A), (e)(2)). But a held-over rule takes effect as otherwise provided (Section 801(d)(3)). Only the opportunity to consider and disapprove is extended.

If a joint resolution of disapproval is enacted into law, the rule is deemed not to have had any effect at any time (Section 801(f)). If a rule that is subject to any statutory, regulatory, or judicial deadline for its promulgation is not allowed to take effect, or is terminated by the passage of a joint resolution, any deadline is extended for one year after the date of enactment of the joint resolution (Section 803). A rule that does not take effect, or is not continued because of passage of a disapproval resolution, may not be reissued in substantially the same form. Indeed, any reissued or new rule that is "substantially the same" as a disapproved rule cannot be issued unless it is specifically authorized by a law enacted subsequent to the disapproval of the original rule (Section 801(b)(2)).

Section 802(a) provides a process for an up-or-down vote on a joint resolution of disapproval within a 60-day period (excluding days when either house is adjourned for more than three days). The period begins running either on the date on which the Section 801(a)(1) report is submitted, or when the rule is published in the Federal Register, whichever is later.

The law spells out an expedited consideration procedure for the Senate. If the committee to which a joint resolution is referred has not reported it out within 20 calendar days, it may be discharged from further consideration by a written petition of 30 Members of the Senate, at which point the measure is placed on the calendar. After committee report or discharge, it is in order at any time for a motion to proceed to consideration. All points of order against the joint

resolution (and against consideration of the measure) are waived, and the motion is not subject to amendment or postponement, or to a motion to proceed to other business. If the motion to consider is agreed to, it remains as unfinished business of the Senate until disposed of (Section 802(d)(1)). Debate on the floor is limited to 10 hours. Amendments to the resolution and motions to postpone or to proceed to other business are not in order (Section 802(d)(2)). At the conclusion of debate, an up-ordown vote on the joint resolution is to be taken (Section 802(d)(3)).

There is no special procedure for expedited consideration and processing of joint resolutions in the House. But if one house passes a joint resolution before the other house acts, the measure of the other house is not referred to a committee. The procedure of the house receiving a joint resolution "shall be the same as if no joint resolution had been received from the other house, but the vote on final passage shall be on the joint resolution of the other house" (Section 802(f)(1)(2)).

Section 805 precludes judicial review of any "determination, finding, action or omission under this chapter." This would insulate from court review, for example, a determination by the OIRA administration that a rule is major or not, a presidential determination that a rule should become effective immediately, an agency determination that "good cause" requires a rule to go into effect at once, or a question as to the adequacy of a Comptroller General's assessment of an agency's report.

Discussion

As of January 14, 2004, the Comptroller General had submitted reports pursuant to Section 801(a)(2)(A) to Congress on 488 major rules.[697] In addition, GAO has cataloged the submission of 32,865 non-major rules as required by Section 801(a)(1)(A). To date, 29 joint resolutions of disapproval have been introduced relating to 21 rules. One rule has been disapproved: the Occupational Safety and Health Administration's (OSHA's) ergonomics standard in March 2001. A second rule, the Federal Communication Commission's (FCC's) rule relating to broadcast media ownership, was disapproved by the Senate on September 16, 2003 but was not acted upon by the House.

After eight years, the limited use to which the rulemaking review mechanism has been put does not appear to be attributable to a lack of familiarity with the law, but rather to a number of other factors. Some have argued that agencies are more carefully assessing their regulations to avoid possible congressional disapproval resolutions. Others maintain that the current review process discourages utilization of the act. These critics point to a number of interpretive

[697] U.S. General Accounting Office, Reports on Federal Agency Major Rules, available at [http://www.gao.gov/decisions/majrule/majrule.htm], visited Jan. 22, 2004.

issues concerning the scope of the law's coverage, the judicial enforceability of its key requirements, and whether a disapproval resolution may be directed at part of a rule as factors which introduce uncertainties into the use of the disapproval resolution process.

Specific problems identified by critics of the current process include (1) the lack of a screening mechanism to identify rules that require congressional review; (2) the absence of an expedited review procedure in the House of Representatives; (3) the deterrent effect of the ultimate need for a supermajority of both houses to veto a rule;
(4) the reluctance to disapprove an omnibus rule where only a part of the rule raises objections; (5) the uncertainty of which rules are covered by the act; (6) the uncertainty whether the failure to report a covered rule to Congress can be reviewed and sanctioned by a court; and (7) the scope of the limitation that precludes an agency from promulgating a "substantially similar rule" after the disapproval of a rule. Perceived agency failures to report rules covered by the CRA for review and the lack of any basis to timely challenge the substantiality of agency cost-benefit analyses were the subject of oversight hearings in both houses during the 106th Congress. A product of those inquiries was the passage of the Truth in Regulating Act of 2000, which required the Comptroller General to conduct an independent evaluation of an agency's cost-benefit assessment accompanying a proposed or final economically significant rule when requested by a chair or ranking minority member of a committee of jurisdiction. The CG's evaluations were to be completed within 180 days of the request. Although the CG's evaluations were not integrated to coincide with time requirements of the CRA, they could have provided a basis for prompting review action under this mechanism. However, no monies were ever appropriated for the pilot program, and its authorization expired in January 2004.

Two bills have been introduced in the 108th Congress to address some of the deficiencies cited by critics of the review mechanism. H.R. 110 would require that all rules encompassed by the definition of rule in 5 U.S.C. § 551(4) cannot "have the force and effect of law" unless they are enacted into law by means of expedited consideration procedures established for each house by the proposal. The bill would apparently displace the current CRA mechanism. H.R. 3356 would amend the CRA by establishing a Joint Administrative Procedures Committee (JAPC) composed of 24 Members, 12 from each house, which would act as an oversight and screening body for Congress with respect to existing and proposed major rules. The bill also would provide for expedited consideration procedures for joint resolutions of disapproval for the House of Representatives comparable to those of the Senate; authorize the JACP, within 30 days after the required report to Congress was received, to report a committee resolution recommending that each standing committee with jurisdiction to which such report was provided report a joint resolution of disapproval; and would allow an agency to reissue or promulgate a new rule to replace a disapproved rule if it carried out the recommendation, if any, of the JACP in the report submitted by

the joint committee to the committees of jurisdiction recommending disapproval action. Neither of the bills has as yet received committee action.

Selected Source Reading

Cohen, Daniel and Peter L. Strauss. "Congressional Review of Agency Regulations." Administrative Law Review, vol. 49 (winter 1997), pp. 95-110.

CRS Report RL30116. Congressional Review of Agency Rulemaking: An Update and Assessment After Nullification of OSHA's Ergonomics Standard, by Morton Rosenberg.

Parks, Julie A. "Lessons in Politics: Initial Use of the Congressional Review Act." Administrative Law Review, vol. 55 (2003), pp. 187-210.

Pfohl, Peter A. "Congressional Review of Agency Rulemaking: The 104th Congress
and the Salvage Timber Directive." Journal of Law and Politics, vol. 14
(winter 1998), pp. 1-31.

Rosenberg, Morton. "Whatever Happened to Congressional Review of Agency Rulemaking?: A Brief Overview, Assessment, and Proposal for Reform." Administrative Law Review, vol. 51 (fall 1999), pp. 1051-1092.

Morton Rosenberg

E. Freedom of Information Act

Statutory Intent and History

The Freedom of Information (FOI) Act was originally adopted by Congress in 1966 (80 Stat. 250) and was codified in 1967 (81 Stat. 54; 5 U.S.C. § 552), when it also became operative law. As enacted, the FOI Act replaced the public information section of the Administrative Procedure Act (APA) (60 Stat. 237), which was found to be ineffective in providing the public with a means of access to unpublished records of federal departments and agencies. Subsection (a) of the FOI Act reiterated the requirements of the APA public information section that certain operational information — e.g., organization descriptions, delegations of final authority, and substantive rules of general policy — be published in the Federal Register.

Subsection (b) statutorily established a presumptive right of access by any person — individual or corporate, regardless of nationality — to identifiable, existing, unpublished records of federal departments and agencies without having to demonstrate a need or even a reason for such a request. Subsection (b)(1)-(9) lists nine categories of information that may be exempted from the rule of disclosure. The burden of proof for withholding material sought by the public was placed upon the government. Denials of requests could be appealed to the head of the agency holding the sought records, and ultimately pursued in federal district court. The law specifies the direct costs which agencies may recover when responding to requests for records.

The product of 11 years of investigation and deliberation in the House of Representatives and half as many years of consideration in the Senate, the FOI Act was legislated by Congress in the face of considerable opposition by the executive departments and agencies. This opposition produced a hostile environment for the development, passage, and early administration of the statute. As a result, portions of the law have been subjected to a high judicial gloss for reasons of both clarification and interpretation. To maintain faithful administration of the FOI Act and to preserve its purpose, Congress has found it necessary to conduct vigorous oversight of its implementation and, on four occasions, to amend its provisions.

Reporting in 1972 on the initial implementation of the statute, a House oversight committee concluded that the "efficient operation of the Freedom of Information Act has been hindered by 5 years of foot-dragging by the Federal bureaucracy ... of two administrations."[698] To remedy the situation, the following amendments to the FOI Act were approved in 1974 (88 Stat. 1561): (1) a request need only "reasonably describe" the material being sought; (2) only the direct costs of

[698] U.S. Congress, House Committee on Government Operations, Administration of the Freedom of Information Act, H.Rept. 92-1419, 92nd Cong., 2nd sess. (Washington: GPO, 1972), p. 8.

search for and duplication of requested records could be recovered by agencies; (3) documents could be furnished without charge or at reduced cost if doing so would be in the public interest; (4) a court might inspect records in camera when making a determination concerning their exemption from disclosure; (5) response to an initial request must be made within 10 working days, and to an administrative appeal request, within 20 working days; (6) responsive pleading to an FOI Act lawsuit must be made within 20 days; (7) complainants who substantially prevail in FOI Act lawsuits may be awarded court costs and attorney fees; and (8) any segregable portion of a requested record shall be disclosed after exempt parts are deleted. The amendments also expanded the definition of agency for FOI Act matters, required agencies to report annually on FOI Act administration and operations, and clarified two of the statute's exemptions.

In 1976, an FOI Act amendment clarifying the language of the third exemption to the rule of disclosure was attached to the Government in the Sunshine Act, another open government law (90 Stat. 1241, at 1247).

Additional amendments to the FOI Act were enacted in 1986 as a rider to an omnibus anti-drug abuse law (100 Stat. 3207-48). These modifications strengthened protections concerning law enforcement records and revised the fee and fee waiver provisions of the FOI Act. In this latter regard, separate fee arrangements were prescribed when records are requested (1) for commercial use; (2) by an educational or noncommercial scientific institution or a news media representative; and (3) by all others besides these types of requesters. The Office of Management and Budget was mandated to issue government-wide fee and fee waiver guidelines.[699]

The most recent amendment of the FOI Act occurred in 1996 during the closing weeks of the 104th Congress. These amendments (110 Stat. 3048), addressing shortcomings in administration as well as the new challenges posed by electronic forms and formats, inclusively defined covered records, required materials to be provided in the form or format requested, increased the initial response period from 10 to 20 days, encouraged agencies to maintain multitrack processing systems based upon the complexity of requests received, established expedited processing in cases where a "compelling need" is demonstrated, and modified agency reporting requirements, among other changes.

Major Provisions

Subsection (a) of the FOI Act requires that certain operational information — e.g., organization descriptions, delegations of final authority, and substantive rules of general policy — be published in the Federal Register.

[699] These guidelines are found in the Federal Register, vol. 52, Mar. 27, 1987, pp. 1001210020.

Subsection (b) prescribes a procedure whereby any person may request access to identifiable, existing, unpublished records of the federal departments and agencies. No need, 'or even a reason', for such a request must be demonstrated. The burden of proof for withholding material sought by the public is placed upon the government.

Although the statute specifies nine categories of information which may be protected from disclosure, these exemptions do not require agencies to withhold records, but merely permit access restriction. Allowance is made in the law for the exemption of (1) information properly classified for national defense or foreign policy purposes as secret under criteria established by an executive order; (2) information relating solely to agency internal personnel rules and practices; (3) data specifically excepted from disclosure by a statute which either requires that matters be withheld in a non-discretionary manner, or establishes particular criteria for withholding, or refers to particular types of matters to be withheld; (4) trade secrets and commercial or financial information obtained from a person and privileged or confidential; (5) inter- or intra-agency memoranda or letters which would not be available by law except to an agency in litigation; (6) personnel, medical, and similar files the disclosure of which would constitute an unwarranted invasion of personal privacy; (7) certain kinds of investigatory records compiled for law enforcement purposes; (8) certain information relating to the regulation of financial institutions; and (9) geological and geophysical information and data, including maps, concerning oil and gas wells. Disputes over the availability of agency records may ultimately be settled in court.

Agencies responding to FOI Act requests are permitted by the statute to charge fees for certain activities — document search, duplication, and review — depending on the type of requester: a commercial user; an educational or noncommercial scientific institution, whose purpose is scholarly or scientific research; a news media representative; or the general public. However, requested records may be furnished by an agency without any charge or at a reduced cost, according to the law, "if disclosure of the information is in the public interest because it is likely to contribute significantly to public understanding of the operations or activities of the government and is not primarily in the commercial interest of the requester." Both the Office of Management and Budget and the Department of Justice coordinate FOI Act policy and activities within the executive branch.

Discussion

The effective operation of the FOI Act owes much to diligent congressional oversight and corrective amendment of the statute. Initial agency hostility to the statute has subsided over the subsequent 35 years, but some agency administrative practices adverse to the effective operation of the law continue to be problematic. Ongoing judicial scrutiny and interpretation is closely watched by Congress for departures from congressional intent. Apart from these continuing challenges, information developments, such as more widespread government use

of e-mail, could prompt congressional review of whether additional FOI Act adjustments may be needed.

Selected Source Reading

Foerstel, Herbert N. Freedom of Information and the Right to Know. Westport, CT: Greenwood Press, 1999.

Hammitt, Harry A., David L. Sobel, and Mark S. Zaid, eds. Litigation Under the Federal Open Government Laws 2002. Washington: Electronic Privacy Information Center, 2002.

Congress. House. Committee on Government Operations [and] Senate Committee on the Judiciary. Freedom of Information Act and Amendments of 1974 (P.L. 93-502). Source Book: Legislative History, Texts, and Other Documents. Joint committee print. 94th Congress, 1st session. Washington: GPO, 1975.

Congress. House. Committee on Government Reform. A Citizen's Guide on Using the Freedom of Information Act and the Privacy Act of 1974 to Request Government Records, H.Rept. 108-172. 108th Congress, 1st session. Washington: GPO, 2003.

Congress. Senate Committee on the Judiciary. Freedom of Information Act Source Book: Legislative Materials, Cases, Articles. S.Doc. 93-82. 93rd Congress, 2nd session. Washington: GPO, 1974.

General Accounting Office. Information Management: Progress in Implementing the 1996 Electronic Freedom of Information Act Amendments. GAO-01-378. March 2001.

Harold C. Relyea

F. Privacy Act

Statutory Intent and History

In the Privacy Act of 1974 (5 U.S.C. § 552a) Congress mandated personal privacy protection in several regards concerning federal agency operations and practices. Its eclectic provisions can be traced to several contemporaneous events prompting congressional interest in securing personal privacy.

Since the years of the late 19th century, various developments — not the least of which the introduction of new, intrusive technologies — have contributed to more disparate understandings of the concept of privacy and infringements upon it. Congress made an initial effort at legislating a new kind of privacy protection in 1970 when enacting the Fair Credit Reporting Act regulating the collection and dissemination of personal information by consumer reporting entities (84 Stat. 1128; 15 U.S.C. § 1681 et seq.).

With the Crime Control Act of 1973, Congress prohibited federal personnel and state agencies receiving law enforcement assistance funds pursuant to the statute from making unauthorized disclosures of personally identifiable criminal history research or statistical information. It also permitted "an individual who believes that criminal history information concerning him contained in an automated system is inaccurate, incomplete, or maintained in violation of this [law] ... to review such information and to obtain a copy of it for the purpose of challenge or correction" (87 Stat. 197, at 215-216; 42 U.S.C. § 3789g).

That same year, the Advisory Committee on Automated Personal Data Systems, established by Secretary of Health, Education, and Welfare Elliot L. Richardson in early 1972, offered an important consideration. The panel's July 1973 final report recommended "the enactment of legislation establishing a Code of Fair Information Practice for all automated personal data systems." Such a code would: punish unfair information practice with civil and criminal penalties; provide injunctive relief to prevent violations of safeguard requirements; empower individuals to bring suits for unfair information practices to recover actual, liquidated, and punitive damages, in individual or class actions; and allow the recovery of reasonable attorneys' fees and other costs of litigation incurred by individuals who bring successful suits.[700]

Congressional efforts to legislate notice, access, and emendation arrangements for individuals concerning personally identifiable records maintained on these individuals by federal departments and agencies began in the House in June 1972, but did not extend beyond the subcommittee hearing stage during the 92nd

---

[700] U. S. Department of Health, Education, and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, Records, Computers, and the Rights of Citizens (Washington: GPO, 1973), pp. xxiii and 50.

Congress. However, a few days before these inaugural House hearings on legislation that would evolve into the Privacy Act, a burglary occurred at Democratic National Committee headquarters. It was the beginning of the Watergate incident, which would significantly affect attitudes toward privacy protection legislation and the leadership for such legislation.

Legislation leading to the enactment of the Privacy Act began in the House largely to create a procedure whereby individuals could learn if federal agencies maintained files on them, review the contents of the records in these files, correct inaccuracies they contained, and know how this information was being used and by whom. In the Senate, a privacy protection bill sponsored by Senator Sam Ervin Jr., initially sought largely to establish a Federal Privacy Board and to create standards and management systems for handling personally identifiable information in federal agencies, state and local governments, and other organizations. Other aspects of privacy policy were added to these bills as they moved through their respective houses of Congress, and then were reconciled in a somewhat unusual manner to create an amalgamated bill acceptable to the House, the Senate, and the President.

House hearings began in mid-February 1974 under Representative William S. Moorhead, chairman of the Subcommittee on Foreign Operations and Government Information of the Committee on Government Operations, and a principal manager of the legislation. The subcommittee held markup discussions in May, June, and July. These deliberations resulted in a clean bill (H.R. 16373), which was introduced by Representative Moorhead with 13 bipartisan co-sponsors in mid-August and favorably reported by the subcommittee without a dissenting vote. The Committee on Government Operations considered the legislation in mid-September, substituted revised text for the original language, and favorably reported it. President Gerald Ford, who had recently succeeded to the Oval Office after President Richard Nixon's early August resignation, endorsed the House bill in an October 9 statement.[701] The measure was considered by the House on November 20 and 21, and approved, with amendments, on a 353-1 yea-and-nay vote.[702]

A somewhat different counterpart privacy proposal emerged in the Senate. Senator Ervin introduced his bill (S. 3418) on May 1, 1974, with bipartisan cosponsorship. Hearings on this and related legislation occurred in June. During June, July, and August, staff of the Senate Committee on Government Operations, its Ad Hoc Subcommittee on Privacy and Information Systems, and the Subcommittee on Constitutional Rights of the Committee on the Judiciary —

---

[701] U.S. Office of the President, Public Papers of the Presidents of the United States: Gerald R. Ford, 1974, Book I (Washington: GPO, 1976), pp. 243-244.

[702] Congressional Record, vol. 120, Nov. 20, 1974, pp. 36643-36660; ibid., Nov. 21, 1974, pp. 36955-36977.

all panels chaired by Senator Ervin — further refined the language of the bill. In a mid-August committee markup, a staff-developed version of the measure was amended and favorably reported to the Senate.

The new text of the bill would have established the Privacy Protection Commission, composed of five members appointed by the President from private life and subject to Senate approval. The commission would have been responsible for compiling and publishing an annual directory of information systems subject to the provisions of the bill, enforcing the legislation, and developing model guidelines for its implementation, including the conduct of research in this regard. The bill also would have established federal agency standards and management systems for handling information relating to individuals. These included fair information practice principles, disclosure standards, mailing list restrictions, and civil and criminal penalties.

On November 21, the Senate considered the Ervin legislation; amendments developed by committee staff and the Office of Management and Budget (OMB) were adopted, and the resulting version of the legislation was approved.[703] The following day, the Senate took up the House counterpart bill, struck its language and substituted in lieu thereof the language of the Ervin bill, and approved the amended version of the House bill.[704]

With only a few weeks remaining before the 93rd Congress would adjourn sine die, House and Senate managers found they had very little time to reconcile the two differing bills. There was, however, strong desire for the passage of such legislation, not only as a so-called Watergate reform, but also as a tribute and memorial to Senator Ervin, who was retiring from congressional service. Consequently, Representative Moorhead and Senator Ervin, with the concurrence of their respective committees, agreed to the rare arrangement of having their committee staffs negotiate a mutually agreeable legislative measure. After this effort reduced 108 substantive differences to eight, the leaders of the respective House and Senate committees brought those to resolution.[705] In lieu of a conference committee report, a staff analysis of the compromise legislation was produced.[706] The major concession was the relegation of the enforcement commission to the status of a temporary national study commission. Its oversight responsibilities were vested in OMB, but without enforcement authority.

---

[703] Congressional Record, vol. 120, Nov. 21, 1974, pp. 36882-36921.

[704] Ibid., Nov. 22, 1974, pp. 37064-37069.

[705] Ibid., Dec. 17, 1974, p. 40400.

[706] See ibid., pp. 40405-40408.

On December 11, the House adopted the Senate bill after striking its original language and inserting in lieu thereof provisions of its own bill.[707] The Senate concurred in the House amendment by passing its own amendment on a 77-8 vote on December 17, clearing the measure for further House action.[708] The following day, the House agreed to the Senate amendments with an amendment of its own,[709] and the Senate concurred with the House amendments the same day, clearing the measure for the President's signature.[710] The Privacy Act was signed into law by President Ford on December 31, 1974 (88 Stat. 1896; 5 U.S.C. § 552a). In his signing statement, the President said the new law "signified an historic beginning by codifying fundamental principles to safeguard personal privacy in the collection and handling of recorded personal information by federal agencies."[711]

Major Provisions

The Privacy Act provides privacy protection in several ways. First, it sustains some traditional major privacy principles. For example, an agency shall "maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity" (5 U.S.C. § 552(e)(7)).

Second, similar to the Fair Credit Reporting Act, the Privacy Act provides an individual who is a citizen of the United States, or an alien lawfully admitted for permanent residence, with access and emendation arrangements for records maintained on him or her by most, but not all, federal agencies. General exemptions in this regard are provided for systems of records maintained by the Central Intelligence Agency and federal criminal law enforcement agencies.

Third, the statute embodies a number of principles of fair information practice. For example, it sets certain conditions concerning the disclosure of personally identifiable information; prescribes requirements for the accounting of certain disclosures of such information; requires agencies to "collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs"; requires agencies to specify

---

[707] Ibid., Dec. 11, 1974, pp. 39200-39204.

[708] Ibid., Dec. 17, 1974, pp. 40397-40413.

[709] Ibid., Dec. 18, 1974, pp. 40879-40886.

[710] Ibid., pp. 40730-40731.

[711] Public Papers of the Presidents of the United States: Gerald R. Ford, 1975, Book I, pp. 1-2.

their authority and purposes for collecting personally identifiable information from an individual; requires agencies to "maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination"; and provides civil and criminal enforcement arrangements.

Discussion

Since its enactment, the Privacy Act has been amended on five occasions. In 1982, the Debt Collection Act added a new exception to the disclosure prohibition for disclosures made to consumer credit reporting agencies (96 Stat. 1749, adding 5 U.S.C. § 552a(b)(12)). That same year, the Congressional Reports Elimination Act changed the annual report requirement of the Privacy Act and modified the provision for publication of agency systems of records (96 Stat. 1819, at 1821-1822, modifying 5 U.S.C. § 552a(e)(4) and (p)). In 1984, the Central Intelligence Agency Information Act resolved a long-standing controversy by specifying that the Privacy Act is not authority "to withhold from an individual any record which is otherwise accessible to the individual under the provisions of" the Freedom of Information Act (96 Stat. 2209, at 2211-2212, adding 5 U.S.C. § 552a(q)(2)). Amendments in 1988 (102 Stat. 2507, adding 5 U.S.C. § 552a(o),(p),(q), and (u), and amending 5 U.S.C. § 552a(a), (e), and (v)) and 1990 (104 Stat. 1388-334, modifying 5 U.S.C. § 552a(p)) established new procedures and data protection boards to ensure privacy, integrity, and verification of data disclosed for computer matching.

Perhaps the facet of the Privacy Act that has been the most successful is its access procedure. The volume of access requests by record subjects has grown steadily, for the most part, since the Privacy Act was first implemented. It is, however, about a third of the access request volume of the Freedom of Information Act. Moreover, it appears that the total denial caseload is small in proportion to request volume.

Similarly, the volume of requests to amend personal records is also steadily growing, though it is not nearly so great as the volume of access requests, and the total denial caseload is small in proportion to the amendment request volume.

In a June 2003 report, the General Accounting Office urged improved leadership and guidance by the Office of Management and Budget to improve agency compliance with the Privacy Act. Around this same time, as public revelations about the efforts of some agencies to engage in data mining for homeland security purposes — searching private sector databases for personal information — became known, some urged amendment of the Privacy Act to clarify its scope regarding such practices.

Selected Source Reading

Hammitt, Harry A., David L. Sobel, and Mark S. Zaid, eds. Litigation Under the Federal Open Government Laws 2002. Washington: Electronic Privacy Information Center, 2002.

Congress. House. Committee on Government Reform. A Citizen's Guide on Using the Freedom of Information Act and the Privacy Act of 1974 to Request Government Records. H.Rept. 108-172. 108th Congress, 1st session. Washington: GPO, 2003.

Congress. Senate Committee on Government Operations [and] House Committee on Government Operations. Legislative History of the Privacy Act of 1974: S. 3418 (Public Law 93-579), Source Book on Privacy. Joint committee print. 94th Congress, 2nd session. Washington: GPO, 1976.

General Accounting Office. Privacy Act: OMB Leadership Needed to Improve Agency Compliance. GAO-03-304. June 2003.

Privacy Protection Study Commission. Personal Privacy in an Information Society. Washington: GPO, 1977.

_____. The Privacy Act of 1974: An Assessment, Appendix 4. Washington: GPO, 1977.

Harold C. Relyea

G. Federal Advisory Committee Act

Statutory Intent and History

Congress formally acknowledged the merits of using advisory committees to obtain expert views drawn from business, academic, government, and other interests when it enacted the Federal Advisory Committee Act (FACA) in 1972 (5 U.S.C. Appendix; 86 Stat. 700).

The legislative history pertaining to FACA reveals that Congress had two major concerns about advisory committees before 1972. The first concern was that the public perceived many advisory committees as duplicative and inefficient, and otherwise lacking adequate controls or oversight. The second concern was the widespread belief that advisory committees did not adequately represent the public interest, and that committee meetings were too often closed to the public.

Congressional enactment of FACA established the first requirements for the management and oversight of federal advisory committees to ensure impartial and relevant expertise. As required by FACA, the General Services Administration (GSA) administers and provides management guidelines for advisory committees. GSA also submits an annual report to the President and Congress, based on the information provided by the federal agencies concerning the meetings, costs, and membership of advisory committees. During FY2003, GSA reported a total of 953 advisory committees, with 31,385 individuals serving as members during the year. Related expenditures of $282.5 million were used in FY2003 to provide member compensation, travel and per diem expenses, and other administrative costs associated with advisory committees. On March 14, 2000, GSA announced the elimination of its annual report on advisory committees, relying instead on its website to make available the detailed reports covering each committee's activities during the fiscal year.[712] GSA also issues an annual summary report for Congress pertaining to advisory committee management and performance.

Major Provisions

FACA requires that the advice provided by advisory committees be objective and accessible to the public. Each advisory committee meeting is presumptively open to the public, with certain exceptions. Adequate notice of meetings must be published in advance in the Federal Register. Subject to the requirements of the Freedom of Information Act, all papers, records, and minutes of meetings must be made available for public inspection.

FACA contains guidelines for membership, mandating that any legislation establishing an advisory committee be "fairly balanced in terms of the points of

[712] The GSA website is available at [http://fido.gov/facadatabase], visited Dec. 11, 2003.

view represented and the functions to be performed," and that the committee's recommendations not be inappropriately influenced by the appointing authorityor by any special interest.

Each advisory committee must file a charter containing its mandate and duties, frequency of meetings, membership, and the agency to which, or official to whom, the committee reports. The act requires the Library of Congress to maintain a depository of committee reports, papers, and charters. Pursuant to FACA, each advisory committee goes out of existence after two years unless its charter is renewed or is otherwise prescribed by statute.

Discussion

Since the enactment of FACA in 1972, congressional oversight hearings have revealed that, while the goals of FACA are still relevant, some of its provisions have occasionally needed clarification. From 1983 through 1989, legislation was introduced in the Senate to strengthen FACA's management controls, as well as to establish new ethical, financial, and conflict of interest disclosure requirements for committee members.[713] These proposed amendments were never enacted, in part due to the stringent disclosure requirements required of potential committee members. In 1997, FACA was amended to provide for increased public participation in activities by committees created by the National Academy of Sciences and the National Academy of Public Administration in support of executive branch decision making processes.[714]

Because federal agencies needed clarification of FACA's statutory requirements, GSA began issuing administrative and interpretive guidelines in 1983 pertaining to the implementation of FACA. These final rules provide guidance to agency committee management officers (CMOs) for the establishment and management of advisory committees. On January 14, 2000, GSA issued a proposed rule for revised management guidelines in the Federal Register.[715] The following year, on July 19, 2001, GSA issued its final rule providing additional guidance to CMOs based on statutory provisions and internal agency procedures.[716]

In order to curtail the proliferation of advisory committees, President William Clinton issued E.O. 12838 in 1993, requiring the elimination of one-third of the

---

[713] S. 1641 was introduced on July 19, 1983, and S. 2127 was introduced on Nov. 17, 1983; S. 2721 was introduced on Aug. 10, 1988, and S. 444 was introduced on Feb.23, 1989.

[714] 111 Stat. 2689.

[715] 65 Federal Register 2504.

[716] 41 C.F.R. § 102-3 (2003, pp. 11-44).

advisory committees not created by statute.[717] In addition, executive branch departments and agencies were proscribed from administratively creating new advisory committees without the approval of the Director of the Office and Management and Budget (OMB). The following year, as part of the National Performance Review, Vice President Albert Gore issued a memorandum indicating each agency should reduce advisory committee costs by 5%. The memorandum also stated that President Clinton would not support legislation establishing new advisory committees or exemptions from FACA.[718] On October 5, 1994, OMB issued Circular No. A-135, entitled "Management of Federal Advisory Committees." This circular requires OMB and GSA to monitor agency compliance with E.O. 12838 to reduce the number of advisory committees.

Selected Source Reading

CRS Report RL30260, Federal Advisory Committees: A Primer, by Stephanie Smith.

Congress, House Committee on Government Reform and Oversight, Subcommittee on Government Management, Information, and Technology, Oversight of the Federal Advisory Committee Act, hearings, July 14, 1998, 105th Cong., 2nd sess. Washington: GPO, 1999.

General Accounting Office, Federal Advisory Committee Act: Views of Committee Members and Agencies on Federal Advisory Committee Issues, GAO Report GAO/GGD-98-147. Washington: GAO, 1998.

U.S. General Accounting Office, Federal Research: The National Academy of Sciences and the Federal Advisory Committee Act, GAO Report GAO/RCED99-17. Washington: GAO, 1988.

Stephanie Smith

---

[717] 3 C.F.R., 1994 Comp., p. 590.

[718] U.S. Office of the Vice President, "Memorandum for the Heads of Executive Departments and Agencies on the Management of Federal Advisory Committees," June 28, 1994, Annual Report of the President on Federal Advisory Committees (Washington: GPO, 1995), p. A7.

H. Government in the Sunshine Act

Statutory Intent and History

The Government in the Sunshine Act (90 Stat. 1241; 5 U.S.C. § 552b) was initially enacted in 1976. It requires collegially headed federal executive agencies whose members are appointed by the President with the advice and consent of the Senate to hold certain meetings in public. The act applies to meetings during which deliberations determine, or result in the joint conduct or disposition of, official agency business. The act applies to more than 45 federal collegial bodies, consisting primarily of independent regulatory boards and commissions having from three to seven members. The statute specifies 10 exceptions to its rule of openness that may be invoked by the agencies. Any doubt as to whether a meeting should be open or closed, however, is to be resolved in favor of an open meeting, according to the act's legislative history. Decisions to close a meeting are subject to judicial review.

Major Provisions

The major provisions of the Sunshine Act include (1) a presumption of open meetings; (2) public notice of an agency meeting, indicating the time, location, subject of the meeting, whether the meeting is open or closed, and the name and telephone number of the official designated to respond to requests for information about the meeting; (3) 10 exemptions by which an agency may close a portion or all of a meeting and withhold information; (4) procedures an agency is to follow when closing a meeting, which include a majority vote of the members and certification by the general counsel that the meeting may properly be closed; and (5) judicial review of an agency's action to close a meeting.

A meeting may be closed if it involves: (1) national security matters that are specifically authorized by an executive order to be protected and are properly classified; (2) internal personnel rules and practices; (3) matters specifically exempted from disclosure by statute; (4) trade secrets and commercial or financial information obtained from a person and privileged or confidential; (5) formal censure or accusation of a crime; (6) clearly unwarranted invasion of personal privacy; (7) law enforcement investigatory records or information; (8) information contained in, or related to, reports used by agencies responsible for the regulation or supervision of financial institutions; (9) information whose premature disclosure would: (a) lead to financial speculation or significantly endanger a financial institution; or (b) significantly frustrate a proposed agency action; or (10) issuance of a subpoena or other related judicial matter.

Discussion

The consensus of observers is that the act has been only partially successful in opening bureaucratic decision making processes to public scrutiny. Although federal agencies now routinely follow the Sunshine Act's requirements, empirical research suggests that, after the law was passed, agency practices changed in

ways that may have served to circumvent openness. The number of meetings, as well as the number of open meetings or partly open meetings, declined steadily from 1979 to 1984 as agencies resorted to wider use of the exemption provisions. In addition, some agencies used notation voting, which permitted members to vote sequentially on paper on the basis of circulated written materials, thereby making formal meetings unnecessary.[719]

The implementation of the Sunshine Act has been characterized by difficulties in finding the proper balance between the value of unfettered public access, on one hand, and candid agency deliberations, on the other.[720] The resulting tension is evident in the disagreements over two issues: (1) the definition of what constitutes a "meeting," for purposes of the act; and (2) whether the act has diminished the collegial nature of decision making, thereby affecting the quality of agency decisions.

Under the act, a meeting is defined as "the deliberations of at least the number of individual agency members required to take action on behalf of the agency where such deliberations determine or result in the joint conduct or disposition of official agency business."[721] Deciding when a deliberation determines or results in agency action, however, has proven to be difficult.

Two opposing views have dominated the discussion regarding the definition of a meeting. Adherents of a broad definition hold that a meeting encompasses every stage of the decision making process, including the early collective inquiry stage when members hold informal discussions and explore various positions. Supporters of a narrower view, in contrast, hold that a meeting encompasses only the more advanced stage of the decision making process, when members focus on a specific proposal or proposals.[722]

The Supreme Court supported the narrower definition in 1984, when it held that under the act, a meeting did not include preliminary discussions among agency

---

[719] See U.S. Congress, Senate Committee on Governmental Affairs, Government in the Sunshine Act: History and Recent Issues, committee print, 101st Cong., 1st sess. (Washington: GPO, 1989), pp. 58-98.

[720] Administrative Conference of the United States, "Report & Recommendation by the Special Committee to Review the Government in the Sunshine Act," Administrative Law Review, vol. 49 (spring 1997), p. 422.

[721] 5 U.S.C. § 552b(a)(2).

[722] For a further development of these views, see David A. Barrett, "Facilitating Government Decision Making: Distinguishing Between Meetings and Nonmeetings Under the Federal Sunshine Act," Texas Law Review, vol. 66, May 1988, pp. 1195-1228.

officials.[723] The Court ruled that consultative process sessions need not be public, because the "statutory language contemplates discussions that 'effectively predetermine official actions.'" It held that, in order to fall under the meeting definition, such discussions must be "'sufficiently focused on discrete proposals or issues as to cause or be likely to cause the individual participating members to form reasonably firm positions regarding matters pending or likely to arise before the agency.'"

In the second area of contention, some research has suggested that open meeting requirements may have suppressed the spirit of candor in meeting discussions and thereby reduced collegiality in organizations subject to the act's provisions. A study of this issue involving multi-member agency officials revealed that many are reluctant to discuss substantive issues at open meetings.[724] Those seeking to amend the act believe that collegial decisions should lead to better, more informed decision making. This goal, they argue, is defeated by the need to open most meetings to the public, which they believe prevents the type of extensive and consequential interaction among members that should be the end product of collegial decision making. To support this view, they cite data consisting of members' recollections of how decisions were made before the act was implemented. Their proposed solution is to amend the act to provide for a limited pilot project that would give agencies greater leeway to close a meeting, provided that within five days of the meeting, a "detailed summary" would be made available to the public. If such a project proved successful, Congress could then make permanent changes in the statute.[725]

Several arguments against amending the act have also been advanced. Some researchers question the view that collegial decision making prior to the implementation of the act was more deliberative and meaningful than it has been since then. They assert that the earlier collegial decision making model was only partially realized. They maintain that decisions from this era "frequently reflected more the influence of staff or of chairpersons in association with staff than a true amalgamation of member views informed by staff expertise."[726] Furthermore, the evidence suggests that "members are inclined to prepare more

---

[723] Federal Communications Commission v. ITT World Communications, 466 U.S. 463 (1984).

[724] David M. Welborn, William Lyons, and Larry W. Thomas, "Implementation and Effects of the Federal Government in the Sunshine Act," Administrative Conference of the United States: Recommendations and Reports 1984 (Washington: GPO, 1985), pp. 199-261.

[725] Administrative Conference of the United States, "Report & Recommendation by the Special Committee to Review the Government in the Sunshine Act," pp. 421-428.

[726] David M. Welborn, William Lyons, and Larry W. Thomas, "The Federal Government in the Sunshine Act and Agency Decision Making," Administration and Society, vol. 20, Feb. 1989, p. 470.

thoroughly for open meetings than for closed ones."[727] Consequently, it could be argued that members are better informed in their decision making than they were prior to the act. Finally, opponents of amending the Sunshine Act have sometimes suggested that it is incumbent upon members of the multi-member agencies to shed their reluctance to deliberate more meaningfully in public meetings.[728]

Selected Source Reading

Barrett, David A. "Facilitating Government Decision Making: Distinguishing Between Meetings and Nonmeetings Under the Federal Sunshine Act." Texas Law Review, vol. 66 (May 1988), pp. 1195-1228.

Berg, Richard K. and Stephen H. Klitzman. An Interpretive Guide to the Government in the Sunshine Act. Washington: GPO, 1978. (New edition expected 2004.)

May, Randolph. "Reforming the Sunshine Act." Administrative Law Review, vol. 49 (spring 1997), pp. 415-428.

Congress. Senate. Committee on Governmental Affairs. Government in the Sunshine Act: History and Recent Issues. Committee print. 101st Congress, 1st session. S.Prt. 101-54. Washington: GPO, 1989.

Congress. Senate. Committee on Government Operations and House Committee on Government Operations. Government in the Sunshine Act — S. 5 (Public Law 94-409): Source Book: Legislative History, Texts, and Other Documents. Joint committee print. 94th Congress, 2nd session. Washington: GPO, 1976.

Henry B. Hogue

---

[727] Ibid., p. 472.

[728] This position is ascribed to representatives of the press by Randolph May in "Reforming the Sunshine Act," Administrative Law Review, vol. 49 (spring 1997), p. 418.

I. Paperwork Reduction Act of 1995

Statutory Intent and History

Replacing the ineffective Federal Reports Act of 1942 (56 Stat. 1078), the Paperwork Reduction Act of 1980 (94 Stat. 2812; 44 U.S.C. § 3501) was enacted largely to relieve the public of the mounting information collection and reporting requirements of the federal government. It also promoted coordinated information management activities on a government-wide basis by the director of the Office of Management and Budget (OMB), and prescribed information management responsibilities for the executive agencies. Realizing that the provisions of the Federal Reports Act were inadequate to control the proliferation of required paperwork, Congress had established the Commission on Federal Paperwork, a temporary national study panel, in 1974 (88 Stat. 1789). The 1980 statute implemented many of the commission's recommendations and reflected a congressional desire to define more clearly the oversight responsibilities of OMB regarding federal information collection and reporting requirements. To assist the OMB Director, the statute established the Office of Information and Regulatory Affairs (OIRA) within OMB, and authorized its administrator to develop and administer uniform information policies in order to ensure the availability and accuracy of agency data collection.

Although OIRA's original authorization expired in 1983, the office was funded on an annual basis from OMB's general appropriations until passage of the Paperwork Reduction Reauthorization Act in 1986 (100 Stat. 3341). This legislation approved funding for OIRA through FY1989, and strengthened congressional oversight of OIRA by requiring Senate confirmation of its administrator. Also, the management focus of the act was sharpened with the 1986 amendments, which refined the concept of "information resources management" (IRM), which is "the planning, budgeting, organizing, directing, training, promoting, controlling, and management activities associated with the burden, collection, creation, use, and dissemination of information by agencies, and includes the management of information and related resources such as automatic data processing equipment." This key term and its subset concepts would receive further definition and explanation in 1995, making IRM a tool for managing the contribution of information activities to program performance, and for managing related resources, such as personnel, equipment, funds, and technology.

Largely due to continued failure to reach an agreement concerning OIRA's regulatory review role, legislative attempts to reauthorize OIRA during the 101st and the 102nd Congresses were unsuccessful. During the 103rd Congress, a reauthorization measure was passed by the Senate by unanimous vote, but the House did not have time to complete action on such legislation. In 1995, as part of the House Republican Contract with America, a revised Paperwork Reduction Act (PRA) was enacted to reauthorize OIRA for six years (109 Stat. 163; 44 U.S.C. § 3501).

Major Provisions

The PRA of 1995 reaffirms the principles of the original 1980 act by reducing the information collection burden on the public, and providing more efficient management of information resources by federal agencies. The statute set 10% paperwork reduction goals for the first two years of OIRA's authorization, and a 5% reduction for the remaining four years. OIRA is required to develop and implement government-wide guidelines for the collection, dissemination, and processing of federal information. The objective of minimizing the paperwork burden for individuals and small businesses is extended explicitly to educational and nonprofit institutions, federal contractors, and tribal governments. The authority and functions of OIRA are revised, specifying information dissemination and related agency oversight responsibilities. Another provision strengthens the public's rights if an agency should require information requests that are not in compliance with the provisions of the PRA.

The federal agencies are required to evaluate proposed collections of information, manage information resources to reduce information collection burdens on the public, and ensure that the public has timely and equitable access to information products and services. Except where specifically authorized by statute, the agencies are prohibited from establishing exclusive, restricted, or other distribution arrangements that interfere with timely and equitable public availability of public information; restricting or regulating the use, resale, or redissemination of public information by the public; charging fees or royalties for resale or redissemination of public information; or establishing user fees that exceed the cost of dissemination. Actions that the agencies must take with respect to information technology are specified, and the Federal Information Locator System is replaced with an agency-based electronic Government Information Locator Service to identify the major information systems, holdings, and dissemination products of each agency.

Discussion

Since 1980, OIRA's implementation of the PRA has been criticized by Congress, the General Accounting Office (GAO), and the business community. An early controversy surrounded OMB's decision to assign OIRA primary responsibility for regulatory reforms and other regulatory functions not associated with OIRA's paperwork responsibilities. In 1983, GAO concluded that only limited progress had been made by OMB in information resources management, and recommended that Congress amend the statute to prohibit OIRA from performing nonrelated duties such as regulatory review.[729]

[729] See U.S. General Accounting Office, Implementing the Paperwork Reduction Act: Some Progress, But Many Problems Remain, GAO/GGD-83-35, Apr. 20, 1983.

The PRA gives OMB significant authority to conduct reviews of federal agency paperwork requirements in proposed rules. Critics of OMB's paperwork clearance powers maintain that OMB has too much discretion in determining agency record-keeping requirements, and has used its authority in a selective and political manner to control the government's information collection activities. Many also believe that its review of rules and reports provides OMB with excessive control of the entire regulatory process.

Even though the PRA stresses the importance of a government-wide information policy, congressional hearings and GAO studies have consistently faulted OMB for neglecting this important issue, while concentrating on paperwork control and regulatory review functions. As federal agencies have made greater use of electronic information technology, criticism has arisen that OIRA focuses on the collection and dissemination of paper documents, while failing to develop policies concerning the use of electronic formats.

In response to the statutory requirement of the PRA that OMB develop and implement uniform and consistent information resources management policy, OMB issued Circular No. A-130, Management of Federal Information Resources, in 1985. The circular set forth government-wide guidelines for the collection, dissemination, and processing of federal information systems and technology. Subsequently, OMB published a series of notices in the Federal Register inviting public comment on proposed revisions of the circular. In July 1994, OMB issued a final revision of A130 to address agencies' internal management practices for information systems and information technology.[730]

Two major segments of the National Defense Authorization Act for FY1996 (110 Stat. 186) contained provisions either amending or glossing the PRA. Subsequently denominated the Clinger-Cohen Act (110 Stat. 3009-393), these segments transfer the authority for information technology acquisitions from the General Services Administration to OMB. The Director of OMB is assigned new duties for coordinating the purchase of information systems with OIRA and the Office of Federal Procurement Policy. As part of the budget process, OMB is required to analyze the costs and risks associated with capital investments for the purchase of federal information acquisitions. The position of Chief Information Officer (CIO) is established within each agency to coordinate and monitor the implementation of information technology programs.

More recent amendments to the PRA were made by the Government Paperwork Elimination Act of 1998 (112 Stat. 2681-749). This statute makes the Director of OMB responsible for providing government-wide direction and oversight regarding "the acquisition and use of information technology, including

---

[730] U.S. Office of Management and Budget, "Management of Federal Information Resources, OMB Circular No. A-130, July 25, 1994," Federal Register, vol. 59, July 25, 1994, pp. 37906-37928.

alternative information technologies that provide for electronic submission, maintenance, or disclosure of information as a substitute for paper and for the use and acceptance of electronic signatures." In fulfilling this responsibility, the director, in consultation with the National Telecommunications and Information Administration (NTIA) of the Department of Commerce, is tasked with developing, in accordance with prescribed requirements, procedures for the use and acceptance of electronic signatures by the executive departments and agencies. A five-year deadline is prescribed for the agencies to implement these procedures.

The Director of OMB is also tasked by the statute to "develop procedures to permit private employers to store and file electronically with Executive agencies forms containing information pertaining to the employees of such employers." In addition, the director, in cooperation with NTIA, is to conduct an ongoing study of the use of electronic signatures under the new law, with attention to paperwork reduction and electronic commerce, individual privacy, and the security and authenticity of transactions. The results of this study are to be reported periodically to Congress.

Finally, electronic records submitted or maintained in accordance with the statute's procedures, "or electronic signatures or other forms of electronic authentication used in accordance with such procedures, shall not be denied legal effect, validity, or enforceability because such records are in electronic form." The act further specifies: "Except as provided by law, information collected in the provision of electronic signature services for communications with an executive agency ... shall only be used or disclosed by persons who obtain, collect, or maintain such information as a business or government practice, for the purpose of facilitating such communications, or with the prior affirmative consent of the person about whom the information pertains."

The PRA authorization of appropriations for OIRA expired at the end of FY2001. When Congress returns to the PRA to reauthorize OIRA appropriations, it will have an opportunity to consider several prevailing issues which may be addressed through amendment or extension of the statute. For instance, critics continue to assert that the act's current provisions do not go far enough to minimize costly reporting burdens for small businesses, educational institutions, and state and local governments. Other issues of concern to some are agency website management and accountability, as well as various aspects of government e-mail management.

<u>Selected Source Reading</u>

Cole, Roland J. and Paul Sommers. "Government Paperwork: Not an Easy Villain
After All." Journal of Policy Analysis and Management, vol. 1 (summer 1982), pp. 554-561.

Plocher, David. “The Paperwork Reduction Act of 1995: A Second Chance for Information Resources Management.” Government Information Quarterly, vol. 13, 1996, pp. 35-50.

U.S. General Accounting Office. Paperwork Reduction Act: Burden Increases and Violations Persist. GAO-02-598T. April 11, 2002.

——. Paperwork Reduction Act: Record Increase in Agencies’ Burden Estimates. GAO-03-691T. April 11, 2003.

CRS Report RL30590, Paperwork Reduction Act Reauthorization and Government Information Management Issues, by Harold C. Relyea.

Harold C. Relyea

J. Regulatory Flexibility Act of 1980

Statutory Intent and History

The Regulatory Flexibility Act (RFA) of 1980 (94 Stat. 1164; 5 U.S.C. §§ 601612) was enacted in response to concerns raised during a White House conference on small business about the differential impact of federal regulations on small business. The RFA requires federal agencies to assess the impact of their forthcoming regulations on small entities, which the act defines as including small businesses, small governmental jurisdictions, and certain small not-for-profit organizations. Under the RFA, federal agencies must prepare a regulatory flexibility analysis at the time that either proposed or certain final rules are issued. The act requires the analysis to describe (1) the reasons why the regulatory action is being considered; (2) the small entities to which the proposed rule will apply and, where feasible, an estimate of their number; (3) the projected reporting, recordkeeping, and other compliance requirements of the proposed rule; and (4) any significant alternatives to the rule that would accomplish the statutory objectives while minimizing the impact on small entities.

A regulatory flexibility analysis is not, however, required if the head of the agency issuing the rule certifies that it will not have a "significant economic impact on a substantial number of small entities." The RFA does not define the terms significant economic impact or substantial number of small entities, thereby giving federal agencies substantial discretion regarding when the act's analytical requirements are triggered. Also, the RFA's analytical requirements do not apply to any final rule for which the agency is not required to publish a proposed rule. Although the original RFA did not permit judicial review of agencies' actions under the act, amendments to the act in 1996, as part of the Small Business Regulatory Enforcement Fairness Act (SBREFA; 110 Stat. 857), permitted judicial review regarding, among other things, agencies' regulatory flexibility analyses for final rules and any certifications that their rules will not have a significant impact on small entities.

In addition, the RFA requires agencies to publish a "regulatory flexibility agenda" in the Federal Register each October and April listing regulations that the agency expects to propose or promulgate and which are likely to have a significant economic impact on a substantial number of small entities. The act also requires agencies to review final rules with a significant impact within 10 years of their promulgation to determine whether they should be amended or rescinded. Another section of the statute requires the chief counsel of the Small Business Administration's (SBA's) Office of Advocacy to monitor and report at least annually on agencies' compliance with the act.

The RFA also requires agencies to ensure that small entities have an opportunity to participate in the rulemaking process, and the 1996 amendments to the act in SBREFA put in place special requirements for proposed rules issued by the Environmental Protection Agency (EPA) and the Occupational Safety and Health Administration (OSHA). EPA and OSHA are required to convene "advocacy

review panels" before publishing a regulatory flexibility analysis for a proposed rule. The review panel must consist of full-time federal employees from the rulemaking agency, the Office of Management and Budget, and SBA's chief counsel for advocacy, and the panel must collect advice and recommendations from representatives of affected small entities about the potential impact of the draft rule.

Major Provisions

The major provisions of the RFA, as amended: (1) require federal agencies to publish in the Federal Register each October and April a list of forthcoming rules that are likely to have a significant economic impact on a substantial number of small entities; (2) require federal agencies to prepare a regulatory flexibility analysis for any covered proposed or final rule that the agency concludes is likely to have a significant economic impact on a substantial number of small entities; (3) require the regulatory flexibility analyses to have certain elements; (4) require EPA and OSHA to convene an advocacy review panel before publishing any proposed rule likely to have a significant economic impact on a substantial number of small entities; (5) require the chief counsel in the Advocacy Office in SBA to monitor agencies' compliance with the act and prepare an annual report; (6) require agencies to review their final rules with a significant impact within 10 years of their promulgation to determine whether they should be amended or rescinded; and (7) permit judicial review of agencies' regulatory flexibility analyses and determinations that their rules do not have a significant economic impact on a substantial number of small entities.

Discussion

The SBA chief counsel for advocacy's reports on the RFA generally indicate that compliance with the act has been uneven. GAO has also repeatedly examined the implementation of the act, and a recurring theme in GAO's reports is the varying interpretation of the RFA's requirements by federal agencies. Agencies differ dramatically regarding what constitutes a "significant" economic impact and a "substantial" number of small entities. They also differ on what rules they are required to review within 10 years of their issuance — those that had a significant impact at the time they were issued or those that currently have that impact. In 2001, GAO testified that the promise of the RFA may never be realized until Congress or some other entity defines what a significant economic impact and a substantial number of small entities mean in a rulemaking setting.

The 1996 amendments to the act providing for judicial review and advocacy review panels for EPA and OSHA rules have proven effective. The SBA chief counsel for Advocacy's annual report on the RFA for FY2003 said that judicial review "has encouraged agencies to increase their compliance with the requirements of the RFA." Advocacy review panels have permitted small entities to participate early in the rulemaking process — before proposed rules are written and agencies positions become more fixed.

Selected Source Reading

Freedman, Doris S., Barney Singer, and Frank S. Swain. The Regulatory Flexibility
Act: Orienting Federal Regulation to Small Business. Dickinson Law Review, vol. 93 (1989), pp. 439-478.

Lubbers, Jeffery S. A Guide to Federal Agency Rulemaking, 3rd ed. Chicago: American Bar Association Publishing, 1998.

Administrative Conference of the United States. A Critical Guide to the Regulatory Flexibility Act, Recommendations and Reports. [Paul R. Verkuil.] Washington: GPO, 1981, pp. 203-302.

General Accounting Office. Regulatory Flexibility Act: Agencies' Interpretations of Review Requirements Vary. GAO/GGD-99-55. April 1999.

——. Regulatory Flexibility Act: Key Terms Still Need to Be Clarified. GAO-01669T. April 24, 2001.

U.S. Small Business Administration, A Guide to the Regulatory Flexibility Act. Washington: SBA, 1996.

Curtis W. Copeland

K. Negotiated Rulemaking Act

Statutory Intent and History

The Negotiated Rulemaking Act of 1990, as amended and permanently authorized in 1996 (110 Stat. 3870; 5 U.S.C. §§ 561-570a), seeks to overcome what some observers describe as an adversarial relationship between agencies and affected interest groups that often accompanies the federal rulemaking process. The concept of negotiated rulemaking (sometimes referred to as "regulatory negotiation" or "regneg") emerged in the 1980s as a supplement to the traditional procedure for developing regulations. The act largely codified the practices of those agencies that had previously used the negotiated rulemaking procedure and incorporated relevant recommendations of the now defunct Administrative Conference of the United States (ACUS). The act encourages (but does not require) agencies to consider convening a negotiated rulemaking committee before developing and issuing a proposed regulation under the Administrative Procedure Act (APA), described elsewhere in this compendium. The committee, composed of representatives of the agency and the various interest groups that would be affected by the proposed regulation, addresses areas of concern in the hope that it can reach agreement on a proposed regulation. The agency can (but, again, is not required to) then issue the agreed-upon proposal as a proposed rule, and, if appropriate after public comment, as a final rule under the APA. Since committee agreement is normally by unanimous consent, the expectation is that any rule drafted through negotiated rulemaking would be easier to implement and less likely to be the subject of subsequent litigation. In establishing negotiating committees, agencies must comply with the Federal Advisory Committee Act (described elsewhere in this compendium). Agency actions related to establishing, ending, or supporting the committees are not judicially reviewable.

Following passage of the Negotiated Rulemaking Act, ACUS served as a clearinghouse on regulatory negotiation matters and assisted agencies in establishing procedures for the conduct of regulatory negotiations and the training of personnel. When ACUS was abolished in 1995, some of its resources and responsibilities in the area were assumed by the Federal Mediation and Conciliation Service (FMCS). The Clinton Administration's National Performance Review recommended increased use of negotiated rulemaking, and Executive Order 12866 (September 1993) directed agencies to consider the use of consensual mechanisms, such as negotiated rulemaking, when developing regulations. Congress has sometimes required agencies to use negotiated rulemaking in developing rules in certain areas.

Major Provisions

The major provisions of the act require that (1) a negotiated rulemaking committee consist of at least one member of the agency and no more than 25 members, unless the head of the agency determines that more are needed; (2) the agency select an impartial "facilitator" to chair meetings, subject to the approval

of the committee by consensus; (3) an agreement on any negotiated rulemaking must be unanimous, unless the negotiated rulemaking committee agrees to other conditions; (4) any proposal agreed to by the negotiated rulemaking committee is not binding on the agency or other parties; and (5) the head of an agency, when deciding whether to establish a negotiated rulemaking committee, assure that (a) there are a limited number of identifiable interests that will be significantly affected by the rule; (b) there is a reasonable likelihood that a committee can be convened with a balanced representation of interested parties who are willing to negotiate in good faith; and (c) there is a reasonable likelihood that a committee will reach a consensus on the proposed rule within a fixed period of time. The act also allows agencies to pay reasonable travel and per diem expenses, and reasonable compensation, to committee members under certain conditions.

Discussion

Negotiated rulemaking is a possible supplement to, but not a replacement of, the normal rulemaking procedures that agencies are required to follow under the APA. For any proposal agreed to by a negotiated rulemaking committee to take effect, the agency must still develop and issue it as a regulation under the provisions of the APA. The use of negotiated rulemaking by federal agencies is strictly voluntary. Also, negotiated rulemaking does not impair any rights otherwise retained by agencies or private parties. Even if agreement is reached on a proposal by a negotiated rulemaking committee, neither the agency nor the other members of the committee are bound by the agreement. An agency need not issue the proposed regulation drafted by the committee. If an agreed-upon proposal is issued by the agency as a regulation under the APA, it may still be challenged in court by parties who previously agreed to it in committee.

Agencies are encouraged to convene and use a negotiated rulemaking committee only when certain conditions are expected to produce a successful or favorable result (e.g., easy identification of those likely to be affected by the rule and, where differences exist, the parties' willingness to consider each others' points of view). Since agreement by the parties generally must be by unanimous consent, it is essential that the parties involved be willing to compromise in order to reach agreement. The fact that participants may change their minds and later challenge a regulation they initially supported can increase their willingness to participate in the process.

These factors can, however, also serve to limit the instances when agencies see negotiated rulemaking as a viable option. In addition, agency experience with the technique indicates that negotiated rulemaking can be more costly than conventional rulemaking methods, particularly at the front end of the process. Finally, research indicates that negotiated rulemaking does not appear to reduce the overall time taken to issue a rule or to make rules more likely to avoid litigation. These findings are particularly notable given that agencies are instructed to use negotiated rulemaking only when they expect success. Other

research, however, indicates that negotiated rulemaking can increase satisfaction with the substance of the final rule and with the overall process.

Selected Source Reading

Coglianese, Cary. "Assessing Consensus: The Promise and Performance of Negotiated Rulemaking." Duke University Law Journal, vol. 46 (1997), pp. 1255-1349.

Langbein, Laura I. and Cornelius M. Kerwin. "Regulatory Negotiation versus Conventional Rule Making: Claims, Counterclaims, and Empirical Evidence." Journal of Public Administration Research and Theory, vol. 10 (2000), pp. 599 632.

Lubbers, Jeffery S. A Guide to Federal Agency Rulemaking, 3rd ed. Chicago: American Bar Association Publishing, 1998, pp. 127-131.

U.S. Administrative Conference of the United States, Negotiated Rulemaking Sourcebook. Washington: GPO, 1995.

Curtis W. Copeland

L. National Environmental Policy Act

Statutory Intent and History

The National Environmental Policy Act of 1969 (NEPA) was enacted on January 1, 1970 (83 Stat. 852; P.L. 91-190; 42 U.S.C. § 4321). The act is considered to be landmark legislation which "set the Nation on a new course of environmental management" (H.Rept. 92-316). The Preamble to the law states:

To declare a national policy which will encourage productive and enjoyable harmony between man and his environment; to promote efforts which will prevent or eliminate damage to the environment and biosphere and stimulate the health and welfare of man; to enrich the understanding of the ecological systems and natural resources important to the Nation; and to establish a Council on Environmental Quality.

Its "action-forcing" directives are meant to ensure that environmental values are given appropriate consideration in all programs of the federal government. Its policy declaration and its procedures for environmental impact assessment have been adopted in many similar state laws, and also by other nations.

The preparation of environmental impact statements (EISs) has heightened awareness of, and attention to, the environmental effects of actions by federal agencies while also increasing public participation. The requirements of the law have played a limited role in what decisions are ultimately made because the law is procedural, and does not establish environmental standards. It has spawned an enormous amount of information-gathering and analysis activities, which have been criticized by supporters as (substantively or scientifically) inadequate and by critics as too burdensome.

The National Environmental Policy Act should be distinguished from the substantive body of environmental protection laws, which attempt to correct pollution and resource problems ranging from air and water quality and noise and toxic substances control to the various statutes related to resource development, such as surface mining regulation, coastal zone and offshore management, or various public land programs. In contrast, NEPA is a relatively short policy declaration and impact assessment law designed to avoid or prevent such problems by informing the public about environmental consequences before a project is begun, and has been more associated with "administrative reforms" within federal agencies than with any particular aspect of (physical) environmental protection. NEPA compliance is required in connection with many other laws, if the action is one that triggers the EIS preparation criterion of "significantly affecting the quality of the human environment."

Government-wide rules of the Council on Environmental Quality (CEQ) require impact statement preparation to be integrated as much as possible with studies, surveys, and analyses under other federal environmental review laws — such as the Endangered Species Act, the Fish and Wildlife Coordination Act, the National

Historic Preservation Act, and, for example, water quality permits, as well as executive orders on floodplain management and wetlands protection. However, once an agency complies with NEPA's information-based procedures, the act's effect on ultimate decisions is limited by the agency's other mandates.

While there now seems to be agreement about the utility of assessing the environmental consequences of major federal actions, the long-term compliance trends depend on whether individual agencies will continue to adapt their practices to the streamlined, but rigorous, process in CEQ regulations for more fully integrating the impact analyses with agency plans and programs. Otherwise, lessened compliance could evolve and lead to new legal challenges.

Enforcing requirements for preparation of environmental impact statements is partially achieved through public participation and judicial reviews. The role of the courts in interpreting and enforcing compliance has been perhaps the most controversial aspect of NEPA's previous implementation. Some NEPA compliance issues have been raised anew in court challenges — especially during a period when program changes affect federal resource management of public lands. Typical of the effects on NEPA compliance are the EIS "categorical exclusions," issued by federal agencies which permit additional activities on public lands that would now be excluded from the NEPA process, unless considered as part of overall assessments in broad, "areawide EISs." An evaluation of the cumulative results of these excluded actions is often not feasible. (See reference for 2003 NEPA Task Force, as well as specific legislative provisions for streamlining compliance for grazing, P.L. 108-7 and 108-11; forest health, P.L. 108-148; and aviation projects, P.L. 168-176.)

Major Provisions

Title I.
Section 101: Policies and Goals. (a) Congress declared: "it is the continuing policy of the federal government ... to create and maintain conditions under which man and nature can exist in productive harmony, and fulfill the social, economic, and other requirements of present and future generations of Americans. (b) In order to carry out the policy ... it is the continuing responsibility of the federal government ... to improve and coordinate federal plans, functions, programs, and resources" to achieve six broadly stated goals that address future environmental quality objectives, with the paramount concerns including "responsibilities ... as trustee of the environment for succeeding generations," attaining "beneficial uses of the environment without degradation, or risk to health or safety"; preserving "diversity" of natural, historic, and cultural heritages; achieving a "balance between population and resource use"; and enhancing the "quality of renewable resources and ... maximum attainable recycling."

Section 102: Administration. Congress directed that, to the fullest extent possible, the laws of the United States shall be administered in accordance with

these policies, and further directed all federal agencies to incorporate the policies and goals through information and methods for appropriate consideration of environmental values by using "a systematic, interdisciplinary approach," and by considering "presently unquantified environmental amenities and values."

Section 102(2)(C): Environmental Impact Statements. As an "actionforcing" mechanism to carry out those policies and procedures, agency officials are required to include a "detailed statement" of environmental impacts as part of "every recommendation or report on proposals for legislation and other major federal actions significantly affecting the quality of the human environment." This statement of environmental impact is to assess any "adverse environmental effects," and alternatives to the proposed action, local short-term uses of the environment in relation to "long-term productivity," and "any irreversible and irretrievable commitments of resources" involved.

Prior to taking action, the responsible federal official is to consult any federal agency with jurisdiction or special expertise on any environmental impacts and to make the "statement and the comments and views of the appropriate Federal, State, and local agencies...available to the President, the Council on Environmental Quality, and to the public."

Other provisions of Section 102 require federal agencies to (1) separately develop alternative courses of actions for unresolved resource conflicts; (2) "support ... international cooperation in ... preventing ... a decline in the quality of mankind's world environment"; (3) provide advice and information to other units of governments, institutions, and individuals; (4) develop ecological information on resource-oriented projects; and (5) assist the CEQ.

Section 103: Review. Section 103 requires agencies to "review their present statutory authority ... for ... any deficiencies ... which prohibit full compliance," while Sections 104 and 105 affirm existing environmental authorities, and supplement them with NEPA.

Title II.
Title II created in the Executive Office of the President a three-member Council on Environmental Quality to oversee the administration of national environmental policy and to assist in the President's annual Environmental Quality Report to Congress. This report is to examine (1) the status and condition of the natural environment; (2) trends in the quality, management, and utilization of the environment, and their effects; (3) the adequacy of natural resources; (4) a review of environmental programs and activities; and (5) a program for remedying deficiencies, along with legislative recommendations.

Another major duty of the council is to advise and recommend policies to the President. (The council's authority to guide the NEPA process — including its new regulations — has been supplemented by Executive Orders 11514, 11991, and 12114.)

Highlights of Judicial Interpretation of NEPA. Major court decisions involving the National Environmental Policy Act have:

- held it to be a "full disclosure" law — pertaining to federal agencies administrative records and information concerning impacts — for actions subject to the act;
- required "strict compliance" with the procedures — entailing a unique balancing analysis of the environmental costs and benefits of a proposed action;
- ruled that the consideration of alternatives to the proposed action must be of a broad nature and not necessarily confined to an agency area of statutory authority;
- further ruled that the alternatives and environmental consequences must be given full consideration in decision making (and subject to Administrative Procedure Act compliance);
- affirmed the long-standing practice of preparing regional or programmatic impact statements for related federal actions (i.e., "comprehensive impact statements");
- supplemented the public participation afforded through EIS comment procedures by liberally construing standing requirements applicable to persons seeking judicial review of agency NEPA compliance; and
- upheld the provisions for obtaining access to relevant information through the Freedom of Information Act.

The Council on Environmental Quality's authority to issue its implementing regulations — binding upon the federal agencies — has been broadly endorsed by the Supreme Court, whose reviews of lower court opinions have held procedural compliance with NEPA to be sufficient.

Discussion

A continuing issue for future NEPA implementation is its effect on the policy level of decision making, given its early application — and some say its overemphasis on procedural matters — at the project level. This "level of assessment" issue, and its potential for "trivialization" of the act's basic policy purposes, seems to be of less concern as greater experience is gained in applying the law, since site-specific, project level assessments generally serve real purposes in the government's decision making processes — i.e., public accountability for agency actions; a framework for citizen participation in resolving controversies; and a more systematic approach for generating environmental information. Furthermore, numerous, but "properly scoped," impact statements that are prepared efficiently can conceivably minimize "on the ground" impacts at the present time, given the limitations in the methodologies for assessing the broader scope and longer-term environmental effects.

Another recurring question is whether NEPA's clear requirement for environmental assessments of agencies' legislative proposals is being adequately implemented or enforced — under the regulations' new flexible criteria — to address environmental concerns at the earliest stages of program initiatives originating in the executive branch. While the impact assessment and interagency review process has increasingly been used as an integral framework for structuring some decision making activities — i.e., relating the NEPA analysis to project feasibility or federal or state coordination activities — the longer-term question is whether these advantages outweigh the procedural uncertainties that would be associated with analyzing environmental impacts of more fundamental policy choices. For example, in the 1990s, the President's authority to negotiate new international trade agreements (without the most formal level of NEPA compliance) was upheld.

The most basic policy issue regarding the viability of the overall NEPA process is in maintaining a sufficiently neutral and flexible environmental information, assessment, and review procedure to accommodate actions and decisions of the utmost variety, complexity, and controversy to which the law applies — without the mechanics of the procedures themselves becoming a part of the controversy. In part, this is a matter of efficiency — of how usefully the process serves public decision making by holding agencies accountable without undue regulatory-type burdens — and partly a matter of equity, so that all reasonable alternatives, points of view, and parties to a decision can (over time) benefit from informed debate about environmental effects.

Selected Source Reading

Caldwell, Lynton K. The National Environmental Policy Act: An Agenda for the Future. Bloomington, IN: Indiana University Press, 1998.

"Charting the Boundaries of NEPA's Substantive Mandate: Stryker's Bay Neighborhood Council, Inc v. Karlen," Environmental Law Reporter 10 (February 1980), pp. 10039-10044.

Raymond, James F. "A Vermont Yankee in King Burger's Court: Constraints on Judicial Review under NEPA." Boston College Environmental Affairs Law Review, vol. 7 (1979), pp. 629-664.

Taylor, Serge. Making Bureaucracies Think. Stanford, CA: Stanford University Press, 1984.

Council on Environmental Quality. Environmental Quality — [the 27th] Annual Report. Washington: GPO, 2000. (See Part I on NEPA.)

National Environmental Policy Act. "Implementation of Procedural Provisions; Final Regulations." Federal Register, vol. 43, no. 230 (November 29, 1978), pp.

55978-56007. (Codified in the Code of Federal Regulations at 40 C.F.R. Parts 1500-1508.)

Council on Environmental Quality. The National Environmental Policy Act: A Study of Its Effectiveness. Washington: GPO, 1997.

The NEPA Task Force Report to the Council on Environmental Quality: Modernizing NEPA Implementation. September 2003. (Online edition available at [http://ceq.eh.doe.gov/ntf/report/index.html], visited January 27, 2003.)

CRS Report RL32024. Background on NEPA Implementation for Highway Project: Streamlining the Process, by Linda G. Luther.

Congress. House. Committee on Resources. Problems and Issues with the National Environmental Policy Act of 1969. Hearings. 105th Congress, 2nd session. Washington: GPO, 1998.

Congress. Senate. Committee on Energy and Natural Resources. Application of the National Environmental Policy Act. S.Hrg. 104-81. 104th Congress, 1st session. Washington: GPO, 1995.

Harry Steven Hughes

M. E-Government Act of 2002

Statutory Intent and History

The E-Government Act of 2002 (116 Stat. 2899; P.L. 107-347) was enacted to enhance access to government information and the delivery of information and services to citizens, employees, and other agencies and entities. To meet this goal, the statute authorizes $345 million over four years for e-government initiatives. It also assigns considerable influence to the Office of Management and Budget (OMB) to ensure that information technology (IT) investments throughout the federal government embrace a citizen-centered, cross-agency, and performance-based strategy.

As defined in the statute, e-government refers to "the use by Government of web-based Internet applications and other information technologies, combined with processes that implement these technologies, to (A) enhance the access to and delivery of Government information and services to the public, other agencies, and other Government entities; or (B) bring about improvements in Government operations that may include effectiveness, efficiency, service quality, or transformation" (116 Stat. 2902). Both the term and the concept of e-government are relatively new in government parlance. The phrase appeared, without explanation, in the initial September 7, 1993 report of the National Performance Review (NPR).[731] A joint report of the NPR and the Government Information Technology Services Board, issued on February 3, 1997, gave the term more prominence and substance.[732] Almost three years later, in a December 17, 1999 memorandum to the heads of executive departments and agencies, President William Clinton directed these officials to take certain actions in furtherance of "electronic government."[733]

President George W. Bush indicated his support for e-government initiatives early in his Administration when he proposed the creation of an e-government fund. In advance of his proposed budget for FY2002, the President released, on February 28, 2001, A Blueprint for New Beginnings: A Responsible Budget for America's Priorities. Introduced as a 10-year budget plan, the Blueprint, among other innovations, proposed the establishment of an electronic government account, seeded with "$10 million in 2002 as the first installment of a fund that

---

[731] Office of the Vice President, From Red Tape to Results: Creating a Government That Works Better & Costs Less, Report of the National Performance Review (Washington: GPO, 1993), p. 112.

[732] Office of the Vice President, Access America: Reengineering Through Information Technology, Report of the National Performance Review and the Government Information Technology Services Board (Washington: GPO, 1997).

[733] U.S. National Archives and Records Administration, Office of the Federal Register, Public Papers of the Presidents of the United States: William J. Clinton, 1999 (Washington: GPO, 2001), p. 2317.

will grow to a total of $100 million over three years to support interagency electronic Government (egov) initiatives." Managed by OMB, the fund was foreseen as supporting "projects that operate across agency boundaries," facilitating "the development of a Public Key Infrastructure to implement digital signatures that are accepted across agencies for secure online communications," and furthering "the Administration's ability to implement the Government Paperwork Elimination Act of 1998, which calls upon agencies to provide the public with optional use and acceptance of electronic information, services and signatures, when practicable, by October 2003."[734] About one month later, on March 22, OMB announced that the Bush Administration recommended doubling the amount to be allocated to the e-government fund, bringing it to $20 million. House appropriators, however, were particularly reluctant to provide more than a quarter of the amount sought by the President. While expressing general support for the purposes of the fund, they also recommended that the Administration work with the House Committee on Government Reform and the Senate Committee on Governmental Affairs to clarify the status of its authorization. The E-Government Act establishes an E-Government Fund in the Treasury of the United States with specific levels of appropriations authorized through FY2006 and "such sums as are necessary for fiscal year 2007" (116 Stat. 2908).

Pursuant to an OMB Memorandum of July 18, 2001, an E-Government Task Force was established to create a strategy for achieving the e-government goals of the Bush Administration. It subsequently identified 23 interagency initiatives designed to better integrate agency operations and IT investments. These initiatives, sometimes referred to as the Quicksilver projects, were grouped into five categories: government to citizen, government to government, government to business, internal efficiency and effectiveness, and addressing cross-cutting barriers to e-government success. Examples of these initiatives included an E-Authentication project, led by the General Services Administration to increase the use of digital signatures; the eligibility assistance online project (also referred to as GovBenefits.gov), led by the Department of Labor to create a common access point for information regarding government benefits available to citizens; and the Small Business Administration's One-Stop Business Compliance project (later renamed Business Gateway), designed to help businesses navigate legal and regulatory requirements. An additional initiative, a government-wide payroll process project, was subsequently added by the President's Management Council. In 2002, the E-Clearance initiative, originally included as part of the Enterprise Human Resources Integration project, was established as a separate project, for a total of 25 initiatives. These projects became part of the President's Management Agenda — FY2002, submitted to Congress in August 2001 and featuring five

---

[734] U.S. Executive Office of the President, Office of Management and Budget, A Blueprint for New Beginnings: A Responsible Budget for America's Priorities (Washington: GPO, 2001), pp. 179-180.

interrelated government-wide initiatives: Strategic Management of Human Capital, Competitive Sourcing, Improved Financial Performance, Expanded Electronic Government, and Budget and Performance Integration.[735]

After the Clinger-Cohen Act of 1996, the E-Government Act takes the next step to improve IT investment and management, requiring OMB to provide a report to Congress annually on the status of e-government. Rather than simply identifying and reporting IT investment at each agency, the statute appears to have engendered a cultural change in IT procurement, from consolidating and integrating IT investments to encouraging performance-based, citizen-centered, cross-agency planning. The statute designates OMB as the lead organization for all federal executive branch IT purchasing and planning, and all federal executive branch agencies must comply with OMB guidance to ensure implementation of e-government.

Major Provisions

The E-Government Act is organized in five titles containing sections which amend various titles of the United States Code. Title I of the statute, denominated Office of Management and Budget Electronic Government Services, amends Title 44, United States Code, with a new Chapter 36 on Management and Promotion of Electronic Government Services. In addition to defining key terms, Title I establishes an Office of Electronic Government within OMB, headed by an administrator, who is appointed by the President without Senate confirmation. The administrator assists the Director of OMB with all functions assigned in Chapter 36, as well as those assigned to the director by Title II of the statute, and "other electronic government initiatives." The administrator is also responsible for assisting the OMB Director, deputy director for management, and administrator of the Office of Information and Regulatory Affairs "in setting strategic direction for implementing electronic Government" relevant to certain specified statutory authorities.

Title I of the statute also establishes a Chief Information Officers Council, chaired by the OMB deputy director for management and composed largely of department and agency chief information officers. The council plays an advisory and coordination role. Other features of Title I are creation of the E-Government Fund to support e-government projects; establishment of a government-wide program "to encourage contractor innovation and excellence in facilitating the development and enhancement of electronic Government services and processes"; and mandating an annual e-government status report by the OMB Director to Congress.

---

[735] U.S. Executive Office of the President, Office of Management and Budget, The President's Management Agenda — FY2002 (Washington: GPO, 2001).

Title II of the statute, pertaining to Federal Management and Promotion of Electronic Government Services, specifies the responsibilities of agency heads regarding electronic government; mandates interoperable implementation of electronic signatures for appropriately secure electronic transactions with government; prescribes criteria for maintaining and promoting an integrated federal Internet portal; promotes individual federal court websites and agency use of IT to increase access, accountability, transparency, and public participation in the development and issuance of regulations; fosters improvements in the methods by which government information, including information on the Internet, is organized, preserved, and made accessible to the public; establishes privacy impact assessments for agencies when developing or procuring IT that collects, maintains, or disseminates personally identifiable information or when initiating a new collection of such information; and creates a federal workforce skills development program for using IT to deliver government information and services.

Title II also amends Subpart B of Part III of Title 5, United States Code, with a new Chapter 37 mandating an Information Technology Exchange Program, facilitating temporary assignments of federal employees to private sector organizations and of private sector employees to federal agencies to enhance IT skills. Other provisions mandate studies and evaluations of (1) community technology centers, public libraries, and other institutions providing computer and Internet access to the public; (2) the use of IT to enhance crisis preparedness, response, and consequence management of natural and man-made disasters; and (3) disparities in Internet access for online government services. Another provision tasks the Administrator of General Services with making a coordinated effort to "facilitate the development of common protocols for the development, acquisition, maintenance, distribution, and application of geographic information."

Title III of the statute, denominated the Federal Information Security Management Act of 2002 (discussed elsewhere in this compendium), amends Chapter 35 of Title 44, United States Code, with a new Subchapter III on information security. It supersedes similar provisions found in Subtitle C of Title II of the Homeland Security Act of 2002 (116 Stat. 2135, at 2155). Excepting national security systems, Subchapter III prescribes a comprehensive program, under the direction of the OMB Director, for ensuring the effectiveness of information security controls over information resources that support federal operations and assets. Covered agencies are required to have performed annually an evaluation of the effectiveness of their information security program and practices.

Title IV authorizes generally, unless otherwise specified elsewhere in the act, "such sums as are necessary" to carry out Titles I and II for FY2003-FY2007.

Title V of the statute, denominated the Confidential Information Protection and Statistical Efficiency Act of 2002, vests the OMB Director with responsibility for

coordinating and overseeing the confidentiality and disclosure policies established by the title. Subtitle A prescribes limitations on the use and disclosure of statistical data or information, and sets fines and penalties for violations of these limitations. Subtitle B, after identifying the Bureau of the Census, Bureau of Economic Analysis, and Bureau of Labor Statistics, as "designated statistical agencies," prescribes the responsibilities, as well as the business data sharing ground rules and limitations, of these agencies.

Discussion

Building upon the Clinger-Cohen Act (described elsewhere in this compendium), the E-Government Act serves as the primary legislative vehicle to guide evolving federal information technology management practices and to promote initiatives to make government information and services available online. In doing so, it also represents a continuation of efforts to realize greater efficiencies and reduce redundancies through improved intergovernmental coordination, and by aligning information technology investments. In addition, while the Bush Administration's Quicksilver initiatives are separate from the E-Government Act, someof thegoals of the Quicksilver initiatives are reinforced by the act's provisions. For example, Section 216 addresses the development of common protocols for geographic information systems, which is also one of the objectives of the Geospatial One-Stop project ([http://www.geo-one-stop.gov/]). Section 203 directs agencies to adopt electronic signature methods. Likewise, the E-Authentication initiative strives to develop a government-wide approach to electronic identity systems ([http://www.cio.gov/eauthentication/]). In addition, some of the act's broader provisions, such as those related to the development of privacy guidelines, information security standards, and the identification of means to bridge disparities in Internet access among citizens, contribute to the technological and regulatory infrastructure needed to support e-government generally.

However, while the law is still relatively new, the rapid pace of technological change and the drive to implement initiatives in a timely manner have raised a number of implementation issues that mayarise duringcongressional oversight. One of these issues involves the recruitment and retention of IT managers, at both the chief information officer (CIO) and project manager levels. As IT projects have become more integrated into the function of a department or agency, the role of CIOs has evolved as well. CIOs are reportedly being called upon not only for their technological expertise, but also to provide strategic leadership in the areas of policy, budget, and contract oversight.[736] The CIO's relationship with top-level department decision makers can also be critical to

[736] Cynthia L. Webb, "Providing the Technology Vision," Washington Post, Mar. 6, 2003, available at [http://www.washingtonpost.com/wp-dyn/articles/A47136-2003Mar5.html], visited Dec. 3, 2003.

successfully implementing e-government initiatives. This suggests that in selecting a department-level CIO, one needs to consider the strengths and weaknesses of choosing a career employee, who may have a deeper contextual understanding of the mission and functions of an organization, and recruiting a candidate from the private sector who may bring a wider range of experiences and perspectives to the position.[737] Similarly, the increased size and complexity of IT projects has further underscored the need for strong project managers to carry out these initiatives. While it is not uncommon for IT project management to be just one of several duties assigned to an individual, some observers have suggested that IT projects with budgets of $5 million or larger should have dedicated, full-time managers. The possibility of requiring federal IT project managers to obtain some form of professional certification has also been raised.[738]

Another issue is information security. In a series of evaluations published since 1997, the General Accounting Office (GAO) has repeatedly reported that the largest federal agencies have made only limited progress in addressing computer security vulnerabilities, citing information security as a government-wide high risk issue. Specifically, GAO has identified six areas of weaknesses: lack of senior management attention to information security; inadequate accountability for job and program performance related to IT security; limited security training for general users, IT professionals, and security professionals; inadequate integration of security into the capital planning and investment control process; poor security for contractor-provided services; and limited capability to detect, report, and share information on vulnerabilities or to detect intrusions, suspected intrusions, or virus infections.[739] For e-government activities, service continuity is considered critical not only for the availability and delivery of services, but also to build citizen confidence and trust. The risks of fraud and misuse of sensitive data are concerns as well. Heightened concerns about homeland security and critical infrastructure protection have also drawn attention to the role of information security. The inclusion of Title III of the E-Government Act (referred to as the Federal Information Security Management Act) permanently re-authorizes and amends the Government Information Security Reform Act (GISRA), providing additional means for congressional overseers to assess this issue.

---

[737] Sara Michael, "Insider Information," Federal Computer Week, Apr. 14, 2003, p. 26.

[738] Sara Michael, "Do Your Project Managers Measure Up?," Federal Computer Week, Nov. 3, 2003, p. 28; Sara Michael, "Execs Call for Full-Time Project Managers," Federal Computer Week, Nov. 5, 2003, available at [http://www.fcw.com/fcw/articles/2003/1103/ web-egov-11-05-03.asp], visited Dec. 3, 2003.

[739] U.S. General Accounting Office, Information Security: Continued Efforts Needed to Fully Implement Statutory Requirements, GAO-03-852T, June 24, 2003, p. 8.

A third issue is the interoperability of technology. Interoperability refers to the ability of a computer system or data to work with other systems or data using common standards or processes. Interoperability is an important part of the larger efforts to improve interagency collaboration and information sharing through e-government and homeland security initiatives. It also represents a significant challenge as the federal government implements cross-agency initiatives, such as the E-Payroll and GovBenefits.gov projects, to eliminate redundant systems and facilitate a "one-stop service delivery" approach to e-government.[740] One means being used to address this issue is the development of a federal enterprise architecture, at the website [http://www.feapmo.gov/]. An enterprise architecture serves as a blueprint of the business functions of an organization, and the technology used to carry out these functions. While this blueprint is still in its early stages, federal agencies are being required to justify their IT investments based partly on their ability to make a strong business case to support each request, and based on how closely the project aligns with the federal enterprise architecture. Decisions made early in the development of the federal enterprise architecture can have significant implications for future IT projects, suggesting that regular assessments of this process may be necessary to help minimize any potential complications.

Other issues include, but are not limited to, balancing the sometimes competing demands of e-government and homeland security, measuring e-government performance, assessing and monitoring the quality of agency IT project "business cases," and balancing cross-agency funding approaches with oversight interests.

Selected Source Reading

U.S. Congress. House. Committee on Government Reform. E-Government Act of 2002. Report to accompany H.R. 2458. 107th Congress, 2nd session. H.Rept. 107-787, part 1. Washington: GPO, 2002.

U.S. General Accounting Office. Electronic Government: Selection and Implementation of the Office of Management and Budget's 24 Initiatives. GAO03-229. November 2002.

——. Electronic Government: Success of the Office of Management and Budget's 25 Initiatives Depends on Effective Management and Oversight. GAO-03-495T. March 13, 2003.

——. Information Security: Continued Efforts Needed to Fully Implement Statutory Requirements. GAO-03-852T. June 24, 2003.

[740] U.S. Executive Office of the President, Office of Management and Budget, Implementing the President's Management Agenda for E-Government - E-Government Strategy, Apr. 2003, p. 9, available at: [http://www.whitehouse.gov/omb/egov/downloads/2003egov_strat.pdf], visited Dec. 3, 2003.

Harold C. Relyea
Jeffrey W. Seifert

N. Federal Information Security Management Act of 2002

Statutory Intent and History

The Federal Information Security Management Act of 2002 (FISMA) replaced what has been commonly referred to as the Government Information Security Reform Act (GISRA),[741] which expired at the end of the 107th Congress. Congress passed two versions of FISMA at the end of the 107th Congress. The first version passed as part of the Homeland Security Act of 2002 (P.L. 107-296, Title X; 116 Stat. 2135, at 2259). The second version passed as part of the E-Government Act of 2002 (P.L. 107-347, Title III; 116 Stat. 2946). The two versions differ slightly. The E-Government Act version takes precedence.[742] The act applies government-wide, including to small and independent agencies of the federal government.

Both GISRA and FISMA represent an effort by Congress to improve federal agency compliance with information security standards and guidelines. Congress put into statute certain requirements, including the requirement that federal agencies submit their information security programs to an annual independent review, and a requirement that the Director of the Office of Management and Budget (OMB) shall report the results of these reviews to Congress.

Congress has long been concerned with securing federal information systems. This concern has grown as the federal government has increased the amount of information it collects and maintains and as the information systems upon which that information is kept become increasingly interconnected and vulnerable to unauthorized access. Both GISRA and FISMA build upon the Computer Security Act of 1987 (P.L.100-235) and the Paperwork Reduction Act of 1995 (P.L. 104-13). The Computer Security Act required agencies to inventory their computer systems and to develop computer security plans for each. The Paperwork Reduction Act authorized the Director of OMB to oversee the development of information resource management policies, including those related to information security. While FISMA repeals or supercedes various provisions of the Computer Security Act from the United States Code, it maintains many of the same roles and responsibilities. Likewise, FISMA expands upon the roles and requirements originally cited in the Paperwork Reduction Act.

---

[741] GISRA was passed as part of the Floyd D. Spence National Defense Authorization Act for FY2001 (P.L. 106-398, Title X, Subtitle G).

[742] In its FY2002 Report to Congress on Federal Government Information Security Reform (May 16, 2003), the Office of Management and Budget cites the E-Government Act version as being applicable (see pp. 6 and 16). Also, the E-Government version contains language that states that while its amendments to Chapter 35, Title 44 of the United States Code stay in effect, the amendments made to Chapter 35, Title 44 by the Homeland Security Act version do not apply. See 44 U.S.C. § 3549, as enacted by the E-Government Act.

Major Provisions

The Federal Information Security Management Act of 2002 has five major provisions. Section 301 of the act amends Chapter 35 of Title 44 of the United States Code by adding a new Subchapter III on Information Security. Section 302 amends 40 U.S.C. § 11331, which relates to the prescription of information security standards. Section 303 of the act amends the National Institute of Standards and Technology Act (NIST; 15 U.S.C. § 278g-3), which assigns to NIST the mission of developing standards for information technology, including security standards for federal information systems. Section 304 amends the National Institute of Standards and Technology Act (15 U.S.C. § 278g-4), which establishes the Information Security and Privacy Advisory Board. Section 305 makes technical changes and conforming amendments, two of which are of some significance.

Chapter 35 of Title 44, United State Code, Subchapter III, on Information Security expands upon the authorities and responsibilities for the development, implementation, review, and oversight of policies and practices associated with securing federal information systems. Specifically, it authorizes the Director of OMB to oversee the development and implementation of information security policies, standards, and guidelines across the federal government. The director's authority includes overseeing the development of policies, principles, standards and guidelines; reviewing and approving or disapproving agency security programs; and, taking actions as authorized by 40 U.S.C. §11303,[743] including budgetary actions, to ensure compliance with policies, standards, and guidelines. However, only the director's authorities under 40 U.S.C. § 11303 extend to national security systems.[744] Development and oversight of standards and guidelines for national security systems are prescribed by law or the President. In addition, FISMA grants to the Secretary of Defense and the Director of Central Intelligence, the authority to oversee the development of information security policies, principles, standards, and guidelines for information systems operated by or for the Department of Defense and the Central Intelligence Agency, if the compromise of information on these systems would have a debilitating impact on

[743] 40 U.S.C. § 11303 details the director's authority to evaluate agency performance-based programs in acquiring information technology.

[744] FISMA defines a national security system as "any information system (including telecommunications system), the function or operation of which: involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapon system or is critical to the direct fulfillment of military or intelligence missions; or is protected at all times by procedures established for information that have been specifically authorized under criteria established by Executive Order or an Act of Congress to be kept classified in the interest of nation security." The definition notes that a system used for routine administrative and business applications (e.g. payroll) shall not be considered a national security system. President Reagan laid out the roles and responsibilities of federal agencies for the protection of national security systems in National Security Decision Directive 145 (NSDD-145). NSDD-145 remains in effect.

the mission of these two agencies. It is not clear if this provision includes systems that do not meet the definition of national security systems.

In addition to assigning the authorities discussed above, Subchapter III also requires each agency to develop and implement an information security program. It prescribes what this program should include. It assigns each agency head the responsibility for developing and ensuring the implementation of the program, including designating a senior agency information security officer whose responsibility is to ensure compliance with the agency's program. It also requires that agencies evaluate their security programs annually and include the results of these reviews in a number of reports required by Congress, including performance reports and financial reports.

Subchapter III also requires that each agency submit its information security program to an annual independent review. The reviews are to be conducted by the agency's inspector general, if it has one, or an outside evaluator. The subchapter requires that the results be submitted to the Director of OMB who is to summarize them in a report to Congress. This perhaps is the major element of FISMA (and GISRA before it) by which Congress intended to ensure adequate oversight and compliance with federal information security requirements.

FISMA amends 40 U.S.C. § 11331 which authorizes the Secretary of Commerce to prescribe standards and guidelines (developed by NIST, see below) pertaining to federal information systems. Those pertaining to information security are to be made mandatory. This section also authorizes the President to disapprove or modify the Secretary's prescriptions and also allows agencies to follow more strict standards, as long as they contain the mandatory standards prescribed by the Secretary.

FISMA also amends 15 U.S.C. § 278g-3, which gives NIST the mission of developing standards, guidelines, and associated methods and techniques for information systems. These standards and guidelines include those for securing federal information systems, except national security systems.[745] FISMA primarily amends this section by specifying that NIST shall, at the least, develop standards for categorizing all agency information and information systems, recommending what type of information or system should be included in each category, and developing minimum security requirements for each category. FISMA also instructs NIST that these standards should, to the most practicable extent possible, be technology neutral and allow for the use of commercial-off-the-shelf products.

The amendments to 15 U.S.C. § 278g-4 rename the Computer System Security and Privacy Advisory Board the Information Security and Privacy Advisory

[745] NSDD-145 assigns this authority to the National Security Agency.

Board. The board, which was originally established by the Computer Security Act, advises the Secretary of Commerce and the Director of OMB on information security and privacy issues and reports to the Secretary, the Director of OMB, the Director of the National Security Agency, and Congress.

Finally, FISMA repeals 40 U.S.C. §11332, which included language originally enacted as part of the Computer Security Act. This language required agencies to develop security plans for their computer systems and to provide personnel training in security awareness and practices. These requirements have been subsumed in agency security program requirements mentioned above. FISMA also amends 44 U.S.C. § 3505 to include a requirement that agencies inventory their major information systems and identify where these systems interface with other systems and networks.

Discussion

Throughout the 1990s, the General Accounting Office (GAO) reported on fundamental problems associated with agency information security plans. In some cases, GAO found that agencies did not have written policies and procedures. In other cases, GAO found that policies and procedures were not enforced. In addition to problems internal to the agencies, GAO cited a lack of oversight to ensure that agencies met their obligations. GISRA addressed these problems by tightening agency requirements in statute (essentially taking OMB's guidelines and putting them in statute). GISRA also addressed the oversight issue by requiring annual independent evaluations of agency security programs, and requiring that the results be reported directly to Congress. OMB's FY2001 Report to Congress on Federal Government Information Security Reform formed the baseline by which to better measure agencies' progress in securing their information systems.

In the FY2002 report, OMB cited both progress and remaining issues within the federal government. For example, out of 7,957 federal systems evaluated, the number of systems for which risk assessments have been done increased from 43% to 65%. OMB cited similar increases for the number of systems with updated security plans, and the number of systems with contingency plans. However, OMB identified six areas in which problems persist: lack of management attention; nonexistent security performance measures; poor security education and awareness; failure to fully fund and integrate security into capital planning; failure to ensure contractors are secure; and lack of detecting, reporting, and sharing information on vulnerabilities.

GAO's evaluation of the FY2002 results[746] was more critical of the progress made. For example, while OMB noted that 11 of 24 agencies had assessed risk for 90% to 100% of their systems, GAO noted that 8 reported that they had assessed fewer than 50%. The House Technology, Information Policy, Intergovernmental Relations and the Census Subcommittee of the House Government Reform Committee, which maintains a computer security report card, noted that while 14 agencies improved their grades, based on the subcommittee's scoring, 14 agencies remain with grades below C, and 8 have failed (again, according to the subcommittee scoring).[747]

Also, there remains some tension over the roles and responsibilities for national security systems versus non-national security systems. Part of the reason Congress passed the Computer Security Act was to ensure that the national security community would not have too great a role in setting computer security standards for civilian federal computer systems.[748] There was a similar debate over the definition of sensitive information which the act sought to protect. While Congress recognized that, in addition to classified information, the government holds sensitive information, the compromise of which could adversely affect the national interest or conduct of federal programs, or the privacy of individuals, Congress did not intend the term to constitute a formal new category of information.[749] The act stipulated that the designation of sensitive implies no determination as to whether it is subject to public disclosure. However, as individual information systems become increasingly interconnected, including the connection of national security systems to civilian and public systems, some in the national security community are concerned about the level of security of these non-national security systems. FISMA maintains the distinction between roles and responsibilities for national security systems and all other systems. Still, it does require NIST to develop guidelines by which agencies can identify national security systems over which they may have control.

---

[746] U.S. Government Accounting Office, Information Security: Continued Efforts Needed to Fully Implement Statutory Requirements, GAO-03-852T, June 24, 2003.

[747] Rep. Adam Putnam, Chairman, Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, House Committee on Government Reform (statement upon the release of the Federal Computer Security Report Card), Dec. 9, 2003. Information regarding the Subcommittee's report card can be found at [http://reform.house.gov/TIPRC/News?DocumentSingle.aspx?DocumentID=2025], visited Dec. 19, 2003.

[748] NSDD-145 gave the National Security Agency authority to set technical computer standards and guidelines for national security systems. Congressional concern is discussed in H.Rept. 100-153 (parts I and II), House Science, Space, and Technology Committee, June 11, 1987.

[749] U.S. Congress, House Committee on Science, Space, and Technology, Computer Security Act of 1987, report to accompany H.R. 145, 100th Cong., 1st sess., H.Rept. 100-153, part 1 (Washington: GPO, 1987), p. 24.

Therefore, the number of systems for which more stringent national security standards must be applied may go up, or down.

Selected Source Reading

Office of Management and Budget. FY2002 Report to Congress on Federal Government Information Security Reform. May 16, 2003.

General Accounting Office. Information Security: Continued Efforts Needed to Fully Implement Statutory Requirements. GAO-03-852T. June 24, 2003.

John D. Moteff

O. Data Quality Act (Information Quality Act (IQA))

Statutory Intent and History

The Data Quality Act of 2001 (DQA) was enacted as Section 515 of the FY2001 Treasury and General Government Appropriations Act (P.L. 106-554, 44 U.S.C. § 3516 note; 114 Stat. 2763A-153). The DQA, enacted in December 2000 as a two-paragraph last-minute addition to the consolidated appropriations bill, took effect on October 1, 2002. There is no specific or explicit language on statutory intent or legislative history.

Major Provisions

The DQA required the Office of Management and Budget (OMB) to issue guidelines ensuring the "quality, objectivity, utility, and integrity" of information disseminated by the government. In turn, the law instructed most federal agencies to issue their own guidelines, following OMB's, by October 1, 2002. The act also required agencies to create an administrative process through which interested groups could challenge agency information and seek corrections. OMB, in its guidelines, further defined information quality, and required agencies to follow certain procedures depending on the use, category, and significance of the information. The resulting agency guidelines have varied depending on the area of agency responsibility. The DQA also required each agency to report periodically to the Director of OMB the number and nature of complaints received by the agency regarding the accuracy of its information, and how such complaints were handled.

Discussion

While there is no specific or explicit documentation of statutory intent or legislative history, the DQA amends the Paperwork Reduction Act (PRA) of 1995, and can be seen as related to other government documents and general management laws as well, such as OMB Circular No. A-110, OMB Circular No. A-130, the Freedom of Information Act, the Privacy Act, and the Government in the Sunshine Act. (The laws are described in detail elsewhere in this compendium.)

Under the PRA, the Office of Information and Regulatory Affairs (OIRA) was created within OMB with oversight responsibilities for other federal agencies regarding paperwork (44 U.S.C. § 3503(a) and (b)). OIRA, among other things, is responsible for developing uniform policies for efficient processing, storage, and transmission of information, within and among agencies. The PRA directed the Director of OMB to foster greater sharing of, dissemination of, and access to public information.

Agencies' data acquisition and publishing rights were stated in OMB Circular No. A-110, Subpart C. Unless specifically waived, federal agencies "have the right … to obtain, reproduce, publish, or use the data first produced under an award."

OMB Circular No. A-130 stated a federal policy of "maximizing the usefulness of information disseminated to the public," but did not provide details about or definitions of quality, integrity, accuracy, or objectivity of information.

The Freedom of Information Act, the Privacy Act, and the Government in the Sunshine Act all contain provisions regulating or generally relating to public access to governmental information, and/or procedures to challenge or correct such information.

The DQA provides more explicitly quality standards for information across the federal government, and procedures to challenge or correct such information.

The DQA applies to all federal agencies that are subject to the PRA. Data quality challenges have been filed with several agencies. Four agencies place all their DQA challenges on their Web pages: the Environmental Protection Agency (EPA); the Commodity Futures Trading Commission (CFTC); the Department of Transportation; and the Forest Service. Discerning other agencies' DQA challenges is a more involved process.

DQA challenges have covered a wide range of complexity. A DQA challenge to the CFTC in September 2003, for example, involved certain data fields missing from a document; the data fields were determined to have resulted from a programming error, and the error was corrected. On the other hand, a lawsuit brought against the White House Office of Science and Technology Policy (OSTP), challenging the data underlying the interagency "National Assessment of the Potential Consequences of Climate Variability and Change" (NACC), was settled out of court on November 6, 2003, with the OSTP posting a notice stating that the NACC was not "subjected to OSTP's Information Quality Act Guidelines."

Proponents contend the law and guidelines will improve the quality of agency science and regulations, and force agencies to regulate based on the best science available. Some of these proponents maintain that the Data Quality Act will help agencies defend their regulations against lawsuits, and reduce the number of lawsuits filed. The U.S. Chamber of Commerce's Vice President, William Kovacs, has praised the act as fair to all groups; under it, the Chamber has challenged information on the EPA website. Some opponents of the law and OMB's guidelines contend the act may have a chilling effect on agency distribution and use of scientific information. These opponents foresee a flood of data quality challenges on a wide range of scientific issues, which, they contend, may tie up agency resources and significantly delay regulations. There is no evidence yet, however, that these concerns have materialized.

Critics also argue that the DQA, and the implementing guidelines, strengthen the position of industrial opponents to federal health and environmental policies and regulations by allowing them an additional method to challenge the science on which the regulations are based. Scientific groups sought to have the draft OMB guidance revised to prevent "harassment" (through repeated data quality

challenges) of scientists working on controversial research, and to avoid imposing new obstacles to the publication of research results. The final OMB guidelines address some of these issues, but still allow challenges to the quality of research underlying official agency policies or research results published on agency websites. The guidelines allow challenges to peer-reviewed findings on a case-by-case basis.

The DQA lacks a judicial review provision allowing for a party to take a data quality dispute to court.

Selected Source Reading

Ad Hoc Committee on Ensuring the Quality of Government Information. Ensuring the Quality of Data Disseminated by the Federal Government. Washington: The National Academies Press, 2003.

U.S. Office of Management and Budget. "Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Information Disseminated by Federal Agencies" Federal Register, vol. 67, no. 36 (February 22, 2003), pp. 8452-8460.

Michael Simpson

II. Strategic Planning, Performance Measurement, and Program Evaluation

A. Inspector General Act of 1978

Statutory Intent and History

Statutory offices of inspector general (OIGs) consolidate responsibility for auditing and investigations within a federal department, agency, or other organization. Established by law as permanent, independent, nonpartisan, and objective units, the OIGs are designed to combat waste, fraud, and abuse (5 U.S.C. Appendix). The early establishments occurred in the wake of major financial and management scandals, first in 1976 in the Department of Health, Education and Welfare — now Health and Human Services (90 Stat. 2429) — and in 1978 in the General Services Administration (GSA). This later episode paved the way for OIGs in GSA and 11 other departments and agencies (92 Stat. 1101). Such offices now exist in nearly 60 federal establishments and entities, including all cabinet departments and the largest federal agencies, as well as many boards, commissions, government corporations, and foundations.[750]

Statutory Underpinnings. Under two major enactments — the Inspector General Act of 1978 (92 Stat. 1101-1109) and the Inspector General Act Amendments of 1988 (102 Stat. 2515-2530) — IGs have been granted a substantial amount of independence and authority to carry out their basic mandate. Each office is headed by an inspector general who is appointed and removable in one of two ways: (1) presidential appointment, subject to the advice and consent of the Senate, and presidential removal in specified federal establishments, including all cabinet departments and larger federal agencies; and (2) agency head appointment and removal in designated federal entities (DFEs), usually smaller boards, foundations, commissions, and corporations.

Coordination and Control. Statutory OIGs have also been affected by several presidential orders designed to improve coordination among the offices and to provide a means for investigating charges of wrongdoing among the IGs themselves and other top echelon officers.

---

[750] Separate from the 56 offices directly under the Inspector General Act of 1978, as amended, are three others, which, for the most part, are modeled after the provisions of the basic IG Act. P.L. 101-193 (103 Stat. 1711-1715) created an OIG in the Central Intelligence Agency, whose IG is appointed by the President by and with the consent of the Senate. P.L. 100-504 (102 Stat. 2530) established an office in the Government Printing Office, the only legislative branch entity with such a statutory IG; in this case, the inspector general is appointed by the head of the agency, the Public Printer. In addition, P.L. 108-106 established an office in the new Coalition Provisional Authority (in Iraq), whose IG is appointed by the Secretary of State. For background information on the offices and their evolution, see the citations in the "Selected Source Reading" at the end of this section.

In 1981, President Ronald Reagan established the President's Council on Integrity and Efficiency (PCIE) as a mechanism to coordinate and enhance efforts to promote integrity and efficiency in government programs and to detect and prevent waste, fraud, and abuse.[751] Chaired by the Deputy Director of the Office of Management and Budget (OMB), PCIE was composed of the statutory IGs at the time plus other appropriate officials from the Office of Personnel Management, Federal Bureau of Investigation, and the Departments of Defense, Justice, and the Treasury, among others. The membership has since been expanded to include the Comptroller of the Office of Federal Financial Management (an officer in OMB), the Director of the Office of Government Ethics, and the Special Counsel in the Office of Special Counsel. In 1992, following the expansion of IGs to designated federal entities, a parallel Executive Council on Integrity and Efficiency (ECIE) was created for IGs in these entities along with other appropriate officials.[752]

Concerns about allegations of wrongdoing by IGs or other high-ranking OIG officials themselves prompted the creation of a new mechanism to investigate such charges. In 1996, President William Clinton established an Integrity Committee, composed of PCIE and ECIE members and chaired by the FBI representative, to receive such allegations; if deemed warranted, these would be referred for investigation to an executive agency with appropriate jurisdiction, including the FBI, or to a special investigative unit consisting of council members.[753]

Major Provisions

Purposes. Three principal purposes or missions guide the OIGs:

- conduct and supervise audits and investigations relating to the programs and operations of the establishment;
- provide leadership and coordination and recommend policies for activities designed to: (a) promote economy, efficiency, and effectiveness in the

[751] Executive Order 12301, issued Mar. 26, 1981.

[752] Both PCIE and ECIE now operate under Executive Order 12805, issued by President George H.W. Bush on May 11, 1992. A proposal to codify the two councils has arisen in the 108th Congress. H.R. 3457 would combine them in statute, creating a new Council of the Inspectors General on Integrity and Efficiency. The General Accounting Office (GAO) surveyed the IGs in 2002, about codification of the IG councils and other matters, and found that a majority of IGs interviewed (34 of 53) "indicated that it was important for the PCIE and ECIE to be established in statute." See U.S. General Accounting Office, Inspectors General: Office Consolidation and Related Issues, GAO-02-575, Aug. 2002, p. 44.

[753] Executive Order 12993, issued by President William Clinton on Mar. 21, 1996.

administration of such programs and operations; and (b) prevent and detect fraud and abuse in such programs and operations; and
- provide a means for keeping the head of the establishment and Congress fully and currently informed about problems and deficiencies relating to the administration of such programs and operations, as well as the necessity for and progress of corrective action.

Appointment, Removal, and General Supervision. Differences in the appointment and removal procedures for IGs exist between those in federal establishments versus those in designated federal entities (see the following section for definitions), although with only a few exceptions, all IGs serve only under the "general supervision" of the agency head.

IGs in Federal Establishments. The President appoints IGs in federal establishments (i.e., cabinet departments and larger federal agencies) by and with the advice and consent of the Senate. The statute also provides that the selection be done without regard to political affiliation and solely on the basis of integrity and demonstrated ability in accounting, auditing, financial analysis, law, management analysis, public administration, or investigations.

The IG Act, as amended, provides that an inspector general may be removed from office only by the President, who then must communicate the reasons for removal to both houses of Congress. There are no explicit restrictions on the President's authority; removal may be with or without cause.

Each inspector general "must report to and be under the general supervision of" the establishment head or, to the extent this authority is delegated, to the officer next in rank below the head, and shall not report to, or be subject to supervision by, any other officer. The restriction on supervision is reinforced by another provision: "Neither the head of the establishment nor any other officer shall prevent or prohibit the Inspector General from initiating, carrying out, or completing any audit or investigation, or from issuing any subpoena."

Exceptions to this prohibition are few and are spelled out with regard just to certain departments and for specified reasons. Only the heads of the Departments of Defense, Homeland Security, Justice, and the Treasury, along with the U.S. Postal Service, are authorized to prohibit an IG audit, investigation, or issuance of a subpoena which requires access to information concerning ongoing criminal investigations, sensitive operational plans, intelligence matters, counterintelligence matters, and other matters the disclosure of which would constitute a serious threat to national security. (Under separate statutory authority, the Director of Central Intelligence has similar power over the Central Intelligence Agency's (CIA's) Inspector General.) Should the agency head exercise this power limiting the IG's discretion and activities, the reasons must be communicated to the IG and then by the inspector general to specified committees of Congress.

The IG Act also provides for two assistant inspectors general within each IG office in the specified federal establishments: i.e., an Assistant Inspector General for Audits and an Assistant Inspector General for Investigations.

IGs in Designated Federal Entities. The 1988 Amendments to the IG Act provide for appointment, removal, and supervision of inspectors general in "Designated Federal Entities," such as the Consumer Product Safety Commission, Federal Communications Commission, Federal Labor Relations Authority, Securities and Exchange Commission, and other usually smaller boards, commissions, corporations, and foundations. The U.S. Postal Service, a public corporation and the government's largest civilian employer, is also a designated federal entity.

The appointment and removal powers over IGs in designated federal entities differ from those governing their counterparts in federal establishments. The IGs in designated entities are appointed by the agency head, who also may remove or transfer the IG; when removing or transferring the IG, the head must promptly communicate in writing the reasons for such action to both houses of Congress. Several caveats to these usual procedures apply to the inspector general in the U.S. Postal Service. This officer is appointed by the Board of Governors and is the only IG with a specified term of office (i.e., seven years). He or she may be removed by the written concurrence of at least seven governors and then only for cause, another distinguishing characteristic from all other statutory inspectors general.

As with the presidentially appointed inspectors general, IGs in the designated federal entities are required to report to and be under the "general supervision" of the agency head. But neither the head nor any other officer is permitted to interfere with an IG audit, investigation, or issuance of a subpoena.

Appropriations and Resources. The 1988 Amendments to the IG Act granted each office of inspector general in a federal establishment a separate appropriation account (31 U.S.C. § 1105(a)(25)), in order to protect its funding level once it had been established by Congress. The OIGs in designated federal entities lack the same appropriations protection.

All IGs have authority to call on other governmental entities for assistance and to hire their own staff. Adequate facilities, equipment, supplies, and other basic resources are to be provided by the host agency. In addition, IGs have access to a Criminal Investigator Academy to train their personnel and an Inspector General Forensic Laboratory (P.L. 106-422).

Duties. Following the act's broad mandates, each inspector general is required to perform specific duties in order to achieve the goals of detecting and preventing waste, fraud, and abuse. These duties illustrate the IG's unique role within the agency and the broad grant of authority delegated by Congress. The IGs are expected to:

- provide policy direction for, and conduct, supervise, and coordinate audits and investigations;
- review existing and proposed legislation and regulations relating to programs and operations;
- make recommendations in the reports concerning the impact of the laws;
- recommend policies for, and conduct, supervise, or coordinate other relevant activities of the establishment;
- recommend policies for, and conduct, supervise, or coordinate relationships with federal agencies, with state and local agencies, and with nongovernmental entities with regard to identifying and prosecuting participants in fraud or abuse; and
- report expeditiously to the Attorney General whenever an inspector general has reasonable grounds to believe that there has been a violation of federal criminal law.

Reporting and Notification Requirements. Complementing the obligation to keep the agency head and Congress "fully and currently informed," IGs are required to make two basic types of reports to the agency head and Congress and to keep them informed through other means.

Semiannual Reports. Inspectors general are required to make semiannual reports, summarizing the OIG's activities for the previous six months, itemizing waste, fraud, and abuse problems, and identifying proposals for corrective action. The 1988 amendments refined and enhanced several of the semiannual reports' ingredients. For example, reports must contain certain entries, some of which include:

- a description of significant problems, abuses, and deficiencies relating to programs and operations;
- a description of recommendations for corrective action;
- an identification of each significant recommendation contained in the previous reports on which corrective action has not been completed; and,
- statistical information relating to costs, management of funds, and related matters.

The IG reports go directly to the agency head, who must transmit them unaltered to appropriate congressional committees within 30 days. After another 60 days, such reports are made available to the public. The agency head is authorized to append comments and specific data and information to the IG reports; this additional information includes statistical tables showing audit reports and dollar value of recommendations of disallowed costs and projected savings of recommendations for funds which could be put to a better use.

This periodic reporting requirement is affected by the Reports Consolidation Act (RCA) of 2000 (P.L. 106-531), approved at the end of the 106th Congress. The enactment encourages the consolidation of financial and performance

management reports within departments and agencies into a single annual report, in order to enhance coordination and efficiency within them; improve the quality of relevant information; and provide it in a more meaningful and useful format for Congress, the President, and the public. As part of this overall plan, RCA provides that the consolidated annual report include a statement from the agency's inspector general; it is to describe the agency's most serious management and performance challenges — the so-called "top 10" challenges that IGs have been identifying over the previous three years — and briefly assess the agency's progress in addressing them. The IG's statement must be submitted to the agency head at least 30 days before it is due; he or she may comment upon it but not change it.

Seven-Day Letter Reports. The Inspector General Act also requires the IG to report immediately to the agency head whenever the inspector general becomes aware of "particularly serious or flagrant problems, abuses, or deficiencies relating to the administration of programs and operations." Such communications must be transmitted — unaltered but allowing for comments the head deems appropriate — by the agency head to the appropriate congressional committees within seven days.

The Intelligence Community Whistleblower Protection Act, as amended, reinforces such notifications.[754] It covers all employees in the intelligence community who want to bring an "urgent concern" based on classified information to the attention of Congress. The process to accomplish this is elaborate and complex — with the inspector general playing a key role in reviewing and transmitting the information to the House and Senate Select Committees on Intelligence, the exclusive recipients — to protect the material from unauthorized disclosure while recognizing the right of Congress (and the agency head) to be notified of such urgent concerns.

Other Notification Provisions. Additionally, the act requires an inspector general to keep the agency head and Congress "fully and currently informed by means of the reports [described above] and otherwise." This concept of keeping the head and Congress informed "otherwise" includes a variety of mechanisms: testifying at congressional hearings, meeting with lawmakers and staff, and responding to requests for information or reports from Congress or its committees.

Authority. In order to carry out the purposes of the law, Congress has granted the inspectors general broad authority. Section 6 of the codified legislation authorizes the IGs, among other things:

---

[754] Codified at 5 U.S.C. Appendix 8H for all agencies directly under the Inspector General Act of 1978 and at 50 U.S.C. § 403q(d)(5) for the CIA.

- to conduct audits and investigations and make reports relating to the administration of programs and operations;
- to have access to all records, reports, audits, reviews, documents, papers, recommendations, or other materials which relate to programs and operations with respect to which the IG has responsibilities under the enactment;
- to request assistance from other federal, state, and local government agencies;
- to issue subpoenas for the production of all information, documents, reports, answers, records, accounts, papers, and other data and documentary evidence necessary to perform the IG's functions;[755]
- to administer to or take from any person an oath, affirmation, or affidavit;
- to have direct and prompt access to the agency head;
- to select, appoint, and employ officers and employees in order to carry out the functions, powers, and duties of the office of the inspector general;
- to obtain the services of experts and consultants on a temporary or intermittent basis, as authorized by 5 U.S.C. § 3109; and
- to enter into contracts and other arrangements for audits, studies, and other services with public agencies as well as private persons, and to make such payments as may be necessary to carry out the law.

The scope of the IGs' investigative authority is seen further in the range of matters the IG may investigate stemming from an employee complaint or disclosure of information. The inspector general is authorized to receive and investigate complaints or information from an employee concerning the possible existence of an activity constituting a violation of law, rules, or regulations, or mismanagement, gross waste of funds, abuse of authority, or a substantial and specific danger to the public health and safety. In such instances, the inspector general shall not disclose the identity of the employee without the employee's consent, unless the IG determines that such disclosure is unavoidable during the course of the investigation. The law also prohibits any reprisals against employees who properly make complaints or disclose information to the IG.

Inspectors general in the federal establishments now have independent law enforcement authority in law (P.L. 107-296). Previously, the criminal investigators in these OIGs had acquired such powers in several different ways: through existing offices that have been transferred to the OIG; through statutory grants affecting specific agencies and jurisdictions; and through special deputation by the U.S. Marshals Service in the Department of Justice. These grants and the attendant processes, however, were seen as cumbersome and time-consuming as well as being limited in scope and duration; the result was an unequal set of powers among OIGs.

---

[755] This section does not permit the IG to use the subpoena power to obtain documents and information from other federal agencies (5 U.S.C. App. 3, § 6).

Notwithstanding these broad powers, inspectors general are not authorized to take corrective action or institute changes themselves. Indeed, the 1978 act specifically prohibits the transfer "of program operating responsibilities" to an inspector general.

Discussion

Statutory inspectors general have been granted a substantial amount of independence, authority, and resources to combat waste, fraud, and abuse in federal programs and operations. The IGs' broad mandate allows them flexibility for the responsibilities they emphasize and the roles they adopt. Their activities can focus on investigations or audits, and increasingly inspections (or program evaluation), depending upon their job orientation, their expertise and experience, the types of programs and operations within the agency, and the problems they perceive. Their roles, moreover, can cross a wide spectrum of possibilities. These can range from a proactive, preventive role, in which the IG functions as an "insider," working closely with management to upgrade agency operations, to an ad hoc reactive, detection role, in which the IG functions as an "outsider," investigating and uncovering illegalities and other misconduct.

Inquiries and concerns have existed about the IGs and their operations: whether certain individual offices and particular IGs are effective, and how this effectiveness is measured and compared. Calls for additional statutory authority — such as testimonial subpoena power — and other enhancements have also been expressed. Proposals relating to the IG community include prescribing a term of office (e.g., seven or 10 years) for IGs in designated federal entities, to help reduce their high turnover rate; changing IG budget submission procedures; making the PCIE and ECIE statutory or combining the two; extending offices to certain agencies which lack one now; transforming some posts in which the IG is appointed by the agency head to one appointed by the President (with Senate advice and consent); placing offices in several designated federal entities under one inspector general or placing one or more of the designated federal entities under the jurisdiction of an IG in a federal establishment; and merging the two statutory offices in the Treasury Department (the Treasury Inspector General for Tax Administration, who covers the Internal Revenue Service, and the Treasury IG who handles the remainder of the department).[756]

Selected Source Reading

---

[756] H.R. 3457, 108th Congress, for instance, would set a term of office for the IGs; allow their removal "for cause", provide for the submission of the IG budget requested amount to OMB and Congress, for comparative purposes; set up a combined Council of the Inspector Generals on Integrity and Efficiency; and provide for personnel flexibilities in office of the inspector general (OIG) hirings, pay, promotion, and reductions in force.

Duffy, Diane T. and Frederick M. Kaiser. "Into the Woods: Mapping New Directions for OIGs." Journal of Public Inquiry, vol. 1 (fall/winter 1999), pp. 27-32.

Hendricks, Michael, Michael F. Mangano, and William C. Moran, eds. Inspectors General: A New Force in Evaluation. San Francisco: Jossey-Bass Inc., 1990.

Journal of Public Inquiry (A Publication of the Inspectors General of the United States) Washington: GPO, serial publication.

Kaiser, Frederick M. "The Watchers' Watchdog: The CIA Inspector General." International Journal of Intelligence and Counterintelligence, vol. 3 (1989), pp. 55-75.

Light, Paul C. Monitoring Government: Inspectors General and the Search for Accountability. Washington: The Brookings Institution, 1993.

Newcomer, Kathryn E. "The Changing Nature of Accountability: The Role of the Inspector General in Federal Agencies." Public Administration Review, vol. 58 (March/April 1998), pp. 129-136.

U.S. Congress. House. Committee on Government Operations. The Inspector General Act of 1978: A Ten-Year Review. H.Rept. 100-1027. 100th Congress, 2nd session. Washington: GPO, 1988.

——. Subcommittee on Government Management, Information, and Technology. The Inspector General Act of 1978: Twenty Years After Passage, Are the Inspectors General Fulfilling Their Mission?. Hearings. 105th Congress, 2nd session. Washington: GPO, 1999.

——. Subcommittee on Government Efficiency. 25th Anniversary of the Inspector General Act. Hearings. 108th Congress, 2nd session. Washington: GPO, 2003.

U.S. Congress. Senate. Committee on Governmental Affairs. Oversight of the Operation of the Inspector General Offices. Hearings. 101st Congress, 2nd session. Washington: GPO, 1990.

——. The Integrity and Effectiveness of the Offices of Inspector General. Hearings. 102nd Congress, 2nd session. Washington: GPO, 1992.

——. The Inspector General Act: 20 Years Later. Hearings. 105th Congress, 2nd session. Washington: GPO, 1998.

——. Inspector General Act Amendments of 1999. S.Rept. 106-510. 106th Congress, 2nd session. Washington: GPO, 2000.

——. Legislative Proposals and Issues Relevant to the Operations of the Inspector General. Hearings. 106th Congress, 2nd session. Washington: GPO, 2000.

U.S. General Accounting Office. Inspectors General: Office Consolidation and Related Issues. GAO-02-575. August 2002.

CRS Report 98-379 GOV. Statutory Offices of Inspector General: Establishment and Evolution, by Frederick M. Kaiser.

CRS Rept. 98-141 GOV. Statutory Offices of Inspector General: A 20th Anniversary Review, by Frederick M. Kaiser (1998).
Frederick M. Kaiser

B. Government Performance and Results Act of 1993

Statutory Intent and History

Congress's stated intent in enacting the Government Performance and Results Act of 1993 (GPRA or the "Results Act"; P.L. 103-62; 107 Stat. 285),[757] was to direct agencies to (1) clarify their program responsibilities and become more cost efficient; (2) account for the performance and outcomes of their activities and programs; and (3) improve management. The legislation reflected Congress's desire to reduce budget deficits and improve congressional decision making by using information about whether statutory objectives are achieved, and about the effectiveness and efficiency of federal programs and spending. The law requires agencies to move from defining budgets in terms of inputs and program outputs, to focus on outcomes and results.[758] Agencies are required to set goals, generate information and reports needed to measure program performance, and move toward performance budgeting. The National Performance Review, state government experiences with performance budgeting, and the "total quality management" (TQM) movement contributed to congressional interest in performance management and budgeting.

The "Results Act" was one of several major pieces of legislation enacted in the 1990s that were intended to improve management and accountability in federal agencies. The others, detailed elsewhere in this compendium, included the Chief Financial Officers Act of 1990 (104 Stat. 2838) that provided for the establishment of chief financial officers (CFOs) in the 24 largest federal departments and agencies, which together control about 98% of the government's gross budget authority. The Government Management Reform Act of 1994 (110 Stat. 3410) required all CFO agencies to prepare and have audited financial statements for their operations beginning with FY1996. The Information Technology Management Reform Act of 1996 (110 Stat. 679, later renamed the Clinger-Cohen Act of 1996, 110 Stat. 3009393) requires agencies to establish performance measures to evaluate how their information technology activities support agency program efforts.

Major Provisions

---

[757] Codified at 5 U.S.C. prec. § 301, § 306; 31 U.S.C. § 1101 & nt, § 1105, §§ 1115-1119, prec. § 9701, §§ 9703-9704; 39 U.S.C. prec. § 2001, §§ 2801-2805.

[758] The statute defines output measure as "the tabulation, calculation, or recording of activity or effort and can be expressed in a quantitative or qualitative manner." Outcome measure means "assessment of the results of a program activity compared to its intended purpose" (Sec. 4(f)).

GPRA directs agencies with budgets over $20 million[759] to develop, in consultation with Congress and other stakeholders, long-term goals and six-year strategic plans to be revised every three years; to set annual performance goals and develop annual performance plans based on the strategic goals; and to report annually on actual performance compared to the targets. Federal agencies started to submit annual performance plans to Congress beginning with the FY1999 budget cycle. The Office of Management and Budget (OMB) submitted the first annual government-wide performance plan with the President's FY1999 budget. The performance report cycle began in 2000 with reports covering FY1999. Quantitative measures are required except when OMB approves non-quantitative alternatives (as outlined in the statute) for programs that cannot be expressed "in an objective, quantifiable, and measurable form ...."

Anticipating bureaucratic obstacles and the need to alter traditional procedures, budget, and reporting systems, Congress recognized that successful implementation of GPRA would require major changes in agencies' cultures and procedures. Thus, Congress phased in GPRA over a seven-year period and authorized pilot projects. Congress attempted to avoid top-down OMB control, and allowed each agency to develop a performance measurement process that conforms to its unique functions. Only federal employees may prepare strategic plans, performance plans, and reports, since these activities are "inherently governmental functions." In addition, guidance issued by OMB admonishes agencies to keep costs down and not increase paperwork.

In statutorily required reports that used the results of the pilot projects, OMB did not recommend changes to the law, and GAO reported that agency implementation varied in quality, utility, and responsiveness, but that improvements could be made.[760] In a letter to Congress, January 18, 2001, reporting as mandated by P.L. 103-62, OMB declined to recommend to Congress that performance budgeting be required statutorily.[761]

---

[759] Except for the Central Intelligence Agency, General Accounting Office, Panama Canal Commission, and the U.S. Postal Service (which is governed by separate, but similar, provisions of the same law).

[760] U.S. Office of Management and Budget, The Government Performance and Results Act, Report to the President and the Congress, May 1997; and U.S. General Accounting Office, The Government Performance and Results Act,1997 Government-wide Implementation Will Be Uneven, GGD-97-109, June 1997.

[761] U.S. Office of Management and Budget, Report to the Hon. J. Dennis Hastert, from Jacob J. Lew, Jan. 18, 2001, and CRS Report RL32164, Performance Management and Budgeting in the Federal Government: Brief History and Recent Developments, by Virginia A. McMurtry.

Major changes to GPRA have been accomplished both by statute and by administrative directive. The Reports Consolidation Act of 2000[762] authorized agencies to combine annual performance reports with financial reports required under the CFO Act. The following year OMB made the consolidation mandatory and set forth a schedule of accelerated deadlines.[763] The performance and accountability reports covering FY2003 were due by January 30, 2004, and beginning with FY2004, the consolidated reports are due by November 15, 2004. The Federal Financial Assistance Management Improvement Act of 1999[764] requires federal agencies and non-federal entities that are recipients of federal financial assistance to set annual goals and to measure compliance relating to efficiency and coordination, delivery of services, and simplification of processing as part of the agency's compliance with GPRA. Most recently, GPRA was amended by the Homeland Security Act of 2002.[765] Agencies are required to augment desciptions in their annual performance plans regarding how they will achieve their performance goals and objectives[766] by also describing the "strategies" and "training" that are required to meet those goals and objectives. In addition, the agency chief human capital officers (CHCOs) established by the Homeland Security Act are required to prepare this portion of agency annual performance plans.[767] The amendment to GPRA also requires agencies to review, in their annual program performance reports, their performance relative to their strategic human capital management.[768]

Significant changes relating to GPRA have also occurred through the annual revisions to OMB Circular No. A-11, "The Preparation, Submission, and Execution of the Budget."[769] In 1995 OMB for the first time issued Part 2, "Preparation and Submission of Strategic Plans," to OMB Circular No. A-11. By 1999, Part 2 covered "Preparation and Submission of Strategic Plans, Annual Performance Plans, and Annual Program Performance Reports." Among the

---

[762] P.L. 106-531, 114 Stat. 2537.

[763] U.S. Office of Management and Budget, Form and Content of Agency Financial Statements, Bulletin No. 01-09, Sept. 25, 2001.

[764] P.L. 106-107, 113 Stat. 1486.

[765] As provided by the Chief Human Capital Officers Act of 2002, enacted as Title XIII of the Homeland Security Act of 2002 (P.L. 107-296; 116 Stat. 2289).

[766] As required by 31 U.S.C. § 1115(a)(3).

[767] See the discussion of Title 5 U.S.C. Chapter 14, elsewhere in this compendium, for more on the establishment and duties of agency CHCOs.

[768] 31 U.S.C. § 1116(d)(5).

[769] A current version of Circular No. A-11 is available electronically at [http://www.whitehouse.gov/omb/circulars/index.html], visited Jan. 22, 2004.

changes made in June 2002 (now found in A-11, Part 6) were requirements that agency annual performance plans include performance goals used in assessments of program effectiveness, that agencies restructure their budget accounts and substitute outputs and outcomes for the current lists of program activities in program and financing schedules, and that agencies integrate performance and budget in performance plans. The revision of A11 in July 2003 requires agencies to prepare performance budgets for FY2005 and to incorporate their GPRA performance plans into their budget requests.

Discussion

A number of congressional hearings and reports overseeing implementation of the law have been produced since 1993.[770] For instance, a committee report on FY1999 performance plans concluded that the plans were "disappointing." It noted that the strategic plans did not lay a good foundation for performance plans; that agencies did not deal with major management problems, lacked reliable data to verify and validate performance, and often did not give results-oriented performance measures; and that many performance measures were not linked to day-to-day activities. The report found that a "culture change" was required to ensure implementation.[771] A report by former Chairman Thompson of the Senate Governmental Affairs Committee critiqued FY1999 performance reports and observed that most do not "inform Congress and the public about what agencies are doing and how well they are doing it."[772]

GAO has published assessments of individual agency GPRA performance plans and reports and has summarized its assessments in a variety of reports and testimony.[773] The House Subcommittee on Government Efficiency, Financial

---

[770] CRS Report RS20257, Government Performance and Results Act: Brief History and Implementation Activities, by Genevieve J. Knezo.

[771] Rep. Dick Armey, Sen. Larry Craig, Rep. Dan Burton, Rep. Bob Livingston, and Rep. John Kasich, The Results Act: It's the Law; the November 1997 Report. (Document available from CRS upon request.)

[772] U.S. Congress, Senate Committee on Governmental Affairs, Management Challenges Facing the New Administration, committee print, report of Senator Fred Thompson, Chairman, 106th Cong., 2nd sess., Oct. 2000, S.Prt. 106-62 (Washington: GPO, 2000).

[773] For individual plans, see "Reports on the Government Performance and Results Act," available at [http://www.gao.gov/], visited Jan. 22, 2004. See also U.S. General Accounting Office, Managing for Results: Using GPRA to Help Congressional Decisionmaking and Strengthen Oversight, T-GGD-00-95, Mar. 22, 2000; and David Walkier, statement of the Comptroller General of the United States, "Results-oriented Government; Using GPRA to Address 21st Century Challenges," in hearing on What Happened to GPRA? A Retrospective Look at Government Performance and Results, Sept. 18, 2003, available at: [http://reform.house.gov/GovReform/Hearings/EventSingle.aspx?EventID=408], visited Dec. 18, 2003.

Management and Intergovernmental Relations held a hearing on "The Results Act: Has It Met Congressional Expectations?" (June 19, 2001). Compliance with GPRA was identified as a major management challenge in Government at the Brink, Urgent Federal Government Management Problems Facing the Bush Administration, released by Senator Fred Thompson.[774]

To mark the 10-year anniversary of enactment of the law, hearings were held by the Subcommittee on Government Efficiency and Financial Management of the House Committee on Government Reform in April 2003,[775] and by the full House Committee on Government Reform in September 2003.[776] Many of the themes enunciated in the earlier reports have continued to resonate throughout the 10 years since enactment. For instance, reporting on GPRA in the FY2004 budget request, OMB said:

Unfortunately, the implementation of this law has fallen far short of its authors' hopes. Agency plans are plagued by performance measures that are meaningless, vague, too numerous, and often compiled by people who have no direct connection with budget decisions. Today, agencies produce over 13,000 pages of performance plans every year that are largely ignored in the budget process.[777]

There is also criticism that Congress does not use performance and results information in authorizing programs or appropriating funding for them.[778] A January 2002 GAO report, Managing for Results: Agency Progress in Linking Performance Plans with Budgets and Financial Statements, said that three-fourths of federal agencies were connecting performance planning, budgeting and financial reporting at aggregated goal levels, but that more links were required at

---

[774] Sen. Fred Thompson, Committee on Governmental Affairs, Government at the Brink, 2 vol. (Washington: June 2001), available at [http://www.senate.gov/~gov_affairs/], visited Jan. 22, 2004, from the "Committee Documents" menu, under "Reports." See also Sen. Fred Thompson, "Thompson Unveils Agency Performance Report Grades," press release, Oct. 30, 2000. (Document available from CRS upon request.)

[775] U.S. Congress, House Committee on Government Reform, Subcommittee on Government Efficiency and Financial Management, Performance, Results, and Budget Decisions, 108th Cong., 1st sess., Apr. 1, 2003, p.73.

[776] U.S. Congress, House Committee on Government Reform, What Happened to GPRA? A Retrospective Look at Government Performance and Results, available at: [http://reform.house.gov/GovReform/Hearings/EventSingle.aspx?EventID=408], visited Dec. 18, 2003.

[777] U.S. Office of Management and Budget, Budget of the United States Government, Fiscal Year 2004, p. 49.

[778] This topic was discussed in statements by witnesses from OMB and GAO, and by the committee chairman in U.S. Congress, What Happened to GPRA? A Retrospective Look at Government Performance and Results.

specific program levels to assist in internal management and congressional decision making.

President George W. Bush's report, The President's Management Agenda (August 2001), stressed results-oriented management and included budget and performance integration as one of five government-wide initiatives.[779] Performance was an important theme in the FY2003 budget request when the Administration said it used performance analyses to make funding decisions for over 100 federal programs across all agencies. This represented the first time a President's budget submission formally attempted to link budget requests with program performance.[780]

The Bush Administration has developed a formal program assessment rating tool (PART) that agencies must use to evaluate program performance. This is intended to "...inform and improve agency GPRA plans and reports, and establish a meaningful, systematic link between GPRA and the budget process."[781] Programs are rated by agency managers and OMB staff according to questionnaires developed by OMB. Circular No. A-11 now requires that agencies' performance budgets include information from the PART assessments. The President's FY2004 budget included a separate volume, Performance and Management Assessments, which arrayed PART evaluations for 234 programs. Other parts of the budget contained information on "Rating the Performance of Federal Programs" and "Budget and Performance Integration." OMB's PART instructions for FY2005 subject an additional 20% of all programs to PART evaluations, with 100% of federal programs to be evaluated this way by FY2008. Critics of PART argue that the "subjectiveness" used in determining performance measures may lead to poor budget decision making practices.[782]

Some agencies have not yet adequately defined their goals, program objectives, expected outcomes, and results, and have not developed appropriate measures for them. It is difficult to develop quantitative or alternative measures for some program areas, for example, programs designed to support basic research or certain diffuse policy objectives. Concerns have been stated about the costs and benefits of developing new results-oriented performance measurement systems,

---

[779] For an overview of the President's Management Agenda, see CRS Report RS21416, The President's Management Agenca: A Brief Introduction, by Virginia A. McMurtry.

[780] "Rigorous OMB Performance Measures Will Be Used to Frame Agency Budget Proposals for FY2004," Washington Fax, Jan. 23, 2002; see the chapter on "Governing with Accountability," in U.S. Office of Management and Budget, Budget of the U.S. Government, Fiscal Year 2003.

[781] See OMB Memorandum M-02-10, July 16, 2002.

[782] S. Haley, "OMB Performance Pressures May Divert Agencies from Important Priorities, House Science Committee Minority Asserts," Washington Fax, Mar. 7, 2003.

about the lack of interagency coordination to use similar measures for similar programs, and about the need to link "Results Act" implementation to the everyday work of program mangers. Some critics recommend that Congress set clear performance goals in authorizing legislation,[783] set clear performance standards in appropriations legislation, and use PART to grade programs and help with funding decisions.

Other issues relate to the plausibility of achieving the intent of the statute, and to its fundamental assumptions and purposes. Some say that GPRA is a wasteful paperwork exercise since, typically, executive and legislative decisions about funding priorities and program continuation are based more on political debate and objectives and less on the kind of performance data that are intended to be generated from the GPRA mandates. Others believe performance management and budgeting are feasible, and assert that accountability and congressional control over the budget will increase as Congress uses objective, results-oriented information to oversee agencies and develop budget priorities.

Selected Source Reading

CRS Report RS20257. Government Performance and Results Act: Brief History and Implementation Activities, by Genevieve J. Knezo.

CRS Report RL32164. Performance Management and Budgeting in the Federal Government: Brief History and Recent Developments, by Virginia A. McMurtry.

Genevieve J. Knezo

[783] Philip Joyce, Linking Performance and Budgeting: Opportunities in the Federal Budget Process, IBM Center for The Business of Government, Oct. 2003, available at [http://www.businessofgovernment.org/pdfs/Joyce_Report.pdf], visited Dec. 18, 2003.

C. Clinger-Cohen Act of 1996

Statutory Intent and History

The Information Technology Management Reform Act (ITMRA; 110 Stat. 679;[784] 40 U.S.C. § 759) was incorporated as an amendment into the National Defense Authorization Act for Fiscal Year 1996 (110 Stat. 186). In October 1996, the name of this act was formally changed to the Clinger-Cohen Act (110 Stat. 3009; 31 U.S.C. § 3512) in recognition of its two principal sponsors. The law provides that each federal agency buy the best and most cost effective information technology available. Under the law, the General Services Administration's (GSA's) role as the central agency for information technology acquisition policy is repealed. Each federal agency is given responsibility for information technology acquisition and management with a Chief Information Officer (CIO) to help achieve this goal. Financial accounting and management responsibilities also are given to each federal agency. The purpose of the law is to streamline and improve information technology procurement policies at federal agencies, as well as give each federal agency the flexibility to make information technology purchases relevant to its mission.

The Clinger-Cohen Act replaced the Automatic Data Processing Act (79 Stat. 1127), the Brooks Act.[785] The Brooks Act, passed in 1965, was intended to address problems of "[p]assive, partial, or informal types of leadership" in the purchase, lease, maintenance, operation, and utilization of automatic data processing (ADP) by federal agencies. At that time ADP technology and its applications were still relatively new although their use was becoming more widespread; however, federal agencies were reporting that they were having greater difficulty complying with Bureau of the Budget regulations for annual agency-wide budget reviews.[786] The Brooks Act centralized and coordinated this process by giving the General Services Administration "operational responsibility" for ADP management, utilization and acquisition through a "revolving fund." (79 Stat. 1126).

In the years following its passage, however, advances in information technology and applications created problems for agencies operating under the Brooks Act. Policymakers, in turn, sought to redress problems that had arisen from a centralized federal acquisition, procurement, and financial accounting system. Increasingly, many viewed the Brooks Act as causing procurement delays, imposing standardized technology and application solutions, and mismatching technology solutions with agency missions. The Information Technology

---

[784] To be codified at 40 U.S.C. § 759 nt, § 1401 & nt, §§ 1411-1413, §§ 1421-1428, §§ 14411442, §§ 1451-1452, § 1461, §§ 1471-1475, §§ 1491-1492, §§ 1501-1503; 41 U.S.C. § 434.

[785] Named after its principal sponsor, former Rep. Jack Brooks.

[786] The Bureau of the Budget was the predecessor agency to the Office of Management and Budget (OMB), before OMB was established via Reorganization Plan No. 2 in 1970.

Management Reform Act (S. 946), introduced by Senator William S. Cohen, was considered bypolicymakers during the 104th Congress. S. 946 was intended to provide the executive branch with the flexibility to acquire technologies and services incrementally, enter into modular contracts with vendors rather than more costly longer-term contracts, and obtain information technologies and services that fit agency needs. A companion bill, identical to the Senate legislation, was introduced by Representative William Clinger (H.R. 830) in the House of Representatives. H.R. 830 was passed by the House of Representatives on February 22, 1995. After H.R. 830 was referred to the Senate, S.946 was substituted for the House legislation.

Many congressional policymakers sought to implement information technology acquisition and procurement management reform during the 104th Congress. Advocates saw an opportunity for implementing the reforms in S. 946 by incorporating the bill into the National Defense Authorization Act for Fiscal Year 1996 (S. 1124), as Division E of the legislation. Congressional policymakers had been interested in reforming and streamlining all Department Defense (DOD) acquisition and procurement processes. By incorporating S. 946 into the FY1996 DOD authorization bill, policymakers brought this reform to all federal agency information technology acquisition and procurement management. The final version of S. 1124 passed the House of Representatives on January 24, 1996, and the Senate on January 26, 1996. It was approved by President Clinton on February 10, 1996. (110 Stat. 679).

Major Provisions

The Clinger-Cohen Act contains extensive procedural, technical, and policy revisions of federal information technology acquisition and procurement management. These provisions can be summarized as (1) repeal of GSA's primary role in setting policy and regulations for federal information technology acquisition, while giving most of this responsibility to individual federal agencies; (2) creation of Chief Information Officers (CIOs) in federal agencies to provide advice to heads of agencies on policies to develop, maintain and facilitate information systems as well as help evaluate, assess, and report on these policies; (3) creation of a simplified, clear, and understandable process of information technology acquisition by federal agencies; and (4) initiation of two specific pilot programs which authorize federal agencies to enter into competitive contracts with the private sector.

The provisions creating the CIOs and establishing the pilot programs have received much attention. The creation of CIOs in federal agencies was based on a perceived need to decentralize federal procurement, application, and evaluation of information technologies, benefit overall government performance, and bring expertise to the federal agencies. The two pilot programs are intended to reward cost savings and performance. The first type of program is the Share-in-Savings pilot program. This program provides acquisition and procurement incentives to the private sector, in which a federal agency can pay private sector contractors an

amount equal to a portion of savings (the share-in-savings) achieved by the government. The second pilot program was the Solutions-Based Contracting pilot program. Under this program, executive branch acquisition of information technology must include criteria that incorporate objectives defined by the federal government as well as a streamlined contractor process. The private sector is allowed to provide solutions to effectively achieve agency objectives. The law also requires that simple and clear selection factors, communication, proposals, evaluation, and system implementation be used by the executive branch.

Discussion

Early oversight of the implementation of the Clinger-Cohen Act immediately following its passage and the departure of its sponsors from Congress was relatively limited.[787] However, as Congress has become increasingly interested in Internet, information technology, and e-government issues, some provisions of the Clinger-Cohen Act have received additional attention in the 107th and 108th Congresses.

One concern has been the recruitment and retention of CIOs. A shortage of qualified CIOs, and regular turnover of personnel, compounded by salary and compensation disparities between government and private sector opportunities, have raised concerns about the government's ability to maintain the momentum and continuity of major e-government and IT initiatives.[788] As IT projects have become more integrated into the function of a department or agency, the role of CIOs has evolved as well. CIOs are being called upon not only for their technological expertise, but also to provide strategic leadership in certain areas of policy, budget, and contract oversight.[789] The CIO's relationship with top-level department decisionmakers can also be critical to successfully implementing e-government initiatives. This suggests that in selecting a department-level CIO, one needs to consider the strengths and weaknesses of choosing a career employee, who may have a deeper contextual understanding of the mission and functions of an organization, and recruiting a candidate from the private sector, who may bring a wider range of experiences and perspectives to the position.[790]

---

[787] Some observers suggest this may have been partly the result of the act's principal sponsors' departure from Congress; in 1997, Senator William Cohen left Congress to become the Secretary of Defense, and Representative William Clinger retired.

[788] Diane Frank, "CIOs Find Crowded Agenda Wearing," Federal Computer Week, June 30, 2003, p. 8.

[789] Cynthia L. Webb, "Providing the Technology Vision," Washington Post, Mar. 6, 2003, available at [http://www.washingtonpost.com/wp-dyn/articles/A47136-2003Mar5.html], visited Dec. 3, 2003.

[790] Sara Michael, "Insider Information," Federal Computer Week, Apr. 14, 2003, p. 26.

Concerns have also been raised about organizational and budgetary obstacles possibly hindering CIO performance. The Clinger-Cohen Act requires that the CIO report directly to the agency head, and have information resource management as a primary function. However, in many cases, these requirements have not been met. Results from GAO studies of government CIOs within the first few years of the enactment of the Clinger-Cohen Act showed that it was not uncommon for CIOs to report to the Deputy Secretary or other agency head subordinates rather than directly to the Secretary. In addition, CIOs frequently wore several hats within their agencies.[791] Due to the apparent lack of more current studies, it is unclear how this situation has evolved in recent years.

The results of the two pilot programs have been mixed. In late 2002, the Solutions-Based Contracting program was repealed by Section 825 of the Bob Stump National Defense Authorization Act for Fiscal Year 2003 (P.L. 107-314). The reason cited in the conference report (H.Rept. 107-772) was that the legislative authority for the program "has never been used and is not likely to be needed." Similar concerns have been raised regarding the relative lack of use of the "share-in-savings" pilot program.[792] In a January 2003 report, GAO observed that "there are few documented examples of SIS contracting in the federal government."[793] One such example is the Department of Education's Office of Student Financial Assistance (OFSA), which has entered into a series of "share-in-savings" contracts with Accenture to modernize its computer systems.[794] While "share-in-savings" programs are considered by many to be forward-thinking policies with the potential to reduce spending and improve the quality of services, some experts contend that there are a number of obstacles to successfully instituting such programs. These include being able to determine baseline costs and an agency's willingness to give the contractor more control over the details (so the contractor will feel it has a chance to achieve the cost savings). Some observers have asserted that agencies believe Congress will reduce their

---

[791] U.S. General Accounting Office, Chief Information Officers: Ensuring Strong Leadership and an Effective Council, GAO-T-AIMD-98-22, Oct. 27, 1997; Information Technology: Update on VA Actions to Implement Critical Reforms, GAO-T-AIMD-00-74, Sept. 21, 2000; and Chief Information Officers: Implementing Effective CIO Organizations, GAO-T-AIMD00-128, Mar. 24, 2000.

[792] Similar concerns were not a significant focus of attention regarding the Solutions-Based Contracting pilot program.

[793] U.S. General Accounting Office, Contract Management: Commercial Use of Sharing-in-Savings Contracting, GAO-03-327, Jan. 2003, p. 3.

[794] Diane Frank, "Education Expands Share-in-Savings," Federal Computer Week, May 14, 2001, p. 44; Tanya N. Ballard, "Acquisition Officials Push Share-in-Savings IT Contracting," GovExec.com , Oct. 3, 2003, available at [http://www.govexec.com/dailyfed/1003/100303t1.htm], visited Oct. 4, 2003.

appropriations once the cost-savings is verified which, while saving the federal government money, will not provide any direct benefits to them (i.e., a reward). Hence, they believe the agencies have limited incentive to actively pursue such contracts. To help address some of these issues, Section 210 of the E-Government Act, signed into law in December 2002, includes provisions that temporarily allow an expanded use of "share-in-savings" contracts. The provision also provides incentives for agencies, such as the ability to retain a portion of the savings realized from the contract. However, at the time of this writing, implementing guidance from OMB is still forthcoming, and the provision expires in 2005.

While the Clinger-Cohen Act remains in effect and its provisions are still relevant to current agency IT management issues, the passage of the E-Government Act (discussed elsewhere in this compendium) represents a shift in the primary legislative vehicle being used to guide evolving federal information technology management practices and to promote initiatives to make government information and services available online. In doing so, it also represents a continuation of efforts to realize greater efficiencies and reduce redundancies through improved intergovernmental coordination, and by aligning information technology investments. As Congress continues to exercise its oversight role over e-government initiatives, it is anticipated that issues related to the intersection of these laws will also be raised.

Selected Source Reading

U.S. General Accounting Office. Government Reform: Using Reengineering and Technology to Improve Government Performance. GAO-T-OCG-95-2. February 2, 1995.

——. Information Technology Investment; A Governmentwide Overview. GAO/AIMD-95-208. July 1995.

——. Chief Information Officers: Ensuring Strong Leadership and an Effective Council. GAO-T-AIMD-98-22. October 27, 1997.

——. Contract Management: Commercial Use of Share-in-Savings Contracting. GAO-03-327. January 2003.

Jeffrey W. Seifert

III. Financial Management, Budget, and Accounting

A. Antideficiency Act

Statutory Intent and History

The so-called Antideficiency Act (33 Stat. 1214, and 34 Stat. 27; 31 U.S.C. §§ 1341-42) actually consists of a series of provisions and revisions incorporated into appropriations laws over the years relating to matters such as prohibited activities, the apportionment system, and budgetary reserves. These provisions, now codified in two locations in Title 31 of the United States Code, continue to play a pivotal role in the execution phase of the federal budget process, when the agencies actually spend the funds provided in appropriations laws.

The origins of the Antideficiency Act date back to the 19th century. The initial portion, enacted in 1870 as Section 7 of the General Appropriations Act for Fiscal Year 1871 (16 Stat. 251), provided:

... that it shall not be lawful for any department of the government to expend in any one fiscal year any sum in excess of appropriations made by Congress for that fiscal year, or to involve the government in any contract for the future payment of money in excess of such appropriations.

The intent was to prevent expenditures in excess of appropriations. Section 5 of the 1870 law also addressed the issue of congressional controls over budget execution, though not the question of preventing deficiencies. Instead, it provided that unexpended balances of appropriations accounts could only be applied to payment of expenses or contracts incurred during that year.

Major legislative provisions, often referred to as the Antideficiency Acts of 1905 and 1906, sought to strengthen the prohibitions of the 1870 law by expanding its provisions, adding restrictions on voluntary services for the government, and imposing criminal penalties for violations. Most importantly, the laws established a new administrative process for budget execution. This process, which remains in use today, is termed "apportionment" and results in the distribution of the budget authority provided in appropriations law to the agencies in installments, rather than all at once.

In order to provide against disproportionate spending rates by agencies, the 1905 legislation mandated that appropriations be "so apportioned by monthly or other allotments as to prevent undue expenditures in one portion of the year that may require deficiency or additional appropriations to complete the service of the fiscal year...." However, the fiscal discipline of this provision was weakened by language allowing apportionments to be "waived or modified in specific cases by the written order of the head of the Executive Department or other Government establishment having control of the expenditure...." (33 Stat. 1257-1258).

This exemption from apportionments by written order provided a broad loophole, widely used by department heads. The 1906 revision sought to tighten the waiver language by stipulating that apportionments could not be waived or modified "except upon the happening of some extraordinary emergency or unusual circumstance which could not be anticipated at the time of making such apportionment" (34 Stat. 48-49). Moreover, any waiver or modification of apportionment was to be justified in writing and communicated to Congress "in connection with estimates for any additional appropriations required on account thereof."

In 1933, with Executive Order 6166 issued pursuant to the Economy Act of 1933 (48 Stat. 16), authority for "making, waiving, and modifying apportionments of appropriations" was transferred from agency heads to the Director of the Bureau of the Budget (BOB).[795] However, BOB had earlier exerted control byadministrative means, such as a circular directing each agency to estimate an indispensable level of funding to carry out its activities. Following review by the Bureau and approval by the President, the remainder of the appropriation, or estimated savings, was to be designated a "General Reserve." So, the apportionment process came to have two objectives: to prevent deficiencies and to effect savings.

The continuing growth and complexity of the federal budget strained the existing system of administrative controls over funds. Eventually, another substantial revision of Antideficiency Act provisions occurred in 1950 (64 Stat. 595), largely based on recommendations in a report to Congress from the Bureau of the Budget and the General Accounting Office (GAO).[796]

The BOB/GAO report suggested that changing conditions during the fiscal year would always require some readjustments, but such changes could be expected to result in surpluses as well as deficiencies. The 1950 amendments incorporated this view and, for the first time, provided a statutory basis for budgetary reserves. The amendments also expanded upon the provisions of earlier regulations by stipulating four justifications for establishing reserves: (1) to provide for

---

[795] Dating to the Budget and Accounting Act of 1921, the Bureau of the Budget was originally located within the Department of the Treasury. The law authorized the President to appoint the director and assistant director of the bureau, however, signifying that it was essentially a presidential entity. When the Executive Office of the President was established in 1939, BOB was the first unit designated as a component. In 1970, BOB was reconstituted as the Office of Management and Budget (OMB).

[796] Report and Recommendations by the Director of the Bureau of the Budget and the Comptroller General of the United States with Respect to the Antideficiency Act and Related Legislation and Procedures. Submitted to Senator Styles Bridges, Chairman of Appropriations Committee, June 5, 1947. Typed manuscript. Cited by Louis Fisher in Presidential Spending Power (Princeton, NJ: Princeton University Press, 1975), p. 155. The provisions were enacted as a part of the general appropriations act for the fiscal year ending June 30, 1951.

contingencies; and to effect savings whenever savings are made possible by or through: (2) changes in requirements; (3) greater efficiency of operations; or (4) other developments subsequent to the date on which such appropriation was made available. The 1950 amendments further spelled out more detailed instructions for the operations of the apportionment process beyond the establishment of reserves, and for subdivision of apportionments at the agency level.

In the mid-1950s, Congress enacted a provision relating to the administration of the apportionment system by the agencies. This 1956 amendment simplified agency systems for subdividing funds by eliminating multiple pockets of funding authority, known as "allowances," so that administrative controls in the apportionment system would consist solely of allotments (P.L. 84-863, 70 Stat. 782). The following year, provisions relating to the apportionment system were further revised. The effect of the changes was to prohibit the request for apportionments or reapportionments necessitating a deficiency or supplemental estimate unless the agency head determined that such action fell within the exceptions expressly set out in the law (71 Stat. 440).

Major Provisions

Four main types of prohibitions are contained in the Antideficiency Act, as amended: (1) making expenditures in excess of the appropriation; (2) making expenditures in advance of the appropriation; (3) accepting voluntary service for the United States, except in cases of emergency; and (4) making obligations or expenditures in excess of an apportionment or reapportionment, or in excess of the amount permitted by agency regulation.

The limitations on expending and obligating amounts (31 U.S.C. § 1341) prohibit an officer or employee of the United States government or of the District of Columbia government from:

- making or authorizing an expenditure from, or creating or authorizing an obligation under, any appropriation or fund in excess of the amount available in the appropriation or fund unless authorized by law; and
- involving the government in any contract or other obligation for the payment of money for any purpose in advance of appropriations made for such purpose, unless the contract or obligation is authorized by law.

The limitations on voluntary services (31 U.S.C. § 1342) prohibit an officer or employee of the United States government or of the District of Columbia government from accepting voluntary services for the United States, or employing personal services in excess of those authorized by law, except in cases of emergency involving the safety of human life or the protection of property.

An entire subchapter (31 U.S.C. §§ 1511-1519) deals with the apportionment system. It contains provisions for definitions and application, for apportionment

and establishment of reserves, for officials controlling apportionments, for the administrative division of apportionments, and for authorized apportionments necessitating deficiency or supplemental appropriations. The subchapter further provides for exemptions, prohibited obligations and expenditures, and sanctions entailing adverse personnel actions and criminal penalties. The subchapter does not apply to Congress (the Senate; the House of Representatives; congressional committees; or a Member, officer, employee, or office of either house of Congress, or of the Office of the Architect of the Capitol) (31 U.S.C. § 1511(b)(3)).

The central enforcement provision is found in Section 1517. An officer or employee of an agency subject to apportionment is prohibited from making obligations or expenditures in excess of an apportionment or reapportionment, or in excess of the amount permitted by agency regulation. Violations are punishable by appropriate administrative discipline, including possible suspension from duty without pay or removal from office (Section 1518), and/or by criminal penalties, including a fine of not more than $5,000, imprisonment for not more than two years, or both (Section 1519).

Discussion

The framework for the apportionment process, as refined in the 1950 amendments, remains the basis for federal budget execution. However, evolution of the process continues, occasionally being modified by statute or executive order, but more frequently affected as a result of agency regulations, decisions of the Comptroller General, and other legal opinions.

The Impoundment Control Act (Title X of the 1974 Congressional Budget and Impoundment Control Act, 88 Stat. 297) amended the 1950 language regarding budgetary reserves in an effort to tighten control over executive branch discretion. The 1974 legislation served to delete the "other developments" justification contained in the 1950 amendments. Henceforth, reserves were to be established "solely to provide for contingencies, or to effect savings whenever savings are made possible by or through changes in requirements or greater efficiency of operations" (88 Stat. 332). Under the 1974 law, reserves were to be considered as a type of deferral, or temporary postponement of spending, in contrast to a rescission, or permanent cancellation.[797]

The prohibitions in the Antideficiency Act against spending monies in advance or in excess of appropriations sometimes lead to "funding gap" situations — when action on appropriations measures is not completed before the start of the new fiscal year and interim continuing resolutions lapse or are themselves delayed. For many years, agency officials generally maintained operations during periods

[797] A restatement of deferral authority was provided in the Balanced Budget and Emergency Deficit Reduction Reaffirmation Act of 1987 (101 Stat. 785-786).

of expired funding, while attempting to cut or postpone all non-essential obligations. Such action, while in technical violation of the Antideficiency Act prohibition on incurring obligations from Congress, was usually redressed by passing continuing resolutions effective retroactively to the beginning of the fiscal year.

The situation changed in the early 1980s with the issuance of two opinions by Attorney General Benjamin Civiletti concerning implications of the Antideficiency Act in instances of funding gaps.[798] According to these opinions, when appropriations lapse, federal managers are to act immediately to terminate the agency's normal operations in an orderly way; however, various exceptions in the Antideficiency Act allow some functions to continue. The Attorney General also stated that the Department of Justice would strictly enforce the criminal provisions of the act in cases of future violations.[799]

Selected Source Reading

Feld, Alan. "Shutting Down the Government." Boston University Law Review, vol. 69 (November 1989), p. 971 ff.

Huyser, Kevin J. "Anti-Deficiency Act." The Army Lawyer (January-February 2003), p. 218.

Sapp, David G. "Antideficiency Act Violations." Air Force Comptroller, vol. 32 (January 1998), pp. 4-9.

U.S. General Accounting Office. Office of General Counsel. Principles of Federal Appropriations Law, 2nd ed., vol. II. Washington: GAO, 1992, pp. 6.9 - 6.99.

Virginia McMurtry

---

[798] "Applicability of the Antideficiency Act Upon a Lapse in an Agency's Appropriations," 4 A Op. O.L.C. 16 (1980); "Authority for the Continuance of Government Functions During a Temporary Lapse in Appropriations," 5 Op. O.L.C. 1 (1981).

[799] See U.S. General Accounting Office, Funding Gaps Jeopardize Federal Government Operations, PAD-81-31, Mar. 3, 1981. The 1980 and 1981 Opinions of the Attorney General are included as appendices. The Budget Enforcement Act of 1990 (104 Stat. 1388573) amended Title 31 to further limit voluntary services allowable under the Antideficiency Act.

B. Budget and Accounting Act of 1921

Statutory Intent and History

The Budget and Accounting Act of 1921 (42 Stat. 20) grew out of Progressive Era views that saw legislatures as inherently corrupt, and sought to place more trust and more authority in executive and administrative institutions. The most important of several studies made on budgeting was that of President Taft's Commission on Economy and Efficiency (1910-1912). The commission's report, however, was virtually silent on the role of the legislature in the executive budget system it recommended, and its proposal languished in Congress. In spite of this, it remained on the national agenda, strongly supported by the Institute for Government Research (later the Brookings Institution), and support for an executive budget was included in presidential platforms by both Republicans and Democrats.[800]

During World War I, the administrative machinery of the federal government was severely taxed, giving new impetus to administrative reform in its aftermath. In 1919, Congress took up the issue of a national budget system, establishing select committees in both the House and Senate to hold hearings and make recommendations. The House Select Committee held 11 days of hearings in September and October 1919. The Senate Committee held four additional days of hearings in December 1919 and January 1920. Legislation embodying these recommendations was passed overwhelmingly in both chambers in 1920, but was vetoed by President Wilson, who questioned the constitutionality of a provision involving his removal power over the proposed office of Comptroller General. After the election of Warren G. Harding to the presidency in 1920, the bill was passed with only minor changes in the removal power provision, and signed into law as the Budget and Accounting Act of 1921.

Characterized as "probably the greatest landmark of our administrative history except for the Constitution itself,"[801] the Budget and Accounting Act established in law the duty of the President to submit each year a single, consolidated budget proposal for congressional consideration. The act stands as the foundation of the modern presidency because it made the President the administrative, as well as political, head of the executive branch. It meant that the President alone was responsible for making budget requests, so that each department and agency would no longer be able to act independently of presidential direction. The act also established the Bureau of the Budget (predecessor of the current Office of

---

[800] It was included in the Republican platform in 1916 and 1920, and the Democratic platform in 1920. In 1916 the Democrats had endorsed a return to consolidated control of appropriations in Congress, but not a presidential budget. See Donald Bruce Johnson, ed. National Party Platforms (rev. ed.), vol. 1, 1840-1956 (Urbana, IL: University of Illinois Press, 1978).

[801] Herbert Emmerich, Federal Organization and Administrative Management (Tuscaloosa, AL: University of Alabama Press, 1971), p. 40.

Management and Budget) to provide the President with the resources necessary to produce such a proposal, and the General Accounting Office, to provide Congress with the resources to ensure accountability.

Major Provisions

The Budget. Sections 201-206 of Title II of the Budget and Accounting Act establishes the requirements for the President to submit a budget proposal to Congress each year. Section 201 originally required the President to submit his budget on "the first day of each regular session [of Congress]." This requirement has been amended on several occasions (see below). Section 201 also lists requirements for the budget's contents, including estimates of expenditures "necessary in his judgment for the support of the Government for the ensuing fiscal year," except that estimates prepared by the legislative branch and the Supreme Court for their own expenditures should be included without revision. Other requirements include estimates of receipts for the ensuing fiscal year; estimates of expenditures and receipts for the fiscal year in progress, and expenditures and receipts of the last completed fiscal year; all essential facts regarding federal debt; and "such other financial statements and data as in his opinion are necessary or desirable." Sections 202-204 establish other requirements for the budget submission — requiring that the President make recommendations on managing any surplus or deficit (Section 202); providing for the transmittal of necessary supplemental estimates (Section 203); and specifying generally the form that estimates take (Section 204). Section 205 dealt with the submission of the FY1923 budget, the first under the act. Finally, Section 206 prohibits departments and agencies from submitting independent budget requests to Congress, as they had in the past, thus affirming the authority of the President as the head of the executive branch.

There has been no fundamental change in this part of the act, although there have been numerous modifications and additions. For example, the requirement in Section 201 that the President's budget be submitted "on the first day of each regular session" was amended by the Budget and Accounting Procedures Act of 1950 (64 Stat. 2317) to read "during the first fifteen days of each regular session." This was subsequently amended to "on or before the first Monday after January 3 of each year (or on or before February 5 in 1986)" by the Balanced Budget and Emergency Deficit Control Act of 1985 (99 Stat. 1037), and finally to "on or after the first Monday in January but not later than the first Monday in February of each year" by the Budget Enforcement Act of 1990 (104 Stat. 1388).

Likewise, the requirements of Section 201 concerning contents of the budget submission have been amended on several occasions, most notably by the Budget and Accounting Procedures Act of 1950, the Legislative Reorganization Act of 1970, the Congressional Budget and Impoundment Control Act of 1974, and the

Balanced Budget and Emergency Deficit Control Act of 1985. These are currently codified in Section 1105 of Title 31, U.S.C.[802]

The general authority of the President over the preparation and submission of the budget was reiterated and clarified in the Budget and Accounting Procedures Act of 1950.

Section 201 was amended by Section 221 of the Legislative Reorganization Act of 1970 to require a supplemental summary of the budget for the ensuing fiscal year to be submitted by June 1 of each year. This was further amended by the Congressional Budget Act to read "on or before July 15."

Section 201 was amended by Section 603 of the Congressional Budget Act of 1974 to require that budget projections be extended from the ensuing fiscal year to "the four fiscal years following the ensuing fiscal year."

Section 201 was amended by Section 605 of the Congressional Budget Act of 1974 to require the President to submit to Congress by November 11 of each year an estimate of budget outlays and proposed budget authority that would be included in the budget for the following year "if programs and activities of the United States Government were carried on during that year at the same level as the current fiscal year without a change in policy."

The Bureau of the Budget. Sections 207-217 of the Budget and Accounting Act established the Bureau of the Budget and delineated its powers and duties. Section 201 formally created the Bureau within the Treasury Department, provided for a director and assistant director, and stated that the Bureau, "under such rules and regulations as the President may prescribe, shall prepare for him the Budget, the alternative Budget, and any supplemental or deficiency estimates, and to this end shall have the authority to assemble, correlate, revise, reduce, or increase the estimates of the several departments or establishments." The newly created Bureau of the Budget went beyond these limited duties under the activist vision of its first director, Charles Dawes. In particular, it used the pre-existing apportionment process as a mechanism to extend its control over agency spending levels by means of administrative regulation.[803] By taking a hand in overseeing the execution of spending actions, as well as in the preparation of budget requests, the Bureau of the Budget exercised management functions from the beginning, and gave the President a strengthened capacity to administer the executive branch.

---

[802] For a listing of the requirements see U.S. General Accounting Office. The President's Budget Submission, AFMD-90-35, 1990, pp. 13-18 (Appendix II: Budget Information Required by Statute).

[803] The apportionment process was mandated under the Antideficiency Act of 1905 (P.L. 58217; 33 Stat. 1257-1258) to prevent deficiencies caused by disproportionate spending rates.

In 1939, the Bureau was made part of the newly created Executive Office of the President,[804] and in 1970 was reconstituted as the Office of Management and Budget.[805] The Chief Financial Officers Act of 1990 (104 Stat. 2838) initiated additional organizational changes within OMB. In particular, it created a new structure within OMB for federal financial management, headed by a new deputy director for management to serve as the federal government's chief financial officer. In addition, it included provisions intended to improve financial management practices generally.

The General Accounting Office. The third major provision of the Budget and Accounting Act was the establishment of the General Accounting Office.[806] The Treasury Act of 1789 established the Treasury Department with a Secretary, comptroller, auditor, treasurer, and register. Among his other duties, the comptroller was responsible for examining the accounts settled by the auditor. As part of the Budget and Accounting Act, Congress sought to establish an office to perform this examination function independent of the Department of the Treasury or the President. Title III abolished the office of comptroller of the Treasury and established the positions of Comptroller General and assistant comptroller general in its place. These new officers would be appointed by the President, with the advice and consent of the Senate, for 15-year terms, and could be removed from office only by joint resolution of Congress. The law transferred from the Treasury not only all powers and duties of the comptroller, but also the auditors, and the Division of Bookkeeping and Warrants, as well as their personnel, offices, and furniture.

In addition to independence, the act also granted substantial authority and responsibility to the Comptroller General. Section 312 provided that he shall investigate "all matters relating to the receipt, disbursement, and application of public funds, and shall make ... recommendations concerning the legislation he may deem necessary to facilitate the prompt and accurate rendition and settlement of accounts and concerning such other matters relating to the receipt, disbursement, and application of public funds as he may think advisable." The Comptroller General was further required to make such investigations and reports as ordered by either chamber of Congress or any committee, and to report

---

[804] U.S. President (Franklin Roosevelt), "Reorganization of the Executive Office of the President, Executive Order 8248, September 8, 1939," Public Papers and Addresses of Franklin Roosevelt, 1939 volume, War — and Neutrality, vol. 8, (New York: Macmillan, 1941), p. 490.

[805] U.S. President (Nixon), "Prescribing the Duties of The Office of Management and Budget and the Domestic Council in the Executive Office of the President," Executive Order 11541, 3 C.F.R. 1966-1970 Comp. (Washington: GPO, 1971), p. 939. For an overview of OMB, see CRS Report RS21665, Office of Management and Budget: A Brief Overview, by Clinton T. Brass.

[806] For an overview of GAO, see CRS Report RL30349, General Accounting Office and Comptroller General: A Brief Overview, by Frederick M. Kaiser.

to Congress on expenditures or contracts made in violation of law, and the adequacy and effectiveness of executive department fiscal practices.

Significant additions were made to the duties and authority of the General Accounting Office by the Legislative Reorganization Act of 1970 (84 Stat. 1140). Section 204 provided that the Comptroller General's responsibilities would include review and analysis of the results of government programs "including the making of cost benefit studies." Section 231 requires the General Accounting Office to provide any necessary assistance to congressional committees. Sections 232, 233, and 234 provide for the dissemination of reports to congressional committees and required notice that reports have been prepared. Section 235 limits the availability of General Accounting Office personnel to congressional committees. Section 236 requires that whenever the General Accounting Office makes a report which contains recommendations to the head of federal agency, the agency must respond to Congress with respect to the recommendations.

Discussion

There has been a continuous stream of interest in reforming the budget process in recent years, but the basic framework established by the Budget and Accounting Act of 1921 has been largely excluded from this deliberation. The role of the President and OMB in preparing budget requests, and the role of GAO in auditing expenditures, have not been seriously questioned, although there have been incremental changes and additions over the years. Rather, it has been in relation to financial management and administration that the act has been part of debates about reform. Notwithstanding the fact that the Chief Financial Officers Act of 1990 created a deputy director for management within OMB, the conflict between management and budgeting responsibilities has given rise to further proposals to divide these duties by creating an entirely new agency.

Selected Source Reading

Dawes, Charles G. The First Year of the Budget of the U.S. New York: Harper & Brothers, 1923.

Fisher, Louis. Presidential Spending Power. Princeton: Princeton University Press, 1975.

Mosher, Frederick C. A Tale of Two Agencies. Baton Rouge, LA: Louisiana State University Press, 1984.

Congress. House. Committee on Government Reform and Oversight. Making Government Work: Fulfilling the Mandate for Change. H.Rept. 104-435. 104th Congress, 1st session. Washington: GPO, 1995.

Congress. Senate. Committee on Governmental Affairs. Office of Management and Budget: Evolving Roles and Future Issues. S.Prt. 99-134. 99th Congress, 2nd session. Washington: GPO, 1986.

Willoughby, William F. The Problem of a National Budget. New York: D. Appleton and Co., 1918.

James Saturno

C. Budget and Accounting Procedures Act of 1950

Statutory Intent and History

The Budget and Accounting Procedures Act of 1950 (64 Stat. 2317) made significant changes to budget procedures within the executive branch and to government accounting and auditing processes. Presidential authority over budget preparation and presentation was expanded (Part I of Title I), principally to allow for performance-type budgeting, and both agency accounting systems and an integrated system for the government as a whole were reformed (Part II of Title I). These provisions are summarized below. The act also made various conforming amendments and provided for the redistribution of appropriations in cases where reorganization of the executive branch transferred authority between departments or agencies (Titles II and III).

The act's budget provisions amended the Budget and Accounting Act of 1921 (42 Stat. 20) and are consistent with the earlier law's purpose. Some provisions were then subsequently amended or otherwise affected by the Legislative Reorganization Act of 1970 (84 Stat. 1140), the Congressional Budget and Impoundment Control Act of 1974 (88 Stat. 297), and the Balanced Budget and Emergency Deficit Control Act of 1985 (99 Stat. 1037).

The act's accounting and audit provisions were enacted as new legislative authority, the Accounting and Auditing Act of 1950. They began with policy declarations that identified the purposes of government accounting — disclosing results of financial operations, informing managers and budget processes, and improving financial controls — in light of the needs and responsibilities of the executive and legislative branches. General Accounting Office audits were to determine the extent to which accounting and financial reporting fulfilled specified purposes, financial transactions complied with legal requirements, and internal control was adequate. Emphasis was placed on the importance of making continual improvements.

The accounting and auditing provisions have been amended numerous times. The most important changes required agencies to maintain accounts on an accrual basis (70 Stat. 782), establish internal accounting and administrative controls (96 Stat. 2467), and perform or undertake audits of the financial statements as required by the Chief Financial Officers Act (104 Stat. 2838). The Federal Financial Management Improvement Act of 1996 (enacted as part of the Omnibus Consolidated Appropriations for Fiscal Year 1997; P.L. 104-208; 110 Stat. 3009389) strengthened reporting and compliance requirements for financial management systems.

In 1982, both the budget and the accounting and auditing provisions were recodified in Title 31 of the United States Code (96 Stat. 877).

Major Provisions

Part I of Title I of the Budget and Accounting Procedures Act expanded the President's authority over budget preparation and presentation. It provided that the budget must conform to requirements and contain estimates in the form and detail that the President determines. When there is a basic change in budget format, the President is to transmit to Congress explanatory notes and tables needed to show where items included in prior budgets are contained in the current budget. The Bureau of the Budget (since 1970, the Office of Management and Budget (OMB)) prepares the budget according to these rules and regulations. Department heads prepare budget requests and submit them to the President. In addition, the President develops programs and regulations for improving statistical information in the executive branch and improved plans for the administration of executive branch agencies. For the Department of Homeland Security, separate detailed analyses by budget function, agency, and initiative area are required beginning with the FY2005 budget submission (Homeland Security Act of 2002, P.L. 107-296, Section 889).

Part II of Title I, the Accounting and Auditing Act, reformed government accounting and auditing processes. Its provisions applygenerallyto departments and independent establishments in the executive branch, with some exceptions.

The Accounting and Auditing Act specified new responsibilities for the Comptroller General, the Secretary of the Treasury, and agency heads. The Comptroller General prescribes accounting principles, standards, and related requirements for each executive agency. They must enable agencies to meet their responsibilities under the act while providing for (1) integration of agency and Treasury Department accounting processes; (2) full disclosure of the results of agency operations; and (3) financial information and controls needed by Congress and the President. In addition, the Comptroller General helps agencies develop their accounting systems. He approves systems that are adequate and conform to his prescriptions, while continuing to review them from time to time.

The Secretary of the Treasury develops coordinated financial accounting and reporting systems that enable integration of accounting results within the Treasury Department and consolidation with the accounting results of other executive agencies. To accomplish these ends, the Secretary is authorized to establish facilities, reorganize accounting functions, and install, revise, or eliminate accounting procedures and reporting. In addition, the Secretary prepares reports on the results of financial operations of the government. The reports include financial data required by OMB for budget preparation and other purposes.

Together, the Comptroller General and the Secretary of the Treasury may issue regulations waiving requirements for warrants pertaining to public moneys and trust funds and for the requisition and advancement of funds. Joint regulations may also allow authorized disbursing agents to pay vouchers by means of checks issued against the general account of the Treasury.

The head of each executive agency establishes and maintains accounting and internal control systems designed to provide (1) full disclosure of financial results of the agency's activities; (2) adequate financial information for agency management; (3) effective control over and accountability for all funds, property, and other assets; (4) reliable accounting results to serve as the basis for agency budget requests and execution; and (5) integration with the Department of the Treasury's central accounting and reporting system.

In addition, the Accounting and Auditing Act states that the General Accounting Office (except as specifically provided by law) shall audit financial transactions of each executive, legislative, and judicial agency in accordance with principles and procedures prescribed by the Comptroller General. In determining these auditing procedures, the Comptroller General must give due regard to generally accepted principles of auditing, including consideration of the effectiveness of agencies' accounting organizations and systems, internal audit and control, and related administrative practices.

Discussion

The Budget and Accounting Procedures Act of 1950 formally increased centralization of the budget process in the executive branch. It strengthened the authority of the President to determine the methods for preparing budget estimates and the way the budget would be presented to Congress. The principal goal was to allow for the development of performance-type budgets, as had been recommended by the Commission on Organization of the Executive Branch of the Government (the first Hoover Commission). However, the legislation probably had greater effect in furthering the development of budgets that are vehicles for expressing policy priorities and influencing the economy.

The Accounting and Auditing Act also increased centralization in the executive branch by directing that the results of agency accounting systems be integrated with a consolidated system within the Department of the Treasury. Perhaps more important, the act also required agency accounting systems to use standards that served broader ends than simply tracking expenditures, such as providing better information to Congress and the President. A further step was taken in this direction in 1956 with the requirement that agencies maintain their accounts on an accrual basis.

The most important legacy of the act may have been congressional encouragement that the government's top three financial managers — the Comptroller General, the Secretary of the Treasury, and the Director of OMB — work together in continually improving government accounting systems. Cooperative steps toward accounting reform eventually led to enactment of the Federal Managers' Financial Integrity Act of 1982, the Chief Financial Officers (CFO) Act, and the Federal Financial Management Improvement Act, all of which are summarized elsewhere in this compendium.

In 1990, the Comptroller General, the Secretary of the Treasury, and the Director of OMB jointly established the Federal Accounting Standards Advisory Board (FASAB) to recommend comprehensive accounting principles specifically for the federal government. A new memorandum of understanding was signed in May, 2003. By the end of 2003, the FASAB had issued 4 financial accounting concepts (concerning the objectives of federal financial reporting, entity and display issues, management discussion and analysis, and the intended audience and qualitative characteristics of the government's consolidated financial report) and 25 financial accounting standards (concerning the treatment of particular assets and liabilities, inventory, direct loans, etc.). In October 1999, the American Institute of Certified Public Accountants (AICPA) recognized the FASAB as the designated entity for establishing generally accepted accounting principles for the federal government. The AICPA action raised the status of FASAB statements and other pronouncements, though it has been criticized by some who question whether the FASAB is sufficiently independent of the federal agencies for which it is developing standards.

Improvements in federal accounting have occurred, but more work remains. GAO found that material weaknesses related to financial systems, fundamental record-keeping and financial reporting, and incomplete documentation have prevented it from expressing an opinion on the government's consolidated financial statements.[807] While 21 of the 24 CFO Act agencies received unqualified opinions for FY2002, GAO noted that most obtained clean audits only after extraordinary, labor-intensive efforts. Major problems included the government's inability to properly account for and report property, plant, and equipment; reasonably estimate and support amounts reported for environmental and other liabilities; support major portions of determinations for the net cost of government operations; fully account for and reconcile intragovernmental activities and balances; and properly prepare all aspects of financial statements. The most notable of these problems were in the Department of Defense. GAO also found material weaknesses in internal control, including problems relating to loans and receivables, improper payments, tax collection, and information security management.

Improved federal accounting systems likely result in savings from better cash management, more effective control of property, and a wider recognition of future obligations. However, improvements are not without cost. Continual progress in the future will depend upon adequate funding and managerial initiative, both of which could be diverted to other priorities. Greater use of expense budgeting, instead of (or in addition to) the obligation accounting now used in the appropriations process, might also help, though this would change

---

[807] U.S. General Accounting Office, Fiscal Year 2002 U.S. Government Financial Statements: Sustained Leadership and Oversight Needed for Effective Implementation of Financial Management Reform, GAO-03-572T, Apr. 8, 2003.

long-standing practice.[808] The extent to which financial accounting reforms should be continued is an issue for Congress to consider.

Selected Source Reading

Anthony, Robert M. "The FASAB's Dilemma." The Government Accountants Journal, vol. 44 (spring 1996), pp. 32-39.

Comes, Wendy and Anne Curtin Riley. "Federal Financial Statements: The Revolution Is Here!" Journal of Accountancy, vol. 187, no. 6 (June, 1999).

Cotton, David L. "Federal Accounting Standards: Close Enough for Government Work?" The Armed Forces Comptroller, vol. 45, no. 2 (summer 2000), pp. 3441.

David, Irwin T. "Financial Information for Policy, Program, and Operating Officials." The Journal of Government Financial Management, vol. 51, no. 1 (spring 2002), p. 10.

Ewar, Sid R. "Managerial Cost Accounting: A Step toward Accountability and Reliable Costing of Federal Programs." The Government Accountants Journal, vol. 48 (spring 1999), pp. 48-53.

Tierney, Cornelius E. Federal Accounting Handbook: Policies, Standards, Procedures, Practices. New York, 2000.

Titard, Pierre L. and Dean W. DiGregorio. "The Changing Landscape of Accounting Standards Setting." The CPA Journal, vol. 73, no. 11 (November 2003), p. 18.

U.S. Congress. House. Committee on the Budget. Federal Budget Process Structural Reform. Hearing. 107th Congress, 1st session, July 19, 2001. Washington: GPO, 2002.

——. House. Committee on Government Reform. Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations. The Federal Financial Management Improvement Act of 1996: Are the Agencies Meeting the Challenge? Hearing. 107th Congress, 2nd session, June 9, 2002. Washington: GPO, 2003.

——. House. Committee on Government Reform. Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations. H.R. 4685,

[808] Robert N. Anthony, "The Fatal Defect in the Federal Accounting System," Public Budgeting and Finance. vol. 20, no. 4 (winter 2000), pp. 1-10.

The Accountability of Tax Dollars Act of 2002. Hearing. 107th Congress, 2nd session, May 14, 2002. Washington: GPO, 2003.

U.S. Executive Office of the President. Office of Management and Budget. Links to OMB circulars and its Office of Federal Financial Management can be obtained from the OMB website, at [http://www.omb.gov], visited January 8, 2004.

U.S. Federal Accounting Standards Advisory Board. Statements of Federal Financial Accounting Concepts and Standards: Volume I, Original Statements. Washington, 2002.

——. Links to other FASAB statements as well as reports, exposure drafts, and newsletters can be obtained from the board's website, at [http://www.fasab.gov], visited January 8, 2004.

U.S. General Accounting Office. Accounting Principles. Standards, and Requirements: Title 2 Standards not Superceded by FASAB Issuances. GAO02-248G. November 2001.

——. Fiscal Exposures: Improving the Budgetary Focus on Long-Term Costs and Uncertainties. GAO-03-213. January 2003.

——. Fiscal Year 2002 U.S. Government Financial Statements: Sustained Leadership and Oversight Needed for Effective Implementation of Financial Management Reform. GAO-03-572T. April 8, 2003.

——. GAO/PCIE Financial Audit Manual.[809] Links to current requirements and related information and guidance can be obtained from the GAO website at [http://www.gao.gov], visited January 8, 2004.

——. Government Auditing Standards (the Yellow Book). Links to current standards and related information and guidance can be obtained from the GAO website at [http://www.gao.gov], visited January 8, 2004.

——. Performance Budgeting: Current Developments and Future Prospects. GAO03-595T. April 1, 2003.

——. Process for Preparing the Consolidated Financial Statements of the U.S. Government Needs Improvement. GAO-04-45. October, 2003.

Bob Lyke

138 PCIE is the President's Council on Integrity and Efficiency.

---

[809] PCIE is the President's Council on Integrity and Efficiency.

D. Balanced Budget and Emergency Deficit Control Act

Statutory Intent and History

After a decade of experience with the Congressional Budget Act of 1974, Congress and the President faced persistent high deficits and increasing budgetary deadlock. In 1985, legislation aimed at bringing the federal budget into balance by the early 1990s was enacted. That legislation, the Balanced Budget and Emergency Deficit Control Act of 1985, was included as Title II in a measure raising the public debt limit.[810] President Reagan signed the measure into law on December 12 as P.L. 99-177 (2 U.S.C. § 901; 99 Stat. 1037-1101). It is commonly referred to as the 1985 Balanced Budget Act or as the Gramm-Rudman-Hollings (GRH) Act, after its three primary sponsors in the Senate — Senators Phil Gramm, Warren Rudman, and Ernest Hollings.

The 1985 Balanced Budget Act was the first of several major laws intended to ensure that the deficit is reduced and spending is controlled, even if Congress and the President fail to achieve these goals through the regular legislative process (see the entry on the Budget Enforcement Acts of 1990 and 1997, elsewhere in this compendium). The act established new procedures involving deficit targets and sequestration to further these purposes. Under sequestration, across-the-board spending cuts would be made automatically early in the fiscal year if needed to keep the estimated deficit within allowed limits. Because implementation of a required sequester was automatic under these procedures, and perceived to be drastic action, many regarded it as providing a strong incentive for Congress and the President to reach agreement through the regular process of legislation meeting the established budgetary goals.

Specifically, the 1985 Balanced Budget Act required the federal budget to be in balance by FY1991. In addition, the act also made extensive changes in the 1974 Congressional Budget Act, largely to incorporate informal changes in practice made in prior years.

Several lawsuits contesting the constitutionality of the 1985 Balanced Budget Act were filed immediately. On February 7, 1986, a special three-judge panel of the U.S. District Court declared that the procedure for triggering sequestration under the act was unconstitutional on the ground that it vested executive power in an officer removable by Congress. (Sequestration would have been triggered pursuant to a report prepared by the Comptroller General, head of the General Accounting Office.) Further, the Court declared that a sequestration order for

---

[810] For a more detailed explanation of the 1985 Balanced Budget Act, see CRS Report 851130 GOV, Explanation of the Balanced Budget and Emergency Deficit Control Act of 1985 — Public Law 99-177 (The Gramm-Rudman-Hollings Act), by Allen Schick (1985); and CRS Report 86-713 GOV, Changes in the Congressional Budget Process Made by the 1985 Balanced Budget Act (P.L. 99-177), by Robert Keith (1986). (These reports are archived and available from the author of this entry in the compendium.)

FY1986, issued on February 1, 1986, was "without legal force and effect," but stayed its judgment (as required by Section 274(e) of the act) pending appeal to the Supreme Court.

The Supreme Court heard arguments in the case, Bowsher v. Synar (478 U.S. 714), on April 23, 1986, and issued its ruling later that year on July 7. Affirming the ruling of the District Court by a vote of 7 to 2, the Supreme Court noted:

To permit an officer controlled by Congress to execute the laws would be, in essence, to permit a congressional veto. Congress could simply remove, or threaten to remove, an officer for executing the laws in any fashion found to be unsatisfactory to Congress. This kind of congressional control over the execution of the laws, Chadha makes clear, is constitutionally impermissible.... It is clear that Congress has consistently viewed the Comptroller General as an officer of the Legislative Branch.

Anticipating the possibilityof invalidation bythe courts, Congress had included "fallback procedures" in the act, under which a presidential sequestration order could be triggered upon the enactment of a joint resolution, reported by a Temporary Joint Committee on Deficit Reduction, setting forth the contents of a joint report of the directors of the Office of Management and Budget (OMB) and the Congressional Budget Office (CBO). The Supreme Court stayed its judgment for 60 days in order to allow Congress time to implement sequestration for FY1986 under the fallback procedures, which Congress did.

Invalidation by the courts of the automatic triggering mechanism for sequestration and the size of the estimated deficit excess for FY1988 (more than $50 billion above the deficit target of $108 billion, according to CBO) prompted calls in 1987 for revision of the 1985 Balanced Budget Act. Major revisions to the act were enacted in 1987, again as a title in a measure raising the public debt limit. President Reagan signed the measure into law on September 29 as P.L. 100-119 (101 Stat. 754-788). Title I of this law is referred to as the Balanced Budget and Emergency Deficit Control Reaffirmation Act of 1987.[811] The main purposes of the 1987 Balanced Budget Reaffirmation Act were to restore the automatic triggering feature of sequestration in a constitutionally acceptable manner (which it did by vesting that authority in the OMB Director) and to extend the time frame for achieving a balanced budget by two years, until FY1993.

[811] For a more detailed explanation of the 1987 Balanced Budget Reaffirmation Act, see CRS Rept. 87-865 GOV, Debt-Limit Increase and 1985 Balanced Budget Act Reaffirmation: Summary of Public Law 100-119 (H.J.Res. 324), by Edward Davis and Robert Keith (1987). (This report is archived and is available from the author of this entry in the compendium.)

During the interim between the enactment of the 1985 Balanced Budget Act and its significant revision in 1987, Congress enacted several measures that modified the sequestration process, for the most part exempting programs from the reductions. Most notably, the Omnibus Budget Reconciliation Act of 1986 (100 Stat. 1874) exempted from sequestration the cost-of-living adjustments (COLAs) of all federal civilian and military retirement and disability programs so that they would be treated in the same manner as Social Security.

Following enactment of the 1987 Balanced Budget Reaffirmation Act (and before significant changes made in 1990), Congress enacted several measures that further modified the sequestration process. In particular, the Omnibus Budget Reconciliation Act of 1987 (101 Stat. 1330) made several technical changes in the 1985 Balanced Budget Act, and the Financial Institutions Reform, Recovery, and Enforcement Act of 1989 (103 Stat. 183) exempted certain federal financial entities from sequestration.

Major Provisions

Deficit Targets and Sequestration Procedures. In order to accomplish the goal of balancing the budget, the act established a series of declining deficit targets, referred to in the act as "maximum deficit amounts."[812] The series began with a deficit target of $171.9 billion for FY1986, which declined after the first year by increments of $36 billion until reaching zero in FY1991.

The deficit targets were enforced by a new set of procedures, referred to as "sequestration." As originally framed, sequestration involved the issuance of a presidential order to permanently cancel annual appropriations and other budgetary resources (except for special funds and trust funds) for the purpose of achieving a required amount of outlay savings in order to reduce the deficit. Any required sequestration reductions would occur toward the beginning of the fiscal year, based upon budget estimates made at that time.

As mentioned above, the Comptroller General was charged with responsibility under the act for determining whether a sequester was necessary each year and, if so, the amount of reductions that would have to be made in individual accounts and programs. His findings regarding the estimated deficit, the amount of any required sequester, the base levels for accounts from which reductions would be made, and the reduction amounts to be presented in annual sequestration reports issued twice each year. An interval of less than two months between the issuance of the two reports in late August and early October provided Congress and the President an opportunity to enact legislation preventing or minimizing a

[812] Although they were used chiefly for purposes of sequestration, the deficit targets also affected the budget resolution process, and therefore were made part of the 1974 Congressional Budget Act.

sequester. The Comptroller General was required to take into consideration sequestration reports issued jointly in August and October by the OMB and CBO directors.

If the Comptroller General found a sequester necessary, the President was required to issue a sequestration order putting into effect the reductions determined by the Comptroller General in his sequestration report. The President did not have discretion under the act to alter the Comptroller General's determinations.

In any year in which a deficit sequester occurred, the entire amount of the deficit excess (the amount by which the estimated deficit exceeded the applicable deficit target) would have to be eliminated. Sequestration could occur for FY1987-FY1990 only if the deficit excess for the year were greater than $10 billion. The $10 billion margin-of-error amount did not apply to FY1986, in which sequestration was capped at $11.7 billion, nor to FY1991, when the budget was required to be balanced.

A formula set forth in the act mandated that half the required outlay reductions be made in defense programs, programs in the National Defense (050) functional category, and half in non-defense programs. In general, sequestration reductions were made uniformly across the range of accounts covered by the process, and were applied uniformly to programs, projects, and activities within these accounts.

Many accounts, involving roughly two-thirds of federal outlays, were exempt from sequestration. For certain programs, the reductions were made under special rules. Medicare, for example, could not be cut more than 2%.

The act provided that the sequestration procedures would not apply during time of war and set forth a means to suspend them in the event of a recession. Finally, the act included procedures by which the President could propose, or Congress could initiate, modifications in a sequestration order.

The 1987 Balanced Budget Reaffirmation Act extended the timetable for achieving a balanced budget by two fiscal years to FY1993, restored the automatic triggering mechanism for sequestration, and made numerous adjustments to the sequestration procedures.

The deficit targets, as revised in 1987, maintained the $36 billion year-to-year decrease, except for FY1989 (when the target was reduced by $8 billion from the prior year) and FY1993 (when the target was reduced by $28 billion from the prior year). The $10 billion margin-of-error amount was retained for this period, except that sequestration reductions were capped at $23 billion for FY1988 and $36 billion for FY1989; no margin-of-error amount was allowed for FY1993, when the budget was expected to be balanced.

The automatic procedure for triggering sequestration was restored by placing it in the hands of the OMB Director. However, the director's authority to estimate and calculate sequestration amounts was carefully circumscribed by various provisions in the act. In particular, the procedures for making baseline estimates were delineated in the act. The new baseline-construction rules approximated more closely the concepts used by OMB in making "current services estimates" and by CBO in making "baseline budget projections." The new rules had the effect of minimizing differences in the estimates and projections of the two agencies, compared to earlier years.

Under the restored automatic procedure, an initial or final sequestration order would be triggered by an initial or revised sequestration report from the OMB Director. The OMB Director was required to give due regard in his report to an advisory sequestration report issued earlier by the CBO director. The Comptroller General was not assigned a role in the triggering process.

The 1987 Balanced Budget Reaffirmation Act retained the basic formula for determining sequestration reductions, but modified the procedures for crediting reductions in programs covered by special rules, such as student loans, foster care, and specified health programs. Additionally, the act authorized the President to exempt all or some military personnel accounts from sequestration, provided timely notice was given to Congress. (This authority previously had been given to the President only for FY1986.)

With regard to the modification of a sequestration order, the 1987 Balanced Budget Reaffirmation Act established two new mechanisms involving the enactment of a joint resolution under expedited procedures. Under the first, the President was authorized to submit to Congress a report proposing changes in the reductions in defense programs so that some programs could be spared cuts if others were cut more deeply (in order to retain the overall level of required reductions). Second, the majority leaders of the House or Senate could initiate legislation that would modify a sequestration order (even effectively canceling it). Both mechanisms would require the enactment of legislation in order to be effective.

Other Budget Process Changes. In addition to establishing the sequestration procedures, the 1985 Balanced Budget Act made other changes in the federal budget process. These other changes mainly involved modifications of the congressional budget process under the 1974 Congressional Budget Act (discussed more fully elsewhere in this compendium).

First, the timetable for congressional budget actions was accelerated. Most notably, the deadline for adoption of the annual budget resolution was advanced one month to April 15. Second, certain practices used by Congress for several years were formally incorporated into the 1974 Congressional Budget Act, including the expansion of budget resolutions to cover three fiscal years and authority to initiate reconciliation procedures in the April budget resolution.

Third, enforcement procedures were tightened, including new restrictions on legislation linked to committee spending allocations under the budget resolution and a requirement that the recommended deficit in the budget resolution not exceed the applicable deficit target. Fourth, the reconciliation process was modified in several ways, including a ban against using reconciliation to make changes in the Social Security program and requirements in the House and Senate that amendments to reconciliation measures be deficit neutral.

In addition to these and many other changes in congressional budgeting made by the act, it also required the President to submit an annual budget consistent with the deficit targets, placed existing off-budget entities on the budget, and placed the Social Security program off budget (except for calculating the deficit for purposes of sequestration).

The law which contained the 1987 Balanced Budget Reaffirmation Act (101 Stat. 754) also included related provisions (in Title II) that affected the congressional budget process, the impoundment control process, and other matters. With respect to the congressional budget process, the 1974 Congressional Budget Act was amended to clarify the application of time limits for the consideration of conference reports on budget resolutions and reconciliation measures, to require the House and Senate to use common economic and technical assumptions, to extend CBO duties under the State and Local Government Cost Estimate Act of 1981 indefinitely, and for other purposes.

The Impoundment Control Act of 1974 was amended to codify the Appeals Court decision in City of New Haven v. United States regarding restrictions on the President's deferral authority and to prohibit the resubmittal of rescission proposals that had been previously rejected by Congress.
Finally, the 1987 Balanced Budget Reaffirmation Act encouraged Congress to experiment with biennial budgeting and required CBO to prepare a report on federal credit programs.

Discussion

The 1985 Balanced Budget Act, as amended, was critically viewed by some for its failure to achieve its principal objective, deficit reduction. During the period covering FY1986 through FY1990, the actual deficit exceeded the deficit target every year. The overage ranged from about $5 billion to $205 billion and was greatest in the later years, despite the revision of the targets in 1987. Further, the manner in which the sequestration process operated and the stringency of the goals generally were perceived as fostering budgetary gimmickry and disruption in the legislative process.

As a result of these concerns, the sequestration process was fundamentally restructured by the Budget Enforcement Act of 1990 (discussed elsewhere in this compendium).

Selected Source Reading

Havens, Harry S. "Gramm-Rudman-Hollings: Origins and Implementation." Public Budgeting & Finance, vol. 6 (autumn 1986), pp. 4-24.

Schick, Allen. The Capacity to Budget. Washington: The Urban Institute Press, 1990.

Stith, Kate. "Rewriting the Fiscal Constitution: The Case of Gramm-Rudman-Hollings." California Law Review, vol. 76 (May 1988), pp. 593-668.

Robert Keith

E. Budget Enforcement Acts of 1990 and 1997

Statutory Intent and History

The Budget Enforcement Act (BEA) of 1990 made numerous and significant changes in the federal budget process by amending several laws, primarily the Balanced Budget and Emergency Deficit Control Act of 1985 (described elsewhere in this compendium).[813] (The BEA of 1990 also amended the 1974 Congressional Budget Act; changes in the 1974 act are discussed in another section of this compendium.) The chief focus of these changes was to revise fundamentally the sequestration process established by the 1985 act, but other important facets of the budget process were affected as well. With respect to sequestration, the BEA changed the focus from deficit targets to limits on discretionary spending (i.e., spending controlled through the annual appropriations process) and a "pay-as-yougo" (PAYGO) requirement on new legislative initiatives affecting revenues and direct spending (i.e., spending controlled outside the annual appropriations process). The main purpose of these changes was to ensure that the substantial deficit savings of several measures enacted in 1990, particularly the Omnibus Budget Reconciliation Act (OBRA) of 1990, were maintained over the five-year time frame of the legislation (covering FY1991-FY1995).

The BEA was enacted as Title XIII of OBRA of 1990 (104 Stat. 1388, 1-630). Although the BEA was formally developed as part of the 1990 reconciliation law, it can be traced to the budget summit negotiations between congressional and administration negotiators that began in early May of 1990 and concluded on September 30 of that year. On June 26, 1990, President George H.W. Bush issued a statement that he and congressional negotiators concurred that any bipartisan budget agreement should include budget process reform "to assure that any Bipartisan agreement is enforceable and that the deficit problem is brought under responsible control."

The sequestration procedures established under the 1985 act, as modified by the BEA of 1990, have been further modified and extended by several other laws, mainly to preserve budget savings made under agreements reached by Congress and the President in 1993 and 1997 and to establish new program categories for enforcement. In 1993, Congress and the President extended the procedures for three more fiscal years, through FY1998. The extension was included as Title XIV of the Omnibus Budget Reconciliation Act of 1993 (107 Stat. 312). In 1994, separate sequestration procedures for programs funded by the Violent Crime Reduction Trust Fund were added to the 1985 act by Title XXXI of the Violent Crime Control and Law Enforcement Act of 1994 (108 Stat. 3009).

---

[813] For a more detailed discussion of the BEA of 1990 and other budget process laws, see CRS Report 98-720 GOV, Manual on the Federal Budget Process, by Robert Keith and Allen Schick (1998).

Significant modifications to the sequestration process were made by the Budget Enforcement Act (BEA) of 1997, which was included as Title X of one of two reconciliation measures enacted into law that year, the Balanced Budget Act of 1997 (111 Stat. 251). The BEA of 1997 extended the discretionary spending limits and pay-as-you-go requirement through FY2002, modified their application, and made various "housekeeping" and technical changes. In 1998, the discretionary spending limits and associated sequestration procedures were changed again, in this instance by the Transportation Equity Act for the 21st Century (TEA-21; P.L. 105-178), in order to establish separate discretionary spending limits for highway and mass transit programs. In 2000, the Interior Appropriations Act for FY2001 (P.L. 106-291), established separate discretionary spending limits for conservation spending.

Finally, in the last few years under the BEA, Congress and the President modified the enforcement mechanisms in order to avoid a sequestration.[814] In 2000 and 2001, the Foreign Operations Appropriations Act for FY2001, P.L. 106-429, raised the FY2001 discretionary spending limits, and the Defense Appropriations Act for FY2002, P.L. 107-117, raised the FY2002 discretionary spending limits. In 1999, 2000, 2001, and 2002, legislation enacted into law required the OMB Director to change the balance on the PAYGO scorecard for certain years to zero. In particular, in 2002, the PAYGO scorecard was set at zero for FY2003 and each year thereafter through FY2006, thereby preventing any future PAYGO sequestration due to legislation enacted before October 1, 2002.

In the absence of any action by Congress and the President to extend the discretionary spending limits and the PAYGO requirement by the end of FY2002, budget legislation is no longer subject to these budget mechanisms.

Major Provisions

Revised Sequestration Procedures. The BEA of 1990, and later laws, changed the sequestration process substantially. While the BEA of 1990 extended the deficit targets in the 1985 Balanced Budget Act through FY1995 (although the budget was not expected to be in balance by this time), it made them adjustable rather than fixed. More importantly, the BEA of 1990 effectively replaced the deficit targets with two new budget enforcement procedures. First, adjustable limits were established for separate categories of discretionary spending. Second, "pay-as-yougo" (PAYGO) procedures were created to require that increases in direct spending or decreases in revenues due to legislative action be offset so that there would be no net increase in the deficit (or reduction of the surplus). Further, the BEA of 1990 retained the exemption of Social Security from cuts under

[814] For more detailed information on these modifications, see CRS Report RL31155, Techniques for Preventing a Budget Sequester, by Robert Keith.

sequestration, but removed the trust fund surpluses from the deficit estimates and other calculations as well.

The revised deficit targets, as initially set by the BEA of 1990, were substantially larger than earlier targets because they excluded the surpluses of the Social Security trust funds and reflected revised economic and technical assumptions. For example, the deficit target for FY1991 was set at $327 billion, and the deficit target for FY1995 was set at $83 billion. The President was required to adjust the deficit targets for FY1991-FY1995, to reflect updated economic and technical assumptions and changes in budgetary concepts and definitions, as applicable, in his annual budget for FY1992 and FY1993. Further, he was authorized to adjust the deficit targets for FY1994 and FY1995, to reflect updated economic and technical assumptions, when he submitted his budget for these fiscal years. (President Clinton chose to use this authority, and made such adjustments in the deficit targets.)

The BEA kept the procedures for a deficit sequester. As under the earlier procedures, half of the required outlays savings would be from defense programs and half from nondefense programs. The margin-of-error amount was set at zero for FY1992 and FY1993 and at $15 billion for FY1994 and FY1995. Sequestration tied to enforcement of the deficit targets would have occurred only if a deficit excess had remained after the other two types of sequestration had been implemented. However, the operation of the other two types of sequestration, together with the adjustability of the deficit targets, effectively made a deficit sequester impossible.

The BEA of 1990 retained sequestration as the means of enforcing the discretionary spending limits and the PAYGO requirement. Like the earlier deficit sequestration procedures, the new sequestration procedures were automatic and were triggered by a report from the OMB Director. For sequestration purposes generally, only one triggering report was issued each year (just after the end of the congressional session). However, OMB reports triggering a sequester in one or more categories of discretionary spending might have been issued during the following session if legislative developments so warranted (i.e., the enactment of a supplemental appropriations measure that violated the limit for one or more discretionary spending categories). The CBO director was required to provide advisory sequestration reports several days before the OMB Director's reports were due.

The discretionary spending limits established by the BEA of 1990 varied in type over the period covered. For FY1991 through FY1993, separate limits were set for new budget authority and outlays for three different categories — defense, international, and domestic. For FY1994-FY1995, the limits on new budget authority and outlays were established for a single category — total discretionary spending. The Omnibus Budget Reconciliation Act of 1993 retained the existing limits for FY1994 and FY1995 without change, and added new limits on total discretionary spending for FY1996-FY1998. In 1994, the Violent Crime Control

Act established separate sequestration procedures for spending from the Violent Crime Reduction Trust Fund through FY2000.

The BEA of 1997 revised the discretionary spending limits again and extended them through FY2002. New categories were established for defense and nondefense spending for FY1998 and FY1999; for FY2000-FY2002, all discretionary spending was merged into a single, general purpose category (except for the separate Violent Crime Reduction category in effect through FY2000). In 1998, TEA-21 established separate outlay limits for two new categories, highways and mass transit, through FY2003. Finally, in 2000, Section 801(a) of the Interior Appropriations Act for FY2001 established separate discretionary spending limits for FY2002-FY2006 under a new category for conservation spending and six related subcategories.

The discretionary spending limits were adjusted periodically — when the President submitted his annual budget and when OMB issued sequestration reports — for various factors, including changes in budgetary concepts and definitions, emergency requirements, and special allowances. Factors upon which adjustments were based changed from time to time. For example, the BEA of 1990 provided for an adjustment due to changes in inflation, but this adjustment was removed by the BEA of 1997.

A sequester under the discretionary spending limits would occur only within the category in which a breach occurred, except that a breach of the highway or mass transit limits would trigger a sequester in the nondefense or total discretionary spending category, as appropriate. If a sequester under this process was required at the end of a session, it was required to occur on the same day as any sequestration tied to enforcement of the PAYGO procedures. During the following session, the enactment of legislation causing a breach in the spending limits would trigger sequestration after 15 days. However, any such enactment occurring during the last quarter of the fiscal year (i.e., between July 1 and September 30) would instead cause the appropriate discretionary spending limits for the next fiscal year to be reduced by the amount of the breach.

Under the PAYGO process created by the BEA of 1990, the multi-year budget effects of legislation proposing new direct spending, or legislation decreasing revenues, were recorded on a rolling PAYGO "scorecard." After the end of each congressional session, any balance on the PAYGO scorecard for the new fiscal year was required to be eliminated through a special sequestration procedure. If a sequester under this process was required, it was required to occur within 15 calendar days after Congress adjourned at the end of a session and on the same day as any sequestration tied to enforcement of the discretionary spending limits (or, in earlier years, the deficit targets). Emergency direct spending and revenue legislation, so designated by the President and in statute, was not covered by the PAYGO sequestration process.

The enforcement procedures for the PAYGO requirement, on the one hand, and the discretionary spending limits, on the other, were separated by a "firewall." Savings made on one side of the firewall could not be used to the advantage of programs on the other side. For example, the cost of tax-cut legislation could not be offset by reductions in annual appropriations acts in order to avoid a PAYGO sequester.

OMB and CBO were each required to prepare annually three different types of sequestration reports, as discussed below. The CBO reports (which are advisory only) preceded the OMB reports by several days, as was the case under prior sequestration procedures. In all three types of reports, OMB was required to explain any differences between its estimates and those of CBO.

If the President was required to issue a sequestration order in any year, the order was to be issued on the same day that the final OMB sequestration report was issued and the order was required to implement without change all of the reductions identified in the OMB report. There was no initial order, unlike under earlier procedures.

Early in the session, OMB and CBO issued sequestration preview reports. The reports provided estimates of the discretionary spending limits, with the adjustments prescribed by law. Also, the reports provided estimates of any net change in the balances on the PAYGO scorecard caused by the enactment of direct spending or revenue legislation subject to the PAYGO process. The OMB preview report contained the same information as the CBO preview report and explained any differences between its estimates and those of CBO.

In August, OMB and CBO issued sequestration update reports to reflect the impact of legislation enacted in the interim. Finally, OMB and CBO issued final sequestration reports shortly after Congress adjourned to end the session. Both reports were required to reflect any pertinent legislation enacted since the update reports were issued. The final reports were required to indicate the baseline amount of budgetary resources and the amount and percentage of the reduction for each account subject to sequestration.

In preparing its update and final sequestration reports, OMB was required to use the economic and technical assumptions that were used in the earlier preview report. (Previously, OMB could determine in late summer the economic and technical assumptions that it would use for sequestration in October.)

During the course of the session, OMB was required to provide Congress with cost estimates of budgetary legislation within seven days of its enactment, so that compliance with the discretionary spending limits and PAYGO requirements could be monitored. The cost estimates were required to be based on the economic and technical assumptions used in the President's most recent budget.

Several other special reports were associated with the sequestration process.

Other Budget Process Changes. The BEA of 1990 and 1997 made other changes in the federal budget process, including (1) moving the deadline for submission of the President's annual budget from the first Monday after January 3 to the first Monday in February; (2) excluding Social Security trust funds from deficit calculations made under the 1985 Balanced Budget Act (and reaffirming of their off-budget status), coupled with establishing separate House and Senate procedures to protect the trust fund balances; (3) enacting the Federal Credit Reform Act of 1990, as a new Title V in the 1974 Congressional Budget Act; and (4) requiring that budget resolutions cover, and be enforced for, at least five fiscal years. Additionally, the BEA included provisions requiring studies and legislative recommendations regarding government-sponsored enterprises, revising the Senate's "Byrd Rule" prohibiting extraneous matter in reconciliation legislation and incorporating it into the 1974 Congressional Budget Act as Section 313, and dealing with various other issues.

Discussion

The BEA of 1990, and the related laws that followed it, generally are regarded as having been more successful than the 1985 Balanced Budget Act (as amended by the 1987 Balanced Budget Reaffirmation Act) in controlling aggregate budget levels. During the period that the discretionary spending limits and PAYGO requirement were in effect, the status of the federal budget changed from the largest deficit recorded in history ($290 billion in FY1992) to unprecedented surpluses ($237 billion in FY2000). Although this dramatic change was due to many factors, the procedures under the BEA were regarded by many as important contributing factors to this accomplishment.

During the 106th Congress, criticisms of the BEA procedures began to mount. While the threat of sequestration was viewed initially as giving the President and Congress a strong incentive to reach agreement on their budgetary goals, thereby avoiding the legislative deadlock that characterized the early 1980s, some Members began to regard the BEA procedures as an impediment to implementing desired budget policy in an era of large surpluses. These Members argued that the BEA procedures should be eliminated, or at least substantially modified, so that Congress and the President could "use" part of the surplus for tax cuts and other actions that otherwise would have been prohibited. Further, some Members asserted that discretionary spending limits for FY2000-FY2002 were unrealistically low, thereby promoting the use of budget "gimmicks," such as the excessive designation of emergency spending, to evade their constraints. More recently, during the 107th Congress, the procedures under the BEA were set aside to respond to the terrorist attacks on September 11, 2001, and the 2001 recession. Subsequently, as noted above, the BEA procedures were allowed to expire on September 30, 2002.

For the foreseeable future, Congress faces an unfavorable budget outlook, exacerbated by an uncertain economic and geopolitical environment. According

to OMB and CBO, current budget projections under existing law, without any legislative changes, show annual deficits in the unified budget (i.e., including federal funds and trust funds) in each of the next few fiscal years.[815] When various proposed spending increases and tax cuts are taken into account, the projections indicate annual deficits for the foreseeable future. For example, OMB projects that if President Bush's FY2004 budget policy proposals are enacted into law, annual unified budget deficits, ranging from $178 billion to $307 billion, will continue through FY2008.

In addition, the economy continues to put a damper on federal revenues. Also, the spending for the war on terrorism and homeland security, and for military and reconstruction operations in Iraq and Afghanistan, could increase the scarcity of current and future federal government resources. Such factors potentially could worsen the already unfavorable budget outlook.[816] Accordingly, the 108th Congress is faced with the issue of whether the expired BEA procedures should be restored, new budget constraints should be enacted, or the existing budget procedures associated with the Congressional Budget Act are sufficient.

Selected Source Reading

Congressional Budget Office. "The Expiration of Budget Enforcement Procedures: Issues and Options." In The Budget and Economic Outlook: Fiscal Years 20042013, pp. 109-121. Washington: CBO, 2003.

Philip, Joyce G. and Robert D. Reischauer. "Deficit Budgeting: The Federal Budget Process and Budget Reform." Harvard Journal on Legislation, vol. 29, (summer 1992), pp. 429-453.

Oak, Dale P. "An Overview of Adjustments to the Budget Enforcement Act Discretionary Spending Caps." Public Budgeting & Finance, vol. 15 (fall 1995), pp. 35-53.

Thurber, James A. and Samantha L. Durst. "The 1990 Budget Enforcement Act: The Decline of Congressional Accountability." In Dodd, Lawrence C. and Bruce I. Oppenheimer, Congress Reconsidered, pp. 375-397. Washington: CQ Press, 1993.

Robert Keith

---

[815] See U.S. Office of Management and Budget, Budget of the U.S. Government, Fiscal Year 2004 (Washington: GPO, 2003), table S-1, p. 311 (for projections with President George W. Bush's budget proposals included) and table S-13, p. 330 (for projections under existing law); and U.S. Congressional Budget Office, The Budget and Economic Outlook: Fiscal Years 2004-2013, Jan. 2003, table 1.1, p. 2 (for CBO's budget baseline projections, under existing law).

[816] For more detailed information on the FY2004 budget throughout the year, see CRS Report RL31784, The Budget for Fiscal Year 2004, by Philip D. Winters.

Bill Heniff Jr.

F. Congressional Budget and Impoundment Control Act

Statutory Intent and History

The Congressional Budget and Impoundment Control Act of 1974 (88 Stat. 302) established the basic framework which is used today for congressional consideration of budget and fiscal policy. The concurrent resolution on the budget, the House and Senate Budget Committees, and the Congressional Budget Office are all provided for in this legislation. In addition, the President's impoundment authority was codified for the first time in Title X, also known as the Impoundment Control Act.

The Congressional Budget Act built upon the knowledge gained in earlier attempts to create a legislative budget, but it chiefly grew out of the combination of several separate movements for congressional reform in the 1960s and 1970s and a series of confrontations with the President over the budget. There were various calls for structural reforms within Congress, and concurrently a desire to make Congress, as a whole, better able to assert its budget priorities more effectively vis-à-vis the President's.

The issue of federal spending approached a crisis in the late 1960s and early 1970s. Increased spending for programs initiated or expanded under the banner of President Lyndon Johnson's "Great Society," combined with that to support military efforts in Vietnam, accelerated concern over budget deficits. A series of spending ceilings were enacted by Congress between 1967 and 1970, but these proved to be largely ineffective. Even so, President Richard Nixon kept the controversy over such ceilings alive during the 1972 presidential campaign by asking for authority to cut federal spending at his own discretion to stay under a proposed $250 billion ceiling in FY1973. Congress declined to approve such an open-ended grant of authority, and while no further spending ceilings were enacted, the crisis over presidential authority to withhold funds escalated.

In response to this battle with President Nixon, Congress established a Joint Study Committee on Budget Control in 1973 which recommended a legislative process to "improve the opportunity for the Congress to examine the budget from an overall point of view, together with a congressional system of deciding priorities." These recommendations were reviewed by committees with legislative jurisdiction in the House and Senate,[817] and eventually enacted as the Congressional Budget and Impoundment Control Act of 1974 (88 Stat. 302).

The intent behind the 1974 Budget Act is still a subject for debate. The act made a number of changes in the way Congress operated, but one thing it did not do was

[817] In the House, H.R. 7130 was referred to the Rules Committee; in the Senate, S. 1541 was referred to the Government Operations Committee and subsequently to the Rules and Administration Committee.

to centralize budget decision making. The budget resolution was a mechanism for deciding the broad outlines of budgetary decision making, but the details about the composition of revenue and spending remained within the jurisdiction of the same committees that had exercised jurisdiction prior to the act. The new budget process built on existing congressional procedures, but did not supersede them. To some, this indicated that the purpose of the Budget Act was merely to create a mechanism for coordinating congressional decision making and for providing budgetary information. Others, however, feel that the Budget Act was created to deal with the problem of structural deficits that arose in the 1970s. One result was that the Budget Act has been the focus of numerous reform proposals over the years, a number of which have been enacted. The most extensive changes occurred as a consequence of the Balanced Budget and Emergency Deficit Control Act of 1985, and the Budget Enforcement Act of 1990 (discussed elsewhere in this compendium).

Major Provisions

Titles I through IX of the Budget Act are collectively known as the Congressional Budget Act of 1974, and Title X is known as the Impoundment Control Act of 1974. Title V, as amended in 1990, is now known as the Federal Credit Reform Act of 1990.

The most salient aspect of the Congressional Budget Act is that it established a congressional budget process. As originally enacted, the Budget Act provided for two budget resolutions, the first to provide planning levels and to be adopted by May 15, and a second to provide binding levels (that is, subjecting legislation that breached these totals to points of order) to be adopted by September 15. This division proved to be impracticable, and for fiscal years 1983-1986, Congress did not adopt a second budget resolution. Instead, the first budget resolution for each of these years included a provision that made the spending and revenue totals in the first resolution binding as of the beginning of the fiscal year (October 1). In 1985, Congress amended the Budget Act to provide that, beginning with FY1987, the spending and revenue totals in a single budget resolution (to be adopted by April 15) would be immediately binding.

As enacted, the Budget Act also required that committees report all authorizing legislation prior to May 15. This requirement tended to create a bottleneck of legislation that made it difficult to complete floor action on authorizing measures prior to consideration of appropriation bills, and was eliminated in 1985.

Currently, Title III requires that Congress approve a concurrent resolution on the budget by April 15 (Section 300), that must be adopted before other budgetary legislation can be considered (although the House may consider appropriation bills after May 15 regardless of the status of the budget resolution) (Section 303). Amounts agreed to in the budget resolution are “cross walked” to each committee with jurisdiction over spending under Section 302.

Title III also contains provisions concerning special procedures for consideration of budget resolutions and reconciliation bills. Debate in the Senate on budget resolutions is limited to 50 hours (Section 305) and on reconciliation bills to 20 hours (Section 310). The amending process is also limited. A germaneness requirement is imposed in the Senate for amendments to both budget resolutions (Section 305) and reconciliation bills (Section 310); amendments to reconciliation bills in either chamber must be deficit neutral (Section 310); and amendments in the Senate to reconciliations must not be extraneous (Section 313).

Section 306 specifically protects the jurisdiction of the Budget Committees. It prohibits floor action on any bill or amendment dealing with matters within the jurisdiction of the Budget Committee not reported by the Budget Committee (or an amendment to a bill reported by the Budget Committee). In addition to jurisdiction over budget resolutions and reconciliation bills, House Rule X, clauses (e)(1)(2) and (3) grant the House Budget Committee jurisdiction over "the congressional budget process, generally" and the "establishment, extension, and enforcement of special controls over the Federal budget, including the budgetary treatment of off-budget Federal agencies and measures providing exemption from reduction under any [sequester order]." In the Senate, a standing order of August 4, 1977, provides that jurisdiction over legislation concerning the budget process be jointly referred to the Senate Budget and Governmental Affairs Committees.

Title IV establishes additional limits on the consideration of certain measures.

For example, although changes can be made in the formulae for entitlement programs which can increase the projected level of expenditures, Section 401(b) of the Congressional Budget Act is designed to limit such increases. Section 401(b)(1) requires that increases in entitlement spending not become effective during the current fiscal year. Section 401(b)(2) further provides that increases that will become effective during a fiscal year be limited to the level allocated under Section 302(b) in connection with the most recent budget resolution or be subject to referral to the Appropriations Committee (for a period not to exceed 15 days).

Title IV also provides that contract authority and debt authority do not exist outside the budget process as a means of financing federal programs. Section 401(a) of the Congressional Budget Act requires that bills that provide authority "to enter into contracts under which the United States is obligated to make outlays" or "to incur indebtedness ... for the repayment of which the United States or new credit authority be effective for any fiscal year only to the extent provided in appropriation Acts."

Finally, the Unfunded Mandates Reform Act of 1995 (discussed elsewhere in this compendium) added Sections 421-428 to the Congressional Budget Act. These sections limit the consideration of unfunded federal mandates to the states.

In addition to establishing the congressional budget process, the Budget Act contains provisions dealing with numerous other aspects of federal fiscal management. Title I established the House and Senate Budget Committees.

Title V, also known as the Federal Credit Reform Act of 1990 (discussed elsewhere in this compendium), was added as a part of the Budget Enforcement Act.[818] The Federal Credit Reform Act specifies the budgetary treatment of federal credit programs, and provides that only the cost to the government of such programs should be on budget, other associated outlays being treated as a means of financing the programs.

Title II created a new congressional agency and outlined its responsibilities. The Congressional Budget Office (CBO) was charged with providing information to Congress. This basic function has not changed, but the nature of the information required by Congress has expanded over time.

These duties are further specified in Section 308 of the Budget Act, which requires that reports for bills providing new spending authority, new budget authority, new credit authority, or changing revenues or tax expenditures include a cost estimate prepared "after consultation with the Director of the Congressional Budget Office." In addition, Section 403 of the act requires the Director of the Congressional Budget Office "to the extent practicable, [to] prepare [a cost estimate] for each bill or resolution of a public character reported by any committee".

Section 424, added by the Unfunded Mandates Reform Act of 1995, placed additional responsibilities on CBO by requiring that it prepare and submit an estimate of the direct cost of all federal intergovernmental mandates contained in each bill reported in the House and Senate.

Title X, the Impoundment Control Act, codifies presidential authority to withhold federal funds which have been appropriated. The act defines such authority as rescissions and deferrals.

Rescission authority established under the Impoundment Control Act allows the President to propose cancellation of funds and to withhold those funds for a 45 day period pending congressional action. If Congress does not approve the

---

[818] As originally enacted, Title V provided for a change in the fiscal year of the federal government. Prior to the Congressional Budget Act, the fiscal year began on July 1 of the preceding calendar year. Since FY1976, the fiscal year has begun on October 1 of the preceding calendar year. This provision and several others in Titles V, VI, VII, and VIII were repealed in 1982 by P.L. 97-258 (96 Stat. 877), An Act to Revise, Codify, and Enact Without Substantive Change Certain General and Permanent Laws, Related to Money and Finance, as Title 31, United States Code, "Money and Finance."

rescission request (or takes no action), the funds must be released at the end of that period. Section 207 of the Balanced Budget and Emergency Deficit Reaffirmation Act of 1987 further codified this authority to allow the President to submit a rescission request only once.

Deferral authority allows the President to withhold funds temporarily, but deferrals may not extend beyond the end of the fiscal year. The Impoundment Control Act originally provided for a one-house veto of any proposed deferral, but this power was negated by the Supreme Court in I.N.S. v. Chadha (103 S.Ct. 715, (1983)). Subsequently, the U.S. Court of Appeals ruled in City of New Haven, Conn. v. United States (809 F.2d 900 (D.C. Cir. 1987)) that the one-house veto provision was not severable from the President's expanded authority in the 1974 law for policy based deferrals. Language clarifying this narrowed base for deferrals was incorporated into the Impoundment Control Act by the Balanced Budget and Emergency Deficit Reaffirmation Act of 1987.

In 1996, Congress enacted provisions to grant the President enhanced rescission authority. Known as the Line Item Veto Act of 1996 (110 Stat. 1200; Sections 10211027 of the Impoundment Control Act; 2 U.S.C. §621), these provisions inverted the existing relationship between Congress and the President regarding proposals for rescissions. Rather than requiring congressional support for a resolution approving the President's proposal, the new law required the enactment of a bill or joint resolution of disapproval to prevent a proposed rescission from becoming effective. A resolution of disapproval would be subject to a presidential veto, so a two-thirds vote in each House would be necessary to override and prevent a rescission. The Line Item Veto Act also expanded the scope of rescission authority. The act provided that in addition to discretionary spending, whenever the President signs a bill into law, he may cancel any item of new direct spending (i.e. entitlements), or certain limited tax benefits.[819]

In 1998, the Supreme Court struck down the act as unconstitutional (Clinton v. City of New York, 524 U.S. 417). It ruled that the Item Veto Act effectively allowed the President to repeal parts of a statute in violation of Article I of the Constitution.

Discussion

The Congressional Budget Act has been judged harshly by its critics despite achieving a significant measure of success. Its enactment resulted in greater control of impoundments, led to a resurgence of Congress's role in setting budget

[819] Defined as any revenue-losing provision that provides a federal tax deduction, credit, exclusion, or preference to 100 or fewer beneficiaries and any federal tax provision to provide temporary or permanent transitional relief for 10 or fewer beneficiaries.

priorities, and increased the attention of Congress to the whole budget. It has not, however, resulted in the orderly process that some had hoped for. Deadlines for adopting budget resolutions and for enacting spending legislation have routinely been missed; the Budget Committees have sometimes been the source of conflict, in part because authority was not significantly redistributed by the act; there is also a perceived redundancy in debating the outlines of budget priorities on the budget resolution and then later debating the details in authorizations and appropriations.

Perhaps because of these shortcomings, Congress has continued to debate the budget process and possible reforms virtually since the Budget Act was signed into law. Reform proposals have generally focused on one of two areas: (1) spending or deficit control mechanisms, as in the Balanced Budget and Emergency Deficit Control Act of 1985, and the Budget Enforcement Act of 1990; and (2) streamlining the decision making process, usually by eliminating one group of decision makers from the process or reducing the frequency of decisions (as with biennial budgeting).

Selected Source Reading

Pfiffner, James P. The President, the Budget, and Congress: Impoundment and the 1974 Budget Act. Boulder, CO: Westview Press, 1979.

Schick, Allen. Congress and Money. Washington: The Urban Institute, 1980.

Congress. Joint Study Committee on Budget Control. Recommendations for Improving Congressional Control Over Budgetary Outlay and Receipt Totals. H.Rept. 93-147. 93rd Congress, 1st session. Washington: GPO, 1973.

Congress. Senate. Committee on Government Operations. Congressional Budget and Impoundment Control Act of 1974, Legislative History. Committee print. 93rd Congress, 2nd session. Washington: GPO, 1974.

James Saturno

G. Chief Financial Officers Act of 1990

Statutory Intent and History

The Chief Financial Officers (CFO) Act of 1990 (104 Stat. 2838)[820] constitutes a significant legislative effort to improve financial management in the federal government. Its passage shortly before the adjournment of the 101st Congress reflected a bipartisan effort stretching over a period of five years. The new CFO Act was heralded by many persons as the most important financial management legislation since the Budget and Accounting Procedures Act of 1950 (64 Stat. 832).

Title I of the CFO Act, "General Provisions," offers congressional findings regarding federal financial management, including identification of some existing weaknesses. Three purposes of the act are set forth:

- improvement of financial management practices by creating a new leadership structure for federal financial management (consisting of two new positions within the Office of Management and Budget (OMB)), and CFOs for the major executive departments and agencies;
- improvement of agency systems of accounting, financial management, and internal controls to assure the issuance of reliable financial information and to deter fraud, waste, and abuse of government resources; and
- production of complete, reliable, timely, and consistent financial information for use by both the executive branch and Congress in the financing, management, and evaluation of federal programs.

When the Social Security Independence and Program Improvements Act of 1994 (108 Stat. 1467) established the Social Security Administration (SSA) as an independent agency and created a new CFO position, the original number of 23 CFO agencies was increased to the current total of 24.[821]

Major Provisions

---

[820] Codified as amended at 31 U.S.C., Chapters 5, 9, 11, and 35; also 5 U.S.C. §§ 5313-5315, 38 U.S.C. § 201 nt, and 42 U.S.C. § 3533.

[821] Of the 24 CFO positions, those in the 14 cabinet-level departments (the Department of Homeland Security is not covered by the CFO Act), the Environmental Protection Agency, and the National Aeronautics and Space Administration are filled by presidential appointees confirmed by the Senate. The remaining eight CFO positions (for the Agency for International Development, Federal Emergency Management Agency, General Services Administration, National Science Foundation, Nuclear Regulatory Commission, Office of Personnel Management, Small Business Administration, and Social Security Administration), along with all 24 deputy CFO positions, are career slots, filled by agency head appointment. See following "Discussion" section for more on creation of additional CFO positions.

Title II, "Establishment of Chief Financial Officers," creates a new leadership structure for federal financial management. A new deputy director for management within OMB, appointed by the President and confirmed by the Senate, serves as the federal government's chief financial officer. His functions with respect to financial management include leadership, policy setting, implementation, and operations, as well as responsibility to carry out the full range of general management duties.

The deputy director for management also performs important coordinating functions within the federal financial management structure, including links to both agency personnel and operations in this area.

Title II also establishes an Office of Federal Financial Management (OFFM) within OMB, funded by a separate line item in OMB's budget and headed by a controller appointed by the President, subject to Senate confirmation. The incumbent, who must have "demonstrated ability" and "extensive practical experience" in financial management, serves as the principal advisor on financial management to the deputy director for management.

The act stipulates qualifications for both the agency CFOs and deputy CFOs. Each of the 24 agency CFOs reports directly to the agency head and is responsible for all agency financial management operations, activities, and personnel. Financial management is broadly defined, with agency CFOs assigned a variety of functions, including producing financial information, establishing an integrated financial management system, developing cost information, and developing systems that provide for systematic performance measurement. The Government Performance and Results Act of 1993 (107 Stat. 285) augmented performance measurement requirements, extending the initial language in the CFO Act regarding "systematic measurement of performance" for selected activities.

The 24 CFOs also are responsible for preparing annual management reports for their agencies, addressed to the agency head and to the OMB Director, within 60 days after the audit report (described below). The OMB Director then transmits the reports to the Senate Committee on Governmental Affairs and the House Committee on Government Reform. Each report contains an analysis of the financial management status of the agency, its financial statements and audit report, and a summary of material weaknesses pursuant to the Federal Managers' Financial Integrity Act of 1982 (96 Stat. 814), as well as other information.[822]

[822] In 2001 the OMB Director, pursuant to authority provided in the Reports Consolidation Act of 2000 (P.L. 106-531), required that agencies combine their annual performance reports with the financial statements and other materials required by the CFO Act, into a consolidated Performance and Accountability Report.

Title III, "Enhancement of Federal Financial Management Activities," covers a variety of subjects. One section requires the Director of OMB to prepare and submit a financial management status report and a government-wide five-year financial management plan to the appropriate committees of Congress. The report details the activities the Director, the controller, and agency CFOs plan to undertake, over the next five years, to improve financial management.[823] Another section establishes the Chief Financial Officers Council, chaired by OMB's deputy director for management; other members include the controller, the Fiscal Assistant Secretary of Treasury, and the 24 agency CFOs.[824] The Council meets periodically and serves as an interagency coordinating body.

The original requirements in the CFO Act for audited financial statements were substantially expanded by provisions in the Government Management Reform Act of 1994 (GMRA; 108 Stat. 3410). Initially, Sections 303 and 304 of the CFO Act provided that all covered agency heads would prepare and submit to OMB audited financial statements for each revolving and trust fund and for accounts that performed substantial commercial functions. In addition, a three-year pilot project (eventually involving 10 of the original 23 agencies) commenced, requiring preparation of audited financial statements for all agency accounts.

GMRA extended the requirement for audited financial statements covering all accounts to include all 24 CFO agencies. Beginning on March 1, 1997, and in each year thereafter, the agency head submits to the OMB Director "an audited financial statement for the preceding fiscal year, covering all accounts and associated activities of each office, bureau, and activity of the agency." Further, not later than March 31, 1998, and in each succeeding year, the Secretary of the Treasury, in coordination with OMB, is to submit to the President and Congress an audited financial statement covering all federal executive branch agencies for the preceding fiscal year. Finally, Sections 305 and 306 revised the mandate and general procedures for financial audits and management reports of government corporations.

The Federal Financial Management Improvement Act (FFMIA) of 1996[825] established a general requirement for CFO agencies to "implement and maintain financial management systems that comply substantially with federal financial management system requirements, applicable federal accounting standards, and

---

[823] The 2003 financial managemnt status report and five-year plan was issued in August 2003. See Office of Management and Budget, 2003 Federal Financial Management Report, Washington, Aug. 2003, available at: [http://www.whitehouse.gov/omb/financial/2003_report_final.pdf], visited Jan. 22, 2004.

[824] The CFO Council charter also includes the statutory deputy CFOs as members.

[825] The FFMIA was enacted as Title VIII in the Omnibus Consolidated Appropriations Act for FY1997; 110 Stat. 3009-389; 31 U.S.C. § 3512 note.

the United States Government Standard General Ledger at the transaction level" (FFMIA is further discussed elsewhere in the compendium). The Accountability of Tax Dollars Act of 2002[826] further amended the CFO Act and extended the coverage of the requirements for preparation of audited financial statements to most executive branch agencies (see further discussion of this law elsewhere in this compendium).

Discussion

The CFO Act provided a new framework for financial management in the executive branch. However, implementation of the various requirements in the act is an ongoing process. For example, the legislation requires that the 24 covered agencies have two financial statements prepared and audited each year: a statement of financial position, and a statement of results of operations. Described simply, the statement of financial position is a balance sheet that shows assets, liabilities, and the aggregate difference (or net position). The statement of results of operations shows revenues and other financing sources, expenses, and the resulting change in net position.

The financial statements are different from agency reports that are used to monitor and control budgetary resources; thus, they provide supplementary information that may be useful to the President, Congress, the Department of the Treasury, GAO, agency managers, and other interested parties. The additional information, however, may not be as important as the discipline that agencies must develop in order to produce it. In order to obtain unqualified audit opinions, agencies not only must improve and integrate their accounting systems, but must also strengthen their managerial control over resources and activities at all levels.

The OMB Director prescribes the form and content of the financial statements. In 2001, the OMB Director required that agencies combine annual performance reports pursuant to the Government Performance and Results Act with the CFO Act financial statements into a consolidated Performance and Accountability Report.[827] At the same time, a schedule of accelerated deadlines was established, with the reports covering FY2002 due February 1, 2003, and FY2003 due January 30, 2004; and beginning with FY2004, the performance and accountability reports are due November 15th.[828]

---

[826] P.L. 107-289, 116 Stat. 2049.

[827] Pursuant to authority provided in the Reports Consolidation Act of 2000 (P. L.106-531; 114 Stat. 2537).

[828] U.S. Office of Management and Budget, Form and Content of Agency Financial Statements, Bulletin No. 01-09, Sept. 25, 2001.

Evidence indicates steady improvement in compliance with the audited financial statements requirements, as more agencies receive clean, or unqualified, opinions. By FY2001,18 CFO Act agencies had received a clean opinion, but OMB noted that agencies have achieved this record of unqualified opinions despite major problems with their financial systems, "by expending significant resources and making extensive manual adjustments after the end of the fiscal year."[829] Some, including GAO, have expressed concern about agencies' capabilities to meet the accelerated deadlines.[830] In August 2003, OMB offered a decidedly upbeat assessment of experiences with the FY2002 financial statements, which were due February 1, 2003, nearly a month earlier than previously:

Not only did all 24 agencies subject to the CFO Act meet this new, shorter deadline, but a record 21 of 24 major departments and agencies received unqualified, or clean, opinions on their 2002 audits. In addition, the agencies combined their financial statements with their performance reports to provide information about agency finances and program performance in one document. Just two weeks later, all agencies met the February 15 deadline for producing for the first time quarterly financial statements.[831]

The growing number of agency financial statements receiving clean opinions may partially reflect increased attention in the executive branch. The Bush Administration in 2001 designated improving financial performance as one of five government-wide initiatives in the President's Management Agenda. In 2002, OMB devised a management scorecard to grade agencies on their progress; one of the core criteria for financial performance is achieving unqualified and timely opinions of the annual financial statements.[832] Obtaining an unqualified opinion on the government-wide financial statements has yet to be achieved, however. In March 2003, the General Accounting Office, for the sixth straight

---

[829] U.S. Office of Management and Budget, 2002 Federal Financial Management Report (Washington, May 1, 2002), p. 11, available at: [http://www.whitehouse.gov/omb/financial/2002_report.pdf, visited Dec. 18, 2003.

[830] U.S. General Accounting Office, Financial Management: Sustained Efforts Needed to Achieve FFMIA Accountability, GAO-03-1062, Sept. 2003, p. 16.

[831] U.S. Office of Management and Budget, 2003 Federal Financial Management Report (Washington, Aug. 2003), p. 16, available at: [http://www.whitehouse.gov/omb/financial/2003_report_final.pdf, visited Dec. 18, 2003.

[832] See CRS Report RS21416, The President's Management Agenda: A Brief Introduction, by Virginia A. McMurtry; and U.S. Office of Management and Budget, Fiscal Year 2004 Budget of the U.S. Government, Performance and Management Assessments (Washington: GPO, 2003), pp. 1-7.

year, issued a disclaimer of opinion following its audit of the government-wide consolidated statements for FY2002.[833]

Three new CFO positions have been created. These additions, however, are not identical to the other 24 CFO positions previously established.[834] In 1993, the law creating the Corporation for National and Community Service (CNCS) provided for a chief financial officer, to be appointed by the President, with advice and consent of the Senate; the listing of duties for the CFO includes some language identical to that found in 31 USC § 902, but other provisions are not the same.[835] Another CFO position came into being early in 2001. A provision in the Treasury and General Government Appropriations Act, 2000, established a new CFO position within the Executive Office of the President (EOP).[836] The CFO for the EOP generally is to "have the same authority and perform the same functions" as other agency CFOs. However, the President may determine that certain statutory provisions applicable to other agency CFOs shall not apply to the new position; Congress must be notified of any such exemptions.

The Homeland Security Act of 2002 provided for a third new CFO position.[837] The law makes no reference to the CFO Act or to Chapter 9 of Title 31. The CFO in the Department of Homeland Security (DHS) is appointed by the President with no Senate confirmation requirement. In addition, unlike all the other CFOs, who report directly to the agency head, the CFO for DHS may report to the Secretary, or to "another official of the Department, as the Secretary may direct."[838] Measures received action in the first session of the 108th Congress to bring the CFO in DHS directly under the CFO Act.[839]

---

[833] U.S. General Accounting Office, Fiscal Year 2002 U.S. Government Financial Statements: Sustained Leadership and Ovesight Needed for Effective Implementation of Financial Management Reform, GAO-03-572T, Apr. 8, 2003.

[834] For more detailed consideration of differences among CFO positions, see CRS Report RL31965, Financial Management in the Federal Government: Efforts to Improve Performance, by Virginia A. McMurtry, pp. 4-5.

[835] P. L. 103-82; 107 Stat. 882, 42 U.S.C. § 12651f.

[836] P. L. 106-58, Sept. 29, 1999; 113 Stat. 430. The provisions relating to the new CFO position are contained in Sec. 638; 113 Stat. 475.

[837] P. L. 107-296, Sec. 103; 116 Stat. 2145.

[838] Ibid., Sec. 702, 116 Stat. 2219.

[839] On Nov. 21, 2003, S. 1567, as amended, passed the Senate by unanimous consent, and on Nov. 25, 2003, S. 1567 was held at the desk in the House, in preparation for floor action. Previously, two House committees ordered reported a companion measure, H.R. 2886. The legislation also deletes the Federal Emergency Management Agency from the listing of CFO agencies, so that

Careful oversight of ongoing activities in the executive branch to improve financial management in the federal government, particularly developments relating to consolidated financial statements, remains an important concern for Congress. With enactment of the Accountability of Tax Dollars Act of 2002, 78 more agencies are required to prepare annual audited financial statements. The ultimate issue may be whether or not the availability of such statements eventually contributes to different and better decisions.

Selected Source Reading

Callahan, John J. "New Frontiers for Federal CFOs." Public Manager, vol. 29 (summer 2000), pp. 13-16.

David, Irwin D. "Financial Information for Policy, Program, and Operating Officials." Journal of Government Financial Management, vol. 51 (spring 2002), pp. 10-17.

Peters, Katherine McIntire. "Fixing Finances" and "Making Changes." Government Executive, vol. 32 (June 2000), p. 68.

Peters, Katherine McIntire. "Making Change." Government Executive, vol. 32 (June 2000), pp. 70-78.

Steinberg, Harold I. "The Chief Financial Officers Act: A Ten Year Progress Report." Government Accountants Journal, vol. 49 (winter 2000), pp. 44-52.

U.S. Congress. House. Committee on Government Reform. Subcommittee on Government Efficiency and Financial Management. Consolidated Financial Statements of the Federal Government for Fiscal Year 2002. Hearing. April 8, 2003, available at: [http://reform.house.gov/GEFM/Hearings/EventSingle.aspx?EventID=380], visited December 18, 2003.

CRS Report RL31965. Financial Management in the Federal Government: Efforts to Improve Performance, by Virginia A. McMurtry.

Virginia McMurtry

FEMA, now moved to the Department of Homeland Security, is not required to prepare separate financial statements.

H. Government Management Reform Act of 1994

Statutory Intent and History

The Government Management Reform Act (GMRA) of 1994 (108 Stat. 3410)[840] incorporated "reinventing government" principles from the National Performance Review (NPR)[841] to pursue needed reforms, particularly with regard to federal personnel and general and financial management. Based upon a six-month study, the NPR Final Report offered over 380 major recommendations for creating "a government that works better and costs less."[842] Several of the NPR recommendations were implemented by executive action, but others required statutory change. The Clinton Administration forwarded a wide-ranging draft measure incorporating the needed legislative provisions, which was introduced in the House on October 28, 1993, as the "Government Reform and Savings Act" (H.R. 3400). An amended version passed the House on November 23, 1993.

Although H.R. 3400 had been jointly referred to 17 House committees having jurisdiction over particular provisions in the measure (11 of which took some action on the measure and six of which were discharged of it), the situation was different in the Senate. Under Senate rules, bill referral goes to the committee that has jurisdiction over the subject matter that predominates in the text; multiple referrals are less common than in the House, since they require unanimous consent of the Senate. So, when the House-passed version of H.R. 3400 was submitted to the Senate, it was referred only to the Governmental Affairs Committee because of its scope as an omnibus government reform bill. Following action by this committee, it was expected that other Senate committees would consider those sections falling within their jurisdictions. Eventually, the Governmental Affairs Committee reported a new bill, S. 2170, much narrower in scope than the original H.R. 3400, and containing only those provisions falling under the committee's jurisdiction, since no other committee took up the House-passed measure.[843] During floor consideration in the Senate, additional provisions were dropped, including enhanced federal debt collection procedures.

---

[840] Codified at 31 U.S.C. § 331, § 501nt, § 1113 nt, prec.§ 3301, § 3301 nt, § 3332, § 3515, and § 3521. Also at 2 U.S.C. § 31, § 31 nt; 3 U.S.C. §104; 5 U.S.C. § 5318, § 6304 and nt; and 28 U.S.C. § 461.

[841] On March 3, 1993, President Bill Clinton announced a six-month performance review of the federal government, under the leadership of Vice President Al Gore. The NPR focused primarily on process, how to make the government function more efficiently and effectively.

[842] U.S. Executive Office of the President, From Red Tape to Results: Creating a Government That Works Better & Costs Less, National Performance Review (Washington: GPO, 1993), pp. 134-153, 160-168.

[843] See U.S. Congress, Senate Committee on Governmental Affairs, Government Management Reform Act of 1994, S.Rept. 103-281, 103rd Cong., 2nd sess. (Washington: GPO, 1993).

On October 13, 1994, President Clinton signed S. 2170 into law, "An Act to provide a more effective, efficient, and responsive Government." In his signing statement, the President noted that, in passing the measure, "[T]he Congress has helped ensure that the Federal Government's managers will have the financial information and flexibility they need to make sound policy decisions and manage resources." He also praised provisions in the GMRA contributing to improved federal financial accountability as well as cutting costs.[844]

Major Provisions

Title I of the Government Management Reform Act of 1994, "Limitation on Pay," requires that automatic cost of living raises for Members of Congress, the Executive Schedule, and the judiciary not exceed those given to General Schedule (GS) federal employees. Title II, "Human Resource Management," limits the number of annual leave days that Senior Executive Service (SES) employees may accrue.

Title III, "Streamlining Management Control," strives to improve the efficiency of federal agencies in meeting statutory requirements for reports to Congress. It allows the Director of the Office of Management and Budget, in his annual budget submission, to publish recommendations to eliminate or consolidate duplicative or obsolete reporting requirements and to adjust deadlines to achieve a more efficient workload distribution or improve the quality of reports.

Title IV contains the "Federal Financial Management Act of 1994," covering a variety of issues, including electronic funds transfer, franchise funds, reporting requirements, and audited financial statements.

Section 402 aids federal agencies in the conversion to electronic delivery of government payments. The section states that all federal wage, salary, and retirement payments shall be paid to recipients by electronic funds transfer, starting on January 1, 1995, for new employees or recipients. Recipients may have the requirement waived by written request. The Secretary of the Treasury may waive the requirement for a group of recipients upon request by the head of an agency, based on standards prescribed by Treasury.

Section 403 authorizes the establishment of franchise funds in six executive agencies on a pilot program basis for five years. The franchising concept draws from the reinventing government principles of competition and the injection of market mechanisms into government operations. Franchise programs would offer administrative support services, such as payroll operations and accounting services, to the participating agency and to other federal agencies on a

---

[844] U.S. Executive Office of the President, Weekly Compilation of Presidential Documents, vol. 30 (Oct. 17, 1994), pp. 2006-2007.

reimbursable basis. The monopoly of internal service providers within federal agencies would be eliminated because office managers would be free to buy from the best provider. Franchise programs will expand or decline with the demand for their services.

Section 404 provided flexibility for the OMB Director in the timing and presentation of statutorily required financial management reports from executive branch agencies to OMB or the President, and from agencies or OMB to Congress.

Flexibility was provided to improve the efficiency of executive branch performance in financial management reporting. This authority initially was limited, however, to reports required by statute to be submitted between January 1, 1995, and September 30, 1997. Adjustments in reporting were made only after consultation with the chairman of the Senate Committee on Governmental Affairs and the chairman of the House Committee on Government Reform and Oversight; written notification to Congress must follow.

Section 405 expands requirements for executive branch agency financial statements contained in Section 303(a) of the Chief Financial Officers Act of 1990 (see discussion elsewhere in this compendium). Section 405(a) requires all 24 agencies covered under the CFO Act to have agency-wide audited financial statements, beginning with FY1996. The annual statements, initially due February 28, 1997, must cover all accounts and associated activities. The requirement is intended to contribute to cost-effective improvements in government operations. The OMB Director is authorized to require additional audited financial statements for components of CFO Act agencies. The OMB Director is also given authority to prescribe the form and content of financial statements.

Section 405(b) provides that for each audited financial statement required from the agency, the person who audits the statement (the inspector general or an independent external auditor) must submit a report on the audit to the head of the agency. This report is to be prepared in accordance with generally accepted government auditing standards.

Section 405(c) of the GMRA further requires that a consolidated audited financial statement for all accounts and associated activities in the executive branch be prepared by the Secretary of the Treasury, in coordination with the OMB Director, and be audited by the Comptroller General.[845] The first such statement,

---

[845] Although all accounts and activities of the executive branch were included in the government-wide financial statement, only CFO Act-covered accounts were audited. Because accounts not covered by the CFO Act constitute only a small portion of executive branch activities, these accounts did not have a significant effect on the government-wide financial statement.

covering FY1997, was submitted to the President and Congress on March 31, 1998. This financial statement is intended to reflect the overall financial position of the executive branch, including assets, liabilities, and results of operations of the executive branch. The specific form and contents of the financial statement are determined by the OMB Director. This financial statement is intended to provide Congress, the President, and the American public with more accurate and useful financial information on the workings of the government.

Discussion

As mentioned previously, most of the provisions in the GMRA reflect recommendations contained in the report of the National Performance Review. For example, the NPR report endorsed the idea of "franchising" internal services; the GMRA provides for a pilot program embracing the approach. Originally, it was anticipated that the pilots would be designated in the spring of 1995, operate for four years and terminate on October 1, 1999. However, delays occurred, with the six pilots not fully in operation until FY1997. In September of 1996, a provision was included in P. L. 104-208, the Omnibus Consolidated Appropriations Act of 1997, extending the pilot program through FY2001. The GMRA required that a report evaluating the franchise funds in the pilot program was due to Congress "within 6 months after the end of fiscal year 1997." A report, addressing the elements specified in the law, was submitted on schedule in March 1998, but as an interim progress report, rather than a final evaluation of the experiences with the six franchise funds included in the pilot program.[846]

The NPR report also called for eliminating unnecessary reports and simplifying the reporting process. The GMRA encouraged weeding out where possible and otherwise consolidating existing reports in an ongoing effort to simplify reporting requirements and to maximize the usefulness of executive branch reports to Congress. Provisions in the Reports Consolidation Act of 2000 (P. L. 106-531; 114 Stat. 2537) restored and enhanced the consolidation authority for financial and performance management reports initially given to the OMB Director in GMRA and, moreover, made the authority permanent. In 2001, the OMB Director required that agencies combine annual performance reports pursuant to the Government Performance and Results Act with the CFO Act financial statements into a consolidated Performance and Accountability Report. At the same time, a schedule of accelerated deadlines was established, with the reports covering FY2003 due by January 30, 2004; beginning with FY2004, the performance and accountability reports are due by November 15th.[847]

---

[846] See The Franchise Fund Pilot Program: An Interim Progress Report. Report to Congress [Washington, 1998]. This interim report was prepared jointly by the Office of Management and Budget, the Entrepreneurial Government Committee of the Chief Financial Officers Council, and the six franchise fund pilots.

[847] OMB, Form and Content of Agency Financial Statements, Bulletin No. 01-09, Sept. 25, 2001.

Another major recommendation in the NPR report was to use the Chief Financial Officers Act of 1990 to improve financial services. The provisions in GMRA relating to annual audited financial statements for federal agencies embody this approach, as discussed.[848]

Selected Source Reading

Peters, Katherine McIntire. "Dollars and Sense." Government Executive, vol. 30 (June 1998), pp. 43-48.

U.S. Congress. Senate. Committee on Governmental Affairs. Government Management Reform Act of 1994. Report to accompany S. 2170. S.Rept. 103 281. 103rd Congress, 2nd session. Washington: GPO, 1994.

——. Reports Consolidation Act of 2000. Report to accompany S. 2712. S.Rept. 106-337. 106th Congress, 2nd session. Washington: GPO, 2000.

CRS Report RL31965, Financial Management in the Federal Government: Efforts to Improve Performance, by Virginia A. McMurtry.

U.S. Office of the Vice President. Improving Financial Management. Accompanying Report of the National Performance Review. Washington: GPO, 1993.

Virginia McMurtry

[848] See "Discussion" section relating to Chief Financial Officers Act elsewhere in this compendium for perspective on the CFO Act amendments contained in GMRA providing for the audited financial statements.

I. Accountability of Tax Dollars Act of 2002

Statutory Intent and History

The Accountability of Tax Dollars Act (ATDA) of 2002 (P.L. 107-289; 116 Stat. 2049) was intended "to expand the types of Federal agencies that are required to prepare audited financial statements to all executive branch agencies in the federal government."[849]

Testifying in support of the legislation, Representative Pat Toomey stated that he first introduced the measure in the 106th Congress (H.R. 5521) "as a good government measure to combat waste, fraud, and abuse at Federal agencies.... I decided to introduce legislation when I learned, to my surprise, that many Federal agencies are simply not required by law to prepare audited financial statements, even though this is a fundamental part of good management and oversight."[850]

In the 107th Congress, H.R. 4685 was introduced on May 8, 2002, by Representative Toomey, with bipartisan cosponsors, and referred to the House Committee on Government Reform. On May 14, 2002, the Subcommittee on Government Efficiency, Financial Management, and Intergovernmental Relations held a hearing, and on June 18, 2002, approved the bill, as amended, by unanimous consent. On October 7, 2002, H.R. 4685 was considered in the House under suspension of the rules and passed, as amended, by voice vote.

A companion bill, S. 2644, was introduced in the Senate on June 19, 2002, and referred to the Committee on Governmental Affairs. Markup was held on October 16, 2002, and S. 2644, with a substitute amendment, was reported favorably by a vote of 9-0. On the following day, the Senate passed H.R. 4685 by unanimous consent. The measure was signed into law on November 7, 2002, with the first audited statements pursuant to the act due on March 1, 2003.

Major Provisions

The Accountability of Tax Dollars Act amends Title 31, United States Code, to bring almost all executive branch agencies under the requirement for preparation of annual audited financial statements that previously applied only to the 24 major departments and agencies covered by the Chief Financial Officers (CFO)

---

[849] U.S. Congress, Senate Committee on Governmental Affairs, Accountability of Tax Dollars Act of 2002, S.Rept. 107-331, 107th Cong., 2nd sess. (Washington: GPO, 2002), p. 1.

[850] U.S. Congress, House Committee on Government Reform, Subcommittee on Government Efficiency, Financial Management, and Intergovernmental Relations, H.R. 4865, the Accountability of Tax Dollars Act of 2002, hearing, 107th Cong., 2nd sess. (Washington: GPO, 2003), p. 8.

Act.[851] Specifically, Section 2(a) changes the list of agencies covered by the audited annual financial statements requirement in 31 U.S.C. § 3515 by deleting the cross-reference to CFO Act agencies and inserting "each covered executive agency." In addition, the new law changed the initial due date for the audited financial statements from March 1, 1997, to March 1, 2003.

The new law further amends Section 3515 by adding two new subsections. Subsection 3515(e) allows the Director of OMB to exempt an agency from the requirement to prepare an annual audited financial statement in a fiscal year under certain circumstances. OMB discretion is possible when the agency budget does not exceed $25 million, and the OMB Director determines the exercise is unwarranted due to the absence of risks associated with the agency's operations, the agency's demonstrated performance, or other relevant factors. If OMB grants such exemptions, the director is to notify the House Committee on Government Reform and the Senate Committee on Governmental Affairs annually of the agencies involved and the reasons for each exemption. Subsection 3515(f) defines the term "covered executive agency" to mean any other executive agency not required by another provision of law to prepare and submit annually to Congress and OMB an audited financial statement. Specifically excluded are bodies subject to Chapter 91 of Title 31 (mainly government corporations).

Section 2(b) of ADTA provides waiver authority for the OMB Director during a transition period under the new law. Specifically, the OMB Director may waive the application of the new law to any non-CFO Act agency for two years following enactment.

Discussion

The Accountability of Tax Dollars Act amends Title 31, United States Code, to expand the types of federal agencies that are required to prepare audited financial statements each year. Prior to its enactment, the 24 major departments and agencies covered by the CFO Act were required to prepare annual financial statements to be audited by their Offices of Inspector General (IG) or outside contractors designated by the IGs. A few agencies, such as the U.S. Postal Service, were required by agency-specific legislation to prepare audited financial statements. Over 20 entities were also previously required to prepare annual financial statements and have them audited pursuant to the Government Corporation Control Act (Chapter 91 of Title 31, described elsewhere in this compendium). Several independent agencies, such as the Federal

[851] 104 Stat. 2838. See discussion of the CFO Act elsewhere in this compendium.

Communications Commission and the Federal Trade Commission, voluntarily prepared audited financial statements.[852]

As noted, the ATDA was passed with virtually no opposition in the 107th Congress, both in committee and during House and Senate floor consideration. The language relating to coverage did evolve during the legislative process, however. Both the House and Senate bills, as introduced, provided a blanket exemption for agencies with budget authority for the fiscal year of less than $25 million. Testimony received during a hearing on H.R. 4685 may have proved important in this regard, when an official from the Federal Elections Commission suggested:

Agency operations and the types of programs administered by an agency should be more important than the size of budget in determining the need for audited financial statements. For example, an agency with a budget less than $25 million that has fiduciary responsibility for a trust fund, administers a grant program, or operates revenue-generating programs may be the type of agency that should prepare audited financial statements ...[853]

As enacted, the ATDA allows the OMB Director to exempt agencies with budgets under $25 million from the audited statements requirement under certain circumstances, but the exemption is not automatic.

With respect to agencies subject to the new law, it is interesting to note that 49 agencies were included as coming under the expanded requirements (before any possible OMB exemptions) in the Senate report accompanying S. 2644.[854] A month later, after the bill was signed into law, a memorandum from the OMB Director listed 78 agencies affected by ATDA.[855]

The OMB Director also exercised the provision in the law to waive the requirement during an initial transition period, allowing agencies not having prepared audited financial statements in the past to have an exemption for FY2002 for the annual financial statements. In the same December 2002

---

[852] U.S. General Accounting Office, "Survey Results of Selected Non-CFO Act Agencies' Views on Having Audited Financial Statements," briefing to the Honorable Patrick J. Toomey, House of Representatives, Nov. 30, 2001, p. 15. Reprinted in hearing on H.R. 4685, p. 27.

[853] Hearing on H.R. 4685, p. 85.

[854] S. Rept. 107-331, pp. 3-4.

[855] U.S. Office of Management and Budget, "Requirements of the Accountability of Tax Dollars Act of 2002," Memorandum for Heads of Selected Executive Agencies from Mitchell E. Daniels Jr., Dec. 6, 2002. There may be further modifications to the list of agencies coming under ATDA's expanded requirement for financial statements, because of possible uncertainty with the statutory definition of covered agency, as described above.

memorandum, the director noted that the newly covered agencies, along with the 24 CFO agencies, are all subject to the provisions of OMB Bulletin 01-09, Form and Content of Agency Financial Statements, beginning with FY2003.[856] This bulletin requires agencies to consolidate their audited financial statements and other financial and performance reports into combined Performance and Accountability Reports and accelerates the deadlines for submission.[857] OMB subsequently waived the requirement in Bulletin 01-09 for preparation and submission to OMB of quarterly unaudited financial statements for FY2003 for the agencies covered by ATDA.[858]

An issue that may be revisited is whether the ATDA agencies should be subject to the additional requirements of the Federal Financial Management Act (FFMIA), as are the 24 CFO Act agencies. The FFMIA requires covered agencies to implement and maintain financial management systems that comply substantially with federal financial management system requirements, applicable federal accounting standards, and the United States General Ledger at the transaction level.[859] H.R. 4685, as reported out of subcommittee, apparently contained language bringing ATDA agencies under the accounting standards provisions of FFMIA.[860] Opposition from the Bush Administration resulted in deletion of the FFMIA provisions prior to floor consideration. As Representative Janice Schakowsky commented during House floor debate:

> *Unfortunately, the bill we have on the floor today is not the bill we have passed out of our subcommittee [House Subcommittee Government Efficiency, Financial Management and Intergovernmental Relations]. The bill we have passed included a section that required the agencies covered under this bill to conform to the accounting standards set out in the Federal Financial Management Improvement Act of 1996. The*

---

[856] U.S. Office of Management and Budget, Form and Content of Agency Financial Statements, Bulletin No. 01-09, Sept. 25, 2001.

[857] Previously, CFO agencies had a deadline of 150 days after the end of the fiscal year (i.e., early March) to submit the reports, but the due date for the combined FY2002 reports was moved up to February 1, 2003; for FY2003, to January 30, 2004; and beginning with FY2004, to November 15, just six weeks after the close of the fiscal year. (See discussion of the CFO Act elsewhere in this compendium.)

[858] U.S. Office of Management and Budget, "Accountability of Tax Dollars Act of 2002 — Implementation Guidance and Executive Forum March 31," Memorandum to Heads of Executive Agencies Subject to Provisions of the Accountability of Tax Dollars Act of 2002, from Mark W. Everson, Mar. 20, 2003.

[859] 110 Stat. 3009-389; 31 U.S.C. § 3512 note. For further background on FFMIA, see discussion elsewhere in this compendium.

[860] There was no written report to accompany H.R. 4685.

> *administration insisted that those [FFMIA] provisions be stripped from the bill, or it would block the bill from coming before the House today.... I am afraid that the administration's opposition to the accounting standards that were in this bill is just one more attempt to make sure that OMB, and not Congress, sets the standards by which agencies are judged.*[861]

As one of five government-wide initiatives under the rubric of the President's Management Agenda,[862] improved financial performance in executive branch agencies has received considerable attention and emphasis from OMB recently. Improving financial management in the federal government remains an important concern for Congress as well. With enactment of ATDA, 78 more agencies are required to prepare annual audited financial statements. Congressional scrutiny of the initial round of audited financial statements prepared by agencies subject to ATDA might prove an informative focus for oversight. The ultimate question may be whether the availability of audited financial statements improves the quality of decisionmaking in the federal government and furthers accountability to the American taxpayers, as envisaged in the ATDA.

Selected Source Reading

CRS Report RL31965. Financial Management in the Federal Government: Efforts to Improve Performance, by Virginia A. McMurtry.

Congress. House. Committee on Government Reform. Subcommittee on Government Efficiency, Financial Management, and Intergovernmental Relations. H.R. 4865, the Accountability of Tax Dollars Act of 2002. Hearing. 107th Congress, 2nd session, May 14, 2002. Washington: GPO, 2003.

Congress. Senate. Committee on Governmental Affairs. Accountability of Tax Dollars Act of 2002. Report to accompany S. 2644. 107th Congress, 2nd session. S.Rept. 107-331. Washington: GPO, 2002.

Virginia McMurtry

---

[861] Rep. Janice Schakowsky, remarks in the House, Congressional Record, daily edition, vol. 148, Oct. 7, 2002, p. H7043.

[862] See U.S. Office of Management and Budget, The President's Management Agenda — FY2002 (Washington: OMB, 2001). For an overview of the PMA, see CRS Report RS21416, The President's Management Agenda: A Brief Introduction, by Virginia A. McMurtry.

J. Federal Managers' Financial Integrity Act of 1982

Statutory Intent and History

The Federal Managers' Financial Integrity Act (FMFIA) of 1982,[863] which amended the Accounting and Auditing Act of 1950, was designed to improve the government's ability to manage its programs. It emerged in the early 1980s and is often seen as the opening to other attempts along this line, including the Chief Financial Officers Act of 1990, the Federal Financial Management Improvement Act of 1996, and the Accountability of Tax Dollars Act of 2002.[864] Adoption of FMFIA followed the conclusions of a number of studies — from congressional committees, the General Accounting Office (GAO), inspectors general, and the executive agencies themselves — that documented significant weaknesses in internal financial and management controls, including inadequate and inaccurate accounting systems and financial reports. These weaknesses, in turn, were seen as contributing to wasteful spending, poor management, ineffective programs, fraud, and billions of dollars in losses.

FMFIA recognized that strong internal controls and accounting systems would help to ensure the proper use of funds and resources, compliance with statutes and regulations, and preparation of reliable financial reports for oversight and policymaking. The enactment, consequently, provides for ongoing evaluations of the internal control and accounting systems that protect federal programs against fraud, waste, abuse, and mismanagement. FMFIA further mandates that the heads of federal agencies report annually to the President and Congress on the condition of these systems and on their actions to correct any material weaknesses which the reports identified. Regulations implementing FMFIA's requirements for financial management systems are contained in Office of Management and Budget (OMB) Circular No. A-127, dealing with management accountability and control.

Major Provisions

Purposes and Objectives. The act requires the head of each executive agency to establish internal accounting and administrative controls, consistent with standards the Comptroller General prescribes, that reasonably ensure three principal objectives:

- that obligations and costs comply with applicable law;

---

[863] P.L. 97-255, 96 Stat. 814-815; codified at 31 U.S.C. § 3512.

[864] For an overview of these and related efforts, see CRS Report RL31965, Financial Management in the Federal Government: Efforts to Improve Performance, by Virginia A. McMurtry.

- that all assets are safeguarded against waste, loss, unauthorized use, and misappropriation; and
- that revenues and expenditures applicable to agency operations are recorded and accounted for properly, so that accounts and reliable financial and statistical reports can be prepared and accountability of the assets maintained.

The standards prescribed by the Comptroller General specifically include those designed to ensure the prompt resolution of all audit findings.

Guidelines. To meet these requirements, FMFIA instructed the Director of OMB, in consultation with the Comptroller General, to establish guidelines that the head of each agency must follow in evaluating the internal accounting and administrative control system of the agency. The OMB Director, however, is authorized to change a guideline when considered necessary.

Required Statements and Reports. By December 31 of each year (beginning in 1983), the head of each executive agency, based on such evaluations, prepares a statement on whether or not the systems of the agency comply with the criteria cited above. If the systems do not comply, then the head issues a report identifying any material weaknesses in the systems and describing the plans and schedule for correcting the weaknesses. Section 4 of the act provides that a separate report state whether the accounting system of the agency conforms to the principles, standards, and requirements of the Comptroller General.

The reports and statements are signed by the head of the agency and submitted to the President and Congress. These products in their entirety are also made available to the public, with an exception, however, for certain sensitive or classified information: i.e., information is deleted if it is specifically prohibited by law or required by executive order to be kept secret in the interest of national security.

The Reports Consolidation Act (RCA) of 2000 (P.L. 106-531; 114 Stat. 2537), approved at the end of the 106th Congress, has implications for FMFIA reports. The new statute is intended to overcome the duplication of effort and lack of coordination among the multiple financial and performance management reporting requirements within an agency. To do so, RCA authorizes the consolidation of such reports into a single annual report from each agency to achieve several purposes: enhance efficiency and coordination among the reporting entities; improve the quality of the information; and provide it in a more meaningful and useful format for Congress, the President, and the public.

Provisions Affecting Offices of Inspectors General. FMFIA also affects offices of inspector general (OIGs), created earlier by the Inspector General Act of 1978 (92 Stat. 1101). Section 3 of the act requires that the President include in the supporting detail of his budget submission the amounts of appropriations he requested for each OIG. Congressional committees are authorized to solicit from

the IG additional information concerning the amount of appropriations he or she requested when the request was originally submitted to agency management or OMB. This provision was designed to help protect the independence of IG offices and ensure their adequate funding. Along these same lines, the Inspector General Act Amendments of 1988 (102 Stat. 2529) provided for a separate appropriations account for each office of inspector general in a federal establishment (i.e., all the cabinet departments and the larger agencies).

Reference in the Chief Financial Officers Act. The Chief Financial Officers (CFO) Act of 1990 (104 Stat. 2847) is connected to the Federal Managers' Financial Integrity Act requirements. The CFO Act calls upon the Director of OMB to submit a financial management status report to appropriate committees of Congress. Part of this report is to be a summary of reports on internal accounting and administrative control systems submitted to the President and Congress as required by FMFIA.

Discussion

Passage of the Federal Managers' Financial Integrity Act in 1982 built upon some of the same concerns that had prompted enactment of the Inspector General Act four years before. FMFIA was boosted at the time by its incorporation as a top priority in Reform '88; these were the Reagan Administration initiatives begun in 1982, which were intended to strengthen management controls in the federal government. The statute was later enhanced by provisions in the Chief Financial Officers Act of 1990 and now plays a role in the President's Management Agenda, initiated by President George W. Bush in 2001.[865] FMFIA continues to provide a framework for strengthening, standardizing, and evaluating internal control and accounting systems as well as for reporting on relevant findings and corrective action. These developments paved the way for high expectations for ferreting out the root causes of waste, fraud, and mismanagement; providing federal managers with specifics about what is wrong and how to correct it; and informing Congress and the public about the underlying problems and their remedies.

FMFIA has received mixed reviews over the years. Initially, it was seen as not reaching its high expectations, according to some commentators who asserted that the law had been ignored or improperly and too narrowly implemented. This occurred, critics contended, because of an over-concern with the process rather than a focus on the objectives of the legislation, confusion or misunderstanding over the law's terminology, and restrictive interpretations of some of its provisions. FMFIA's failure to produce the results intended by

[865] U.S. Office of Management and Budget, The President's Management Agenda — FY2002 (Washington: OMB, 2001); and Fiscal Year 2004 Budget of the U.S. Government, Performance and Management Assessments (Washington: GPO, 2003), pp. 1-7. For an overview and other citations, see CRS Report RS21416, The President's Management Agenda: A Brief Introduction, by Virginia A. McMurtry.

Congress, in part, led to the later passage of other laws (discussed elsewhere in this compendium) designed to improve the general and financial management of the government. These included the Chief Financial Officers Act of 1990, the Government Management Reform Act of 1994, and the Federal Financial Management Improvement Act of 1996.

Since then, however, FMFIA and the related statutes have received more favorable reviews and, evidently, have had a more beneficial impact on federal agencies. According to an OMB study, for instance, "from 2001 to 2002, the number of FMFIA material weaknesses and nonconformances [found] dropped by 22 percent …."[866] Nonetheless, FMFIA and its statutory partners have significant challenges to meet in developing a healthy financial system for the U.S. government across the board.[867]

Selected Source Reading

Cottingham, Warren. "Assessing Implementation of the Financial Integrity Act: GAO Assists OMB." GAO Review, vol. 19 (winter 1984), pp. 20-24.

Dempsey, Charles L. "Federal Managers' Financial Integrity Act: The Role of the Inspector General." Government Accountants Journal, vol. 32 (summer 1983), pp. 15-17.

"Financial Management and Asset Protection." The Journal of Public Inquiry, vol. 1 (spring/summer 2000), pp. 25-34.

Points, Ronald J. and Michelson, Bruce. "Internal Control Standards for the Federal Government." Government Accountants Journal, vol. 32 (1983), pp. 9-14.

Riso, Gerald R. "Reviving Management Controls." Government Executive, vol. 28 (May 1996), pp. 67-68.

Congress. House. Committee on Government Operations. Subcommittee on Legislation and National Security. Implementation of the Federal Managers' Financial Integrity Act. Hearings. 99th Congress, 2nd session. Washington: GPO, 1986.

Congress. Senate. Committee on Governmental Affairs. General Accounting Office Response to Inadequate Management Controls. Hearings. 101st Congress, 1st session. Washington: GPO, 1990.

---

[866] U.S. Office of Management and Budget, 2003 Federal Financial Management Report, p. 12.

[867] Ibid.

General Accounting Office. Financial Integrity Act: Inadequate Controls Result in Ineffective Federal Programs and Billions in Losses. AFMD-90-10. Washington: GAO, 1989.

——. Financial Management: Sustained Efforts Needed to Achieve FFMIA Accountability. GAO-03-1062. September 2003.

——. Internal Control Management and Evaluation Tool. GAO-01-131G. February 2001.

——. Standards for Internal Control in the Federal Government. AIMD-00-21.3.1 November 1999.

CRS Report RL31965. Financial Management: Efforts to Improve Performance, by Virginia A. McMurty.

CRS Report RS21416. The President's Management Agenda: A Brief Introduction, by Virginia A. McMurtry.

U.S. Office of Management and Budget. Federal Financial Management Report (2003). Washington: OMB, 2003.

Frederick M. Kaiser

K. Federal Financial Management Improvement Act of 1996

Statutory Intent and History

The Federal Financial Management Improvement Act of 1996 (110 Stat. 3009389; 31 U.S.C. § 3512 note) incorporates in statute certain financial management system requirements already established as executive branch policy. The law also requires auditors to report on agency compliance with these requirements, and agency heads and management to correct deficiencies within certain time periods.

The act has seven purposes:

- provide for consistency in agency accounting from year to year, and for uniform accounting standards throughout the federal government;
- require federal financial management systems to support full disclosure of financial data so that programs and activities can be considered on their full costs and merit;
- increase accountability and credibility of federal financial management;
- improve performance, productivity, and efficiency of federal financial management;
- establish financial management systems that support controlling the cost of the federal government;
- build upon and complement the Chief Financial Officers Act, the Government Performance and Results Act, and the Government Management Reform Act; and
- increase the capability of agencies to monitor budget execution through reports that compare spending of resources to results of activities.

Enactment of the Federal Financial Management Improvement Act of 1996 (FFMIA) reflects an ongoing effort to reform financial management in the federal government. The 1996 law builds upon prior legislation, including the Chief Financial Officers Act of 1990, the Government Performance and Results Act of 1993, and the Government Management Reform Act of 1994. (See separate entries in this compendium for overviews of these laws.)

The FFMIA also follows up on the work of the Federal Accounting Standards Advisory Board (FASAB). Created pursuant to a 1990 Memorandum of Understanding among the Comptroller General of the United States (who heads the General Accounting office, or GAO), the Director of the Office of Management and Budget (OMB), and the Secretary of the Treasury, FASAB was charged with developing and recommending accounting standards for the federal government.

Once reviewed and adopted by the three principals, the standards are published by OMB and GAO and go into effect. According to the Senate report which accompanied the measure, FFMIA seeks to shift the focus of reform efforts to

implementation of the agreed-upon federal accounting standards. The report further noted: "While development of the accounting standards is an enormous accomplishment, however, the Committee wishes to emphasize that the benefits of good financial management will flow from the implementation of these standards and not simply their promulgation."[868]

After a rather complicated legislative history, the Federal Financial Management Improvement Act was enacted as a part of the Omnibus Consolidated Appropriations Act for FY1997 (P.L. 104-208; 110 Stat. 3009, at 3009-389). Originally introduced as S. 1130 in the summer of 1995 by Senator Hank Brown, the bill was the subject of a Senate Governmental Affairs Committee hearing in December of 1995; the committee then favorably reported a substitute version offered by Senator Brown the following May, and filed a written report on July 30, 1996 (S.Rept. 104-339). The Senate passed S. 1130, as amended by the committee substitute, by unanimous consent on August 2, 1996. Companion measures to S. 1130 were introduced in the House in September (H.R. 4061 and H.R. 4319), but no further action occurred on these bills. Ultimately, both the House and the Senate agreed to the FFMIA provisions under the rubric of the conference agreement.[869] President Clinton signed H.R. 3610 into law on September 30, 1996.

Major Provisions

The Federal Financial Management Improvement Act requires federal agencies to implement and maintain financial management systems that comply substantially with federal financial management system requirements, applicable federal accounting standards, and the United States Government Standard General Ledger (SGL) at the transaction level.

The act requires auditors to report on compliance with these requirements in their financial statement audits. When noncompliance is discovered, auditors

---

[868] U.S. Congress, Senate Committee on Governmental Affairs, Federal Financial Management Improvement Act of 1996, S.Rept. 104-339, 104th Cong., 2nd sess. (Washington: GPO, 1996), p. 6.

[869] Specifically, the text of S. 1130 was approved as Amendment No. 5255 to H.R 3756, the Treasury Postal Service Appropriations, 1997, bill by the Senate on September 11, 1996. In offering the floor amendment, Senator Brown explained that, given the shortness of time left in the session, attaching the measure previously approved by the Senate (S. 1130) to the appropriations measure provided the "best hope for enacting these important reforms into law this year." The following day, however, Senate Majority Leader Trent Lott pulled the Treasury Postal Service bill from the Senate floor when it appeared hopelessly bogged down with other add-ons. Subsequently, the conference report accompanying H.R. 3610, providing for 1997 omnibus consolidated appropriations (H.Rept. 104-863), included the text of the Federal Financial Management Improvement Act as a part of the Treasury Postal Service Appropriations (as added during Senate floor consideration of H.R.3756).

shall include in their report: (1) the entity or organization responsible for the financial management systems; (2) facts pertaining to the failure to comply (including the nature and extent of noncompliance, the primary reason or cause of noncompliance, the entity or organization responsible for the noncompliance, and relevant comments from responsible officers and employees); and (3) a statement of recommended remedial actions and time frames for implementing them.

The head of each agency is also required to determine whether agency financial management systems are in compliance. The determination is based on the report on the agency-wide audited financial statements and other information the head considers relevant and appropriate. If the head agrees that the systems are not in compliance, the head (in consultation with the Director of OMB) establishes a remedial plan that includes resources, remedies, and intermediate target dates necessary to bring about substantial compliance within three years after the auditor's determination. If the agency (with concurrence of the director) determines that more than three years are needed, the remedial plan specifies the most feasible date and designates an official responsible for bringing the systems into compliance. If the head disagrees with the auditor's findings, the Director of OMB shall review the determinations and report on the findings to the appropriate committees of Congress.

The act also requires the Director of OMB and the Comptroller General to make annual reports to Congress. The latter reports on compliance with the financial management system requirements and on the adequacy of applicable accounting standards for the federal government. In addition, inspectors general report to Congress instances and reasons when an agency has not met the intermediate target dates specified in remedial plans.

The act became effective for FY1997.

Discussion

The Federal Financial Management Improvement Act put into statutory law financial management requirements that the executive branch by and large had already established. Thus, its immediate effects were likely minimal, though the requirements for expanded auditor reports and agency remedial plans, including target dates, in cases of noncompliance ought not be underestimated. Supporters of the legislation hoped that an explicit statutory basis for financial management requirements might give them greater visibility and importance, and increase the likelihood that remedial plans would receive higher priority within the agencies and OMB, as well as in annual appropriations.

In its review of FFMIA for FY1997, GAO observed that "it will take time and concerted effort to raise government financial management systems to the level

of quality and reliability envisioned in FFMIA."[870] Two years later, in commenting on the draft of the GAO report for FY1999, the Office of Management and Budget agreed with the assessment of FFMIA's compliance requirements, but contended that the report "does not give credit for progress made or improvement efforts underway by agencies." It also expressed concern that "as currently written in OMB guidance, compliance requirements were black and white — meaning an agency was either compliant or non compliant." GAO agreed that it is important to measure progress and acknowledged that "the agencies are moving in the right direction."[871]

The number of CFO agencies receiving unqualified audit opinions on their financial statements increased steadily, from 11 in FY1997 to 21 in FY2002. Nonetheless, in reviewing the annual audit reports, GAO continued to find that most of the 24 CFO agencies did not comply substantially with FFMIA requirements. In FY2002, auditors reported that 17 agencies were noncompliant with FFMIA systems requirements, 13 were noncompliant with applicable federal accounting standards, and 9 were noncompliant with the Standard General Ledger. After six years of reporting years under FFMIA, only 3 of the 24 CFO agencies complied substantially with all FFMIA requirements, while 8 agencies were reported still not to be in substantial compliance with any of the requirements.[872]

The matter of addressing fundamental problems with agency financial systems has received increased attention in the executive branch. The Bush Administration in 2001 designated improving financial performance as one of five government-wide initiatives in the President's Management Agenda (PMA). In 2002, OMB devised a management scorecard to grade agencies on their progress; one of the core criteria in the financial performance initiative is for agencies to have financial management systems meeting federal financial systems requirements and applicable federal accounting and transaction standards as reported by the agency head (i.e., be in compliance with the FFMIA requirements).[873]

---

[870] U.S. General Accounting Office, Financial Management: Federal Financial Management Improvement Act Results for Fiscal Year 1997, GAO/AIMD-98-268, Sept. 30, 1998, p. 2.

[871] U.S. General Accounting Office, Financial Management: Federal Financial Management Improvement Act Results for Fiscal Year 1999, GAO/AIMD-00-307, Sept. 2000, pp. 14, 43.

[872] U.S. General Accounting Office, Financial Management: Sustained Efforts Needed to Achieve FFMIA Accountability, GAO-03-1062, Sept. 2003, pp. 13-14.

[873] See CRS Report RS21416, The President's Management Agenda: A Brief Introduction, by Virginia A. McMurtry; and U.S. Office of Management and Budget, Fiscal Year 2004 Budget of the U.S. Government, Performance and Management Assessments (Washington: GPO, 2003), pp. 1-7. As of Sept. 30, 2003, three agencies have received a green mark on the scorecard, indicating that they have met all the core criteria for success on the financial management initiative.

Despite steady agency improvement with the audited financial statements requirements, serious problems remain. While praising the accomplishment of agencies in earning unqualified audit opinions on their financial statements, OMB offered this qualification in a 2002 report: agencies have achieved this record of unqualified opinions despite major problems with their financial systems "only by expending significant resources and making extensive manual adjustments after the end of the fiscal year."[874] As a reflection of the depth of agency difficulties with FFMIA, as of September 30, 2002, 17 of the 24 agencies reported to GAO[875] that they were planning to or were in the process of implementing new core financial systems.[876]

In its report on FFMIA compliance in 2003, GAO cautioned about an "expectation gap," given the improvements on the financial statements coupled with the relative lack of success in achieving compliance with FFMIA: "When more agencies receive clean opinions, expectations are raised that the government has sound financial management and can produce reliable, useful, and timely information on demand throughout the year, whereas FFMIA assessments offer a different perspective."[877] On the other hand, the PMA, along with efforts of the Joint Financial Management Improvement Program (JFMIP) Principals,[878] provide impetus for addressing the challenges of FFMIA. According to GAO, during FY2002, the JFMIP Principals "continued the series of regular, deliberative meetings that focused on key financial management reform issues."[879]

Congressional oversight also remains an important prod for agencies to focus on financial management reform. In his opening statement at an oversight hearing

---

[874] U.S. Office of Management and Budget, 2002 Federal Financial Management Report (Washington: May 1, 2002), p. 11, available at: [http://www.whitehouse.gov/omb/financial/2002_report.pdf], visited Dec. 11, 2003.

[875] U.S. General Accounting Office, Core Financial Systems at the 24 Chief Financial Officers Act Agencies, GAO-03-903R, June 27, 2003, p. 5.

[876] JFMIP defines "core financial systems" to include managing general ledger, funding, payments, receivables, and certain basic cost functions. See Joint Financial Management Improvement Program (JFMIP), Core Financial Systems Requirements, SR-02-01 (Washington: JFMIP, 2001).

[877] U.S. General Accounting Office, GAO-03-1062, p. 16.

[878] The JFMIP Principals are the Secretary of the Treasury, the Directors of OMB and the Office of Personnel Management, and the Comptroller General of the United States. Officially recognized in 1948, JFMIP is a cooperative effort of the principals, working with federal agencies, to improve financial management practices throughout the government.

[879] U.S. General Accounting Office, GAO-03-1062, p. 7.

on FFMIA in 2002, Subcommittee Chairman Stephen Horn observed, "We recognize that there are long-standing problems with agency financial management systems. We also recognize that correcting these deficiencies will take time. However, the requirements of this Act must be taken seriously."[880] Since FFMIA does not impose penalties for agencies that are noncompliant, as an early version of the legislation would have authorized, its effectiveness may ultimately depend upon congressional oversight and OMB insistence that agencies comply with relevant standards.

Selected Source Reading

U.S. Congress. House. House Committee on Government Reform. The Federal Financial Management Improvement Act of 1996: Are the Agencies Meeting the Challenge? Hearing before Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations. 107th Congress, 2nd session, June 9, 2002. Washington: GPO, 2003.

——. Senate. Governmental Affairs Committee. Federal Financial Management Improvement Act of 1996. S.Rept. 104-339. Washington: GPO, 1996.

U.S. General Accounting Office. Financial Management: Sustained Efforts Needed to Achieve FFMIA Accountability. GAO-03-1062. September 2003.

——. Other GAO reports on federal accounting and auditing are also available from the agency's website, [http://www.gao.gov], visited January 22, 2004, under the terms financial management or government accounting and financial management.

Joint Financial Management Improvement Program. Core Financial System Requirements. JFMIP-SR-99-4. Washington: GPO, 1999.

Office of Management and Budget. Audit Requirements for Federal Financial Statements. OMB Bulletin No. 01-02. October 16, 2000.

——. Revised Implementation Guidance for the Federal Financial Management Improvement Act, Memorandum from Joshua Gotbaum to Heads of Executive Departments and Establishments, Chief Financial Officers, and Inspectors General, January 4, 2001. Available at [http://www.whitehouse.gov/omb/financial/ffmia_implementation_guidance.pdf], visited December 11, 2003.

---

[880] U.S. Congress, House Committee on Government Reform, Subcommittee on Government Efficiency, Financial Management, and Intergovernmental Relations, The Federal Financial Management Improvement Act of 1996: Are Agencies Meeting the Challenge?, hearing, 107th Cong., 2nd sess., June 6, 2002 (Washington: GPO, 2003), p. 9.

——. 2003 Federal Financial Management Report (Washington: OMB, Aug. 2003). Available at: [http://www.whitehouse.gov/omb/financial/2003_report_final.pdf], visited December 11, 2003.

Bob Lyke
Virginia McMurtry

L. Federal Credit Reform Act of 1990

Statutory Intent and History

In March 1967, the President's Commission on Budget Concepts was created and instructed to make "a thorough and objective review of budgetary concepts."[881] In October 1967, the commission produced a comprehensive report with detailed recommendations on implementing a unified budget. In its report, the commission stated that the two basic functions of the federal budget are resource allocation and macroeconomic stabilization. For resource allocation, the commission believed that the budget should "provide the integrated framework for information and analyses from which the best possible choices can be made in allocating the public's money among competing claims."[882] This function of resource allocation should include comparisons among government programs and between the public and private sectors. For macroeconomic stabilization, the commission maintained that the budget should contain detailed and accurate information in order to evaluate the effects of federal fiscal activities. Furthermore, the budget should include data necessary to undertake discretionary countercyclical fiscal policy. Thus, the commission recommended a unified budget that would include all federal activities.

In the FY1969 budget, the Johnson Administration adopted the unified budget concept, but with some structural differences from the proposal of the commission. From FY1969 until the implementation of credit reform in FY1992, the federal budget recorded federal credit activity on a cash flow basis. Federal credit consists of federal direct loans and federal loan guarantees. In a given fiscal year, the budgetary cost of a particular loan program was net cash flow, which equaled new loans made plus any administrative expenses associated with these loans (rarely recognized in the loan accounts) less any loan fees, repayments of principal, and payments of interest. The federal acceptance of a contingent liability when a loan guarantee was provided was not included in the federal budget, because no cash flow occurred. Some guarantee programs charge fees to the recipient, and these fees were considered offsetting collections. Federal outlays were necessary to compensate lenders for any federal guaranteed loan defaults, but these outlays were not shown in the budget until they were actually paid.

On November 5, 1990, the Omnibus Budget Reconciliation Act of 1990 (OBRA90; 88 Stat. 304) was signed into law. It added a new title, Title V, to the Congressional Budget Act. Title V is also called "the Federal Credit Reform Act of 1990" (FCRA; 101 Stat. 1388; 2 U.S.C. § 621 note). Beginning with FY1992 (October 1, 1991), FCRA changed the budgetary treatment of federal direct loans

[881] U.S. President's Commission on Budget Concepts, Report (Washington: GPO, 1967), p. 105.

[882] Ibid., p.16.

and federal loan guarantees by requiring that the budgetary cost of a credit program be the subsidy cost at the time the credit is provided.

Major Provisions

The four stated purposes of FCRA are to:

- measure more accurately the costs of federal programs;
- place the cost of credit programs on a budgetary basis equivalent to other federal spending;
- encourage the delivery of benefits in the form most appropriate to the needs of beneficiaries; and
- improve the allocation of resources among credit programs and other spending (Section 501 of FCRA).

FCRA never uses the word subsidy; nevertheless, the true budgetary and economic cost of a federal credit program is the subsidy value at the time the credit is provided. FCRA defines the [subsidy] cost as "the estimated long-term cost to the government of a direct loan or loan guarantee, calculated on net present value basis, excluding administrative costs and any incidental effects on governmental receipts or outlays" [Section 502(5A)]. The discount rate used to calculate subsidy costs in terms of present value is the "average interest rate on marketable Treasury securities of similar maturity" [Section 502(5E)].[883] Hence, the subsidy cost of a program is determined by the amount of credit provided and the discount rate used to calculate the net present value of this credit.

Any government action that changes the estimated present value of an outstanding federal credit program is counted in the budget in the year in which the change occurs as a change in the subsidy cost of this program (Section 502(5D)). For example, the federal government could partially forgive the repayment of principal for low income borrowers from a particular credit program which would increase the subsidy cost of the program.

The Director of the Office of Management and Budget (OMB) is responsible for coordinating the estimation of subsidy costs. "The Director may delegate to agencies authority to make estimates of costs" (Section 503(a)). But these agencies must use written guidelines from the Director, which are developed after consultation with the Director of the Congressional Budget Office (CBO). The Director of OMB and the Director of CBO are responsible for developing more accurate historical data on credit programs which are used to estimate subsidy costs (Section 503). The President's budget includes "the planned level of new direct loan obligations and new loan guarantee commitments associated with each appropriations request" (Section 504).

---

[883] The derivation of the discount rate was revised by the Balanced Budget Act of 1997.

Beginning in the FY1992 budget cycle, discretionary programs providing new direct loan obligations and new loan guarantee commitments required appropriations of budget authority equal to their estimated subsidy costs. Credit entitlements (for example, guaranteed student loans) and existing credit programs of the Commodity Credit Corporation have indefinite budget authority (Section 505(a-c)) and do not need an annual appropriation.

Appropriations for the annual subsidy cost of each credit program go to a budget account called a credit program account. Funding for the subsidy costs of discretionary credit programs is provided in appropriations acts and must compete with other discretionary programs for funding available under the constraints of the budget resolution. Most mandatory credit programs receive automatic funding for the amount of credit needed to meet the demand by beneficiaries. Mandatory programs are generally entitlement programs for which the amount of funding depends on eligibility and benefits rules contained in substantive law. The subsidy cost of federal credit for both direct loans and guaranteed loans is scored as an outlay in the fiscal year in which the credit is disbursed by either the federal government or a private lender (504d). For mandatory credit programs, any additional cost from the annual reestimates of subsidies for a credit program is covered by permanent indefinite budget authority. This additional cost is displayed in a subaccount in the credit program account.

Also, beginning in FY1992, a nonbudget financing account was created for each credit program. These financing accounts receive an outlay at the time loans are made in the amount of the subsidy value of new direct or guaranteed loans from their associated credit programs. These accounts also record the government's loan programs' actual cash transactions, both disbursements and receipts, to and from the public. Each loan program gets funds for disbursement to the public by borrowing from the Treasury (Section 502(5E6-7)). Because they are nonbudget, the cash flows into and out of these accounts are not reflected in total outlay, receipts, or surplus/deficit. The budget authority of a credit program provides the means for the credit program account to pay to the financing account an amount equal to that program's estimated subsidy costs.

Another special account, the liquidating account, includes all ongoing cash flows of each credit program resulting from credit advanced prior to October 1, 1991 (Section 502(5E8)). However, the new budgetary procedures under FCRA would apply to modifications made by the U.S. government to credit terms on credit provided before FY1992.[884]

---

[884] U.S. Executive Office of the President, Office of Management and Budget, The Budget System and Concepts, Budget of the United States Government, Fiscal Year 2003 (Washington: GPO, 2002), p. 15.

FCRA does not apply to the credit activities of the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Resolution Trust Corporation, national flood insurance, the National Insurance Development Fund, crop insurance, or the Tennessee Valley Authority (Section 506).

Discussion

The Federal Credit Reform Act of 1990 was brief; it covered only five and one-half pages of the U.S. Code and Administrative News.[885] Numerous details necessary to make the act completely operational were absent. Furthermore, many federal agencies had inadequate financial and accounting systems to implement credit reform.[886]

On July 2, 1992, OMB issued a revised circular which improved and clarified instructions for credit budget formulation.[887] Furthermore, OMB simplified its credit subsidy model to make it easier for agencies to estimate direct loan and loan guarantee subsidies.[888] On January 11, 1993, OMB updated Circular No. A-129 concerning the budgetary treatment of federal credit programs.[889] OMB also revised Circular No. A-11 to include federal credit reform procedures. In Circular No. A-11, OMB explains to agencies how they should fill out credit schedules in preparing their budget requests.[890] Federal agencies working with OMB have steadily improved their compliance with credit reform standards.

Since the passage of the FCRA, OMB has continued to assist agencies in upgrading the quality of subsidy estimates. Beginning with the FY1993 budget, agencies have recorded reestimates of the cost of their credit programs. Aggregate subsidy estimates were adjusted downward for FY1994, upward for FY1995 and FY1996, downward for FY1997, upward for FY1998 and FY1999, and

---

[885] U.S. Code, Congressional and Administrative News, 101st Cong., 2nd sess., vol. 6 (St. Paul, MN: West Publishing Co., 1991), pp. 610-615.

[886] David B. Pariser, "Implementing Federal Credit Reform: Challenges Facing Public Sector Financial Manager," Public Budgeting & Finance, vol. 12, no. 4 (winter 1992), p. 28.

[887] U.S. Executive Office of the President, Office of Management and Budget, Budget of the United States Government, Fiscal Year 1994 (Washington: GPO, 1993), p. 49.

[888] Ibid.

[889] U.S. Executive Office of the President, Office of Management and Budget, Policies for Federal Credit Programs and Non-Tax Receivables, Circular No. A-129 (Washington: continually updated), p. 27.

[890] OMB's Circular Nos. A-11 and No. A-129 may be obtained from OMB's website, [http://www.whitehouse.gov/omb/index.html], visited Jan. 22, 2004.

downward for FY2000, FY2001, FY2002, and FY2003.[891] In the aggregate, downward subsidy reestimates of $13.8 billion were largely offset by upward subsidy reestimates of $11.9 billion.[892]

The trend for the subsidy reestimates has been for the magnitude, either up or down, to increase. In May 2001, CBO stated that it lacked any methodology to forecast the direction or size of future reestimates.[893] FCRA provided for permanent indefinite authority so that new appropriations are not needed to cover the cost of reestimates. Agencies are required to incorporate improved knowledge into their subsidy estimates for future direct loan obligations and loan guarantee commitments.[894]

The General Accounting Office (GAO) examined subsidy estimates for 10 credit programs in five agencies for the period of fiscal years 1992 through 1998. GAO found problems with supporting documentation for subsidy estimates and the reliability of subsidy rate estimates and reestimates in each agency.[895] But GAO concluded that agencies showed improvement over the period in documenting estimates in each agency.[896]

CBO examined credit subsidy reestimates for the period of FY1993 through FY1999. CBO concluded that

Projecting the losses and costs from federal credit assistance is difficult, and errors are inevitable. Although various incentives may exist for agencies to underestimate credit subsidies, the Congressional Budget Office's analysis of corrected reestimates does not reveal any pattern of bias in initial subsidy estimates. However, another problem was uncovered: the reestimates reported in the president's budget are in such disorder that analysts cannot rely on them.

---

[891] U.S. Executive Office of the President, Office of Management and Budget, Analytical Perspectives, Budget of the United States Government, Fiscal Year 2004 (Washington: GPO, 2003), p. 217.

[892] Ibid.

[893] U.S. Congressional Budget Office, An Analysis of the President's Budgetary Proposals for Fiscal Year 2002 (Washington: May 2002), p. 4.

[894] U.S. Executive Office of the President, Office of Management and Budget, Federal Credit Supplement, Budget of the United States Government, Fiscal Year 1997 (Washington: GPO, 1996), pp. 48-49.

[895] U.S. General Accounting Office, Credit Reform: Greater Effort Needed to Overcome Persistent Cost Estimation Problems, GAO/AIMD-98-14, Mar. 1998, pp. 9-10.

[896] Ibid., p. 11.

A few modest changes in current practice could reduce agencies' errors in preparing, reporting, and accounting for estimates and reestimates.[897]

OMB established on-budget credit program receipt accounts to receive payments of earnings from the financing accounts in those unusual cases when federal credit programs are estimated to produce net income, that is, have negative subsidies.[898] Usually payments into a program's receipt account are recorded in the Treasury's general fund as offsetting receipts.[899] "In a few cases, the receipts are earmarked in a special fund established for the program and are available for appropriation for the program."[900]

In October 1990, the Secretary of the Treasury, the Director of OMB, and the Comptroller General established the Federal Accounting Standards Advisory Board (FASAB) to consider and recommend accounting principles for the federal government. On September 15, 1992, the board issued an exposure draft recommending accounting standards for federal credit programs on a basis consistent with credit reform. The board received numerous substantive comments that were considered in revising its exposure draft, and on August 23, 1993, OMB issued the board's revised report titled Accounting for Direct Loans and Loan Guarantees.[901] This report provided extensive detail, including numerous arithmetic examples, clarifying credit reform practices.[902] It further required that federal agencies' use of present value accounting for federal credit programs be consistent with the Federal Credit Reform Act of 1990.[903] Thus, for

---

[897] David Torregrosa, "Credit Subsidy Reestimates, 1993-99," Public Budgeting & Finance, vol. 21, no. 2 (summer 2001), p. 114.

[898] Marvin Phaup, "Credit Reform, Negative Subsidies, and FHA," Public Budgeting & Finance, vol. 16, no. 1 (spring 1996), p. 24.

[899] U.S. Executive Office of the President, Office of Management and Budget, The Budget System and Concepts, Budget of the United States Government, Fiscal Year 2003, p. 14.

[900] Ibid.

[901] For a discussion of the board's conclusions on issues raised by these comments, see U.S. Executive Office of the President, Office of Management and Budget, Accounting for Direct Loans and Loan Guarantees: Statement of the Federal Financial Accounting Standards, no. 2 (Washington: Aug. 23, 1993), pp. 21-42.

[902] For a detailed example of the estimation of credit subsidies, see U.S. General Accounting Office, Credit Subsidy Estimates for the Sections 7(a) and 504 Business Loan Programs, GAO/T-RCED-97-197, July 16, 1997, p. 19.

[903] U.S. Executive Office of the President, Office of Management and Budget, Accounting for Direct Loans and Loan Guarantees: Statement of the Federal Financial Accounting Standards (Washington: GPO, 1993), pp. 21-42.

their credit programs, agencies' accounting procedures are now required to be consistent with their budgetary procedures.

On August 5, 1997, the Balanced Budget Act of 1997 (P.L. 105-33) was enacted.[904] This law (BBA97) amended the Federal Credit Reform Act of 1990 to make some technical changes, including codifying several OMB guidelines. Important changes were:

First, agencies are required to use the same discount rate to calculate the subsidy when they obligate budget authority for direct loans and loan guarantees and when submitting the agency's budget justification for the President's budget.[905] Thus, the dollar value of loans for a specific credit program is known when Congress considers subsidy appropriations for that program. Prior to this change, agencies had used interest rates from the preceding calendar quarter to calculate the subsidy at the time a direct loan was advanced or a loan guarantee was obligated.[906]

Second, agencies are required to use the same forecast assumptions (for example, default and recovery rates) to calculate subsidy rates when they obligate credit and when preparing the President's budget.[907]

Third, agencies are required to transfer end-of-year unobligated balances in liquidating accounts (revolving funds for direct loans and loan guarantees made prior to the effective date of FCRA) to the general fund as soon as practicable after the close of the fiscal year.[908]

Fourth, the same interest rate must be used on financing account debt (which generates interest payments to the Treasury), financing account balances, and the discount rate used to calculate subsidy costs.[909]

Fifth, the definition of the term cost is modified so that the discount rate is based on the timing of cash flows instead of on the term of the loan. Under this new

---

[904] For an explanation of the contents of the Budget Enforcement Act of 1997, see CRS Report 97-931, Budget Enforcement Act of 1997: Summary and Legislative History, by Robert Keith, p. 23 (1997).

[905] U.S. Executive Office of the President, Office of Management and Budget, Analytical Perspectives, Budget of the United States, Fiscal Year 1999 (Washington: GPO, 1998), p. 170.

[906] Ibid.

[907] Ibid.

[908] Ibid.

[909] Ibid.

approach, in the President's budget, a series of different rates would be used to calculate the present value of cost flows over a multi-year period. For example, for a 10-year direct loan (or loan guarantee), costs in the first year would be discounted using the interest rate on a one-year Treasury bill, costs in the second year would be discounted using the interest rate on a two-year Treasury note, etc. Under the prior approach, the interest rate of a 10-year Treasury note would have been used as the discount rate. This prior method proved to be inferior because the flow of semiannual interest payments and the repayment of full principal on the last payment date did not match up well with yearly cost flows.[910]

Selected Source Reading

Pariser, David B. "Implementing Federal Credit Reform: Challenges Facing Public
Sector Financial Managers." Public Budgeting and Finance, vol. 12 (winter 1992), pp. 19-34.

Congress. "Conference Report on H.R. 5835, Omnibus Budget Reconciliation Act of 1990, [Federal Credit Reform Act of 1990]." Congressional Record, daily edition, vol. 136 (October 26, 1990), pp. H12599-H12605.

Congressional Budget Office. Credit Budget Reestimates, 1993-1999. Washington: CBO, 2000.

U.S. Executive Office of the President. Office of Management and Budget. Federal Credit Supplement, Budget of the United States Government, Fiscal Year 2004.
Washington: GPO, 2003.

——. Preparation and Submission of Budget Estimates. Circular No. A-11. Federal Credit Data (sections 33.1-33.4). Washington: OMB, continually updated.

——. Policies for Federal Credit Programs and Non-Tax Receivables. Circular No. A-129. Washington: OMB, revised periodically.

U.S. General Accounting Office. Credit Reform: Greater Effort Needed to Overcome Persistent Cost Estimation Problems. AIMD-98-14. March 1998.

CRS Report RL30346. Federal Credit Reform: Legislative Background, Implementation, and Proposed Modifications, by James M. Bickley.

---

[910] U.S. Congress, Conference Committee, Balanced Budget Act of 1997, Conference Report to Accompany H.R. 2015, H.Rept. 105-217, 105th Cong., 1st sess. (Washington: July 30, 1997), pp. 996-997.

James M. Bickley

M. Federal Claims Collection Act of 1966

Statutory Intent and History

The Federal Claims Collection Act of 1966 (P.L. 89-508; 80 Stat. 308; 31 § 3711(a)-(c)(1)) originated agency authority to collect claims. It was intended to authorize agency heads to attempt collection of all claims of the United States, to compromise certain claims, or to terminate collection action in certain circumstances. Formerly, only a few agencies had been granted these authorities.

Major Provisions

The act defines agency as any department, office, commission, board, service, government corporation, instrumentality, or other establishment in either the executive or legislative branch of the federal government. It defines head of an agency to include, where applicable, commission, board, or other group of individuals having the decisionmaking responsibility of an agency.

The act directs the head of an agency or designee, pursuant to regulations prescribed and in conformity with such standards as may be promulgated jointly by the Attorney General and the Comptroller General, to attempt collection of all claims of the United States for money or property arising out of the activities of, or referred to, the agency.

For such claims of the United States that have not been referred to another agency, including the General Accounting Office (GAO), for further collection action that do not exceed $20,000, exclusive of interest, the head of an agency or designee, pursuant to regulations prescribed by him and in conformity with such standards as may be promulgated jointly by the Attorney General and the Comptroller General, may (1) compromise any such claim, or (2) terminate or suspend collection action on any such claim where it appears that no person liable on the claim has the present or prospective financial ability to pay any significant sum thereon or that the cost of collecting the claim is likely to exceed the amount of recovery.

The Comptroller General or his designee has the same authority for claims referred to GAO by another agency for further collection action. The head of an agency or designee shall not exercise authority over claims as to which there is an indication of fraud. The presentation of a false claim, or misrepresentation on the part of the debtor or any other party having an interest in the claim, shall be considered a violation of the antitrust laws. The head of an agency, other than the Comptroller General, does not have authority to compromise a claim that arises from an exception made by GAO in the account of an accountable officer.

A compromise effected under the act is final and conclusive on the debtor and on all officials, agencies, and courts of the United States, unless procured by fraud, misrepresentation, the presentation of a false claim, or mutual mistake of fact. No accountable officer is liable for any amount paid or for the value of property

lost, damaged, or destroyed, where the recovery of such amount or value may not be had because of a compromise with a person primarily responsible under the act.

Nothing in the act increases or diminishes existing authority of the head of an agency to litigate claims or diminish existing authority to settle, compromise, or close claims.

Discussion

When Congress enacted the Federal Claims Collection Act of 1966, it removed inflexibility in the law and responded to recurrent agency appeals to Congress for relief. If they could not collect amounts they believed due the federal government, agencies that formerly did not have authorities that the act granted had to refer claims to the General Accounting Office for collection. Only a few agencies had authority to compromise claims, i.e., accept a lesser amount in full settlement. Similarly, few agencies could terminate or suspend efforts to collect a claim even when the effort was futile. A compromise settlement was not possible until the matter was referred to the Department of Justice. The $20,000 limit on the amount of a claim that the Federal Claims Collection Act of 1966 granted agency heads to compromise and to terminate collecting subsequently was raised to $100,000. Authority of the Comptroller General to exercise the same authority as an agency head for claims referred to the General Accounting Office subsequently was repealed.

In 1997, GAO published the results of an evaluation of debt collection in some agencies with programs covering about two-thirds of the federal government's delinquent debt. GAO found that each agency it reviewed had a high percentage of debt in bankruptcy, foreclosure, or adjudication, and did not have a uniform method of documenting debt collection. GAO recommended, among other things, improved and standardized reporting requirements to collect debt. A subcommittee of the House Committee on Government Reform (the Subcommittee on Government Management, Information, and Technology, now renamed as the Subcommittee on Government Efficiency and Financial Management) held several oversight hearings on implementing improved debt collection practices. (See the entry for the Debt Collection Improvement Act of 1996, elsewhere in this compendium, which amended the Federal Claims Collection Act of 1966, for subsequent developments and selected source readings relating to collection of claims.)

Selected Source Reading

U.S. Congress. House. Committee on the Judiciary. Federal Claims Collection Act of 1966. S.Rept. 89-1533. 89th Congress, 2nd session. Washington: GPO, 1966. .

U.S. Congress. Senate. Committee on the Judiciary. Federal Claims Collection Act of 1966. S.Rept. 89-1331. 89th Congress, 2nd session. Washington: GPO, 1966.

U.S. General Accounting Office. Principles of Federal Appropriations Law, Chapter 13 (Debt Collection) vol. III (2nd ed.). OGC-94-33. November 1994.

——. Debt Collection: Improved Reporting Needed on Billions of Dollars in Delinquent Debt and Agency Collection Performance. GAO/AIMD-97-48. June 1997.

Thomas Nicola

N. Debt Collection Act of 1982

Statutory Intent and History

The Debt Collection Act of 1982 (P.L. 97-365; 96 Stat. 1749; 31 § 3711 et seq.) amended the Federal Claims Collection Act of 1966. The intent was to enable agencies to disclose information to consumer reporting agencies, authorize administrative offsets, charge minimum annual rates of interest and penalties on indebtedness to the United States, require annual agency reports summarizing the status of loans and accounts receivable, and permit contracts for collection services.

In addition, the act amended the Privacy Act (described elsewhere in this compendium) to clarify the status of consumer collection agencies. It also amended the Internal Revenue Code to authorize certain disclosures of information, Title 5 of the United States Code to authorize salary offsets, Title 18 of the United States Code to protect federal debt collectors, and Title 28 of the United States Code to change the statute of limitations for administrative offsets.

Major Provisions

Amendments to the Federal Claims Collection Act of 1966.
Disclosure of Information. The act authorizes the head of an agency, whenever attempting to collect a claim, to disclose to a consumer reporting agency information from a system of records under certain circumstances. It defines consumer reporting agency, system of records, and head of an agency.

Administrative Offset. The act authorizes the head of an agency, after attempting to collect a claim, to collect it by means of administrative offset, i.e., withholding money payable to or held bythe United States, except that such authority may not be exercised against claims that have been outstanding for more than 10 years. It describes claims eligible for administrative offset and prescribes procedures for it.

Interest and Penalty on Indebtedness. The act requires the head of an agency or designee to charge a minimum annual interest rate on outstanding debts that is equal to the average investment rate for the Department of the Treasury tax and loan accounts for the 12-month period ending on September 30 of each year. The Secretary or designee is required to publish the rate annually by October 31 and may revise it quarterly if the average investment for the 12-month period ending that quarter is greater or less than the existing published rate by 2%.

With some exceptions, the act requires the head of an agency or designee to assess charges to cover costs of processing and handling delinquent claims and to assess a penalty charge, not to exceed 6%, for failure to pay any portion of a debt more than 90 days past due.

Report on Agency Debt Collection Activities. The Director of the Office of Management and Budget, in consultation with the Secretary of the Treasury and Comptroller General of the United States, is directed to establish regulations requiring each agency with outstanding debts annually to prepare and transmit to the Director and the Secretary a report summarizing the status of loans and accounts receivable managed by each agency. The act specifies information that the report must contain. The Director is required to analyze the reports received and report annually to Congress on the management of agency debt collection activities.

Contracts for Collection Services. The act authorizes the head of an agency or designee to enter into a contract with any person or organization, under terms considered appropriate for collection services, to recover indebtedness owed the United States. Any such contract must include provisions specifying that the agency head or designee retains authority to resolve disputes, compromise claims, terminate collection action, and refer the matter to the Attorney General to initiate legal action, and that the contractor is subject to the Privacy Act (5 U.S.C. § 552a), to the extent provided in Subsection (m) of the act, and subject to federal and state laws that pertain to debt collection practices.

Claim for purposes of the Debt Collection Act is defined to include amounts owing on account of loans insured or guaranteed by the United States and all other amounts due the United States from such things as fees, leases, rents, royalties, sales of real or personal property, fines, penalties, taxes, and other sources.

Amendments to Title 5 of the United States Code.
Privacy Act. The act permits disclosure of any record in an agency system of records to a consumer reporting agency without consent of the individual to whom the record pertains, thereby exempting such disclosure from the Privacy Act requirement of prior consent. It exempts a consumer reporting agency from the Privacy Act provision that directs an agency to apply the Debt Collection Act's requirements to a system of records operated by contractors on behalf of an agency.

Salary Offset. The act authorizes the head of an agency or designee to deduct from the current pay account of an employee, member of the Armed Services or Reserve of the Armed Forces the amount of indebtedness owed to the United States, not to exceed 15% of disposable pay. The deductions may be made in monthly installments, or at established intervals, when the agency head or designee determines that the individual is indebted to the United States for debts to which the United States is entitled to be repaid or is notified by the head of another or designee. It grants an individual procedural protections, such as at least 30 days written notice, and opportunities to establish a repayment schedule and receive a hearing if timely requested.

The collection of any amount must be in accordance with standards in the Federal Claims Collection Act of 1966 or with any other statutory authority for collection of claims under any other statutory authority.

Amendments to the Internal Revenue Code.
Requirement That Applicant Furnish Taxpayer Identification Number.
The act directs each agency administering an included loan program to require any person applying for a loan under such program to furnish the person's taxpayer identification number.

Screening Potential Debtors. The Secretary of the Treasury is authorized, upon written request, to disclose to the head of any included federal loan program whether an applicant for a loan under such program has a tax delinquent account. The disclosure shall be made only for the purpose of, and to the extent necessary in, determining the creditworthiness of the applicant.

Included federal program for purposes of the paragraph means any program for which the United States makes, guarantees, or insures loans, and with respect to which there is in effect a determination made by the Director of the Office of Management and Budget (which has been published in the Federal Register) that applying this requirement to such program substantially would prevent or reduce future delinquencies in it.

Disclosure of Mailing Address to Third Parties for Purposes of Collecting Federal Claims. The act generally authorizes the Secretary of the Treasury, upon written request, to disclose the mailing address of a taxpayer for use by officers, employees, or agents of a federal agency for purposes of locating such taxpayer to collect or compromise a claim against the taxpayer.

In the case of an agent of a federal agency which is a consumer reporting agency (within the meaning of the Fair Credit Reporting Act), the mailing address may be disclosed only for the purpose of allowing the agent to prepare a commercial credit report. Statutory safeguards apply to these disclosures.

Protection of Federal Debt Collectors. The Debt Collection Act includes any officer or employee of the United States or any agency thereof designated to collect or compromise a federal claim in accordance with the act in the statute that prescribes punishments for killing or attempting to kill certain officials.

Discussion

Authorities granted by the Debt Collection Act of 1982 enhanced the ability of the government to collect delinquent debts by providing some tools that were available to the private sector.

In June 1997, the General Accounting Office (GAO) published results of an evaluation of debt collection at some agencies whose programs accounted for

about two-thirds of delinquent debt owed to the federal government. GAO found that each agency had a high percentage of bankruptcy, foreclosure, or adjudication and did not have a standard method of documenting debt collection. (See the entry for the Debt Collection Improvement Act of 1966, elsewhere in this compendium, which amended the Federal Debt Collection Act of 1982, for subsequent developments and selected source reading on debt collection.)

Selected Source Reading

Congress. House. Committee on Ways and Means. The Debt Collection Act of 1982. H.Rept. 97-496. 97th Congress, 2nd session. Washington: GPO, 1982.

Congress. Senate. Committee on Governmental Affairs. The Debt Collection Act of 1982. S.Rept. 97-378. 97th Congress, 2nd session. Washington: GPO, 1982.

——. Committee on Finance. The Debt Collection Act of 1981. S.Rept. 97-287. 97th Congress, 1st session. Washington: GPO, 1982.

General Accounting Office. Debt Collection, Improved Reporting Needed on Billions of Dollars in Delinquent Debt and Agency Collection Performance. GAO/AIMD-97-48. June 1997.

General Accounting Office. Principles of Federal Appropriations Law, Chapter 13 (Debt Collection) vol. III (2nd ed.). OGC-94-33. November 1994.

Thomas Nicola

O. Federal Debt Collection Procedures Act of 1990

Statutory Intent and History

The Federal Debt Collection Procedures Act, (P.L. 101-647; 104 Stat. 4789; 28 U.S.C. § 3001), Title XXXVI of the Crime Control Act of 1990, amends Title 28 of the United States Code to provide general civil procedures for collecting debts. The intent is to provide the exclusive civil procedures to recover a judgment on a debt or to obtain, before judgment on a claim for a debt, a remedy in connection with the claim, except where other federal law specifies procedures for recovering on a claim. Subchapters include general provisions, prejudgment and postjudgment remedies, fraudulent transfers involving debt, and amendments to other provisions of law.

Major Provisions

General Provisions. The act prescribes procedures for service of process, enforcement, and notice to the debtor and any person whom the United States, after due diligence, believes has possession, custody, or control of property. The act does not apply with respect to a judgment on a debt if the judgment was entered more than 10 years before the effective date of the act.

Remedies available to the United States may be enforced against property which is co-owned by a debtor and any other person only to the extent allowed by the law of the state where the property is located. Any right or interest of a debt or co-owner in a retirement for federal military or civilian personnel established by the United States or any agency thereof or in a qualified retirement arrangement, however, is not so limited.

A court may modify enforcement procedures. In an action or proceeding under the act, an individual debtor may elect to exempt certain property. The United States or a debtor may request a hearing on the applicability of any exemption claimed by the debtor. Asserting an exemption prevents the United States from selling or otherwise disposing of the property for which the exemption is claimed until a court determines that the debtor has a substantial nonexempt interest in the property.

Prejudgment Remedies. The act authorizes prejudgment remedies of attachment of property (except earnings), appointment of a receiver, garnishment against property (excluding earnings), and sequestration of income from property. It specifies procedures for the United States to apply for such a remedy, the grounds on which one may be sought, the content of an affidavit supporting the application and notice to the debtor, and hearing requirements.

A court may grant a prejudgment remedy if the United States shows reasonable cause to believe, among other things, that a debtor, with the effect of hindering the United States in its effort to recover a debt (1) is about to leave the jurisdiction of the United States; (2) has or is about to assign, dispose of, remove,

conceal, ill treat, waste, or destroy property; (3) has or is about to convert the debtor's property into money, securities, or evidence of debt in a manner prejudicial to the United States; or (4) has evaded service of process by concealing himself, or has temporarily withdrawn from the jurisdiction of the United States. A prejudgment remedy also may be granted if required to obtain jurisdiction within the United States and the remedy would result in obtaining such jurisdiction.

Any property in the possession, custody, or control of a debtor and in which a debtor has a substantial nonexempt interest, except earnings, may be attached pursuant to a writ of attachment. The act authorizes a court to appoint a receiver for property in which a debtor has a substantial interest if procedural requirements are met and the United States shows reasonable cause to believe that there is a substantial danger that property will be removed from the jurisdiction of the court, lost, concealed, materially injured or damaged, or mismanaged. The act specifies the duration, reporting requirements, priority, and compensation of receivers.

The act describes procedures for issuing a writ of garnishment against property (excluding earnings) in which a debtor has a substantial nonexempt interest and which is in the possession, custody, or control of a person other than the debtor to satisfy a claim for a debt. Co-owned property is subject to garnishment to the same extent as it is subject to garnishment under the law of the state where the property is located.

The act provides procedures for issuing a writ of sequestration of income from property in which the debtor has a nonexempt interest as security (and interest and costs) as the United States may recover on a claim for a debt. Such a writ may be issued in an action on a contract in certain circumstances, in an action against the debtor for damages in tort, if the debtor resides outside the jurisdiction of the United States, or in an action to recover a fine, penalty, or tax.

Postjudgment Remedies. The act also addresses postjudgment remedies including judgment lien, enforcement of judgment, execution, installation payment order, garnishment, and discharge.

A judgment in a civil action creates a lien on all real property of a judgment debtor on filing a certified copy of an abstract of a judgment in the manner in which a notice of tax lien would be filed under paragraphs (1) and (2) of Section 6323(f) of the Internal Revenue Code of 1986. A lien is effective, unless satisfied, for a period of 20 years, but, if a renewal request is filed before that period expires, may be renewed for an additional 20 years with court approval.

A debtor who has a judgment lien against his property is not eligible to receive any grant or loan which is made, insured, guaranteed, or financed directly or indirectly by the United States government. Such a debtor also is not eligible to

receive funds directly from the federal government in any program, except funds to which the debtor is entitled as beneficiary, until the judgment is paid in full. The agencyresponsible for such grants and loans may promulgate regulations to allow for a waiver of eligibility.

On proper application, a court may order the United States to sell, in accordance with sections 2001 and 2002 of Title 28 of the United States Code, any real property subject to a judgment lien. This authorization, however, does not preclude the United States from using an execution sale pursuant to Section 3203(g) to sell real property subject to a judgment lien.

A judgment may be enforced by any remedy set forth in the subchapter relating to postjudgment remedies, as well as any other writ pursuant to Section 1651 of Title 28, as necessary to support such remedies, subject to rule 81(b) of the Federal Rules of Civil Procedure.

The act prescribes procedures for execution. All property in which a judgment debtor has a substantial nonexempt interest is subject to levy pursuant to a writ of execution. A debtor's earnings are not subject to execution while in the possession, custody, or control of the debtor's employer. Co-owned property is subject to execution to the same extent that it is so subject under the law of the state where the property is located.

The act authorizes a court to order a judgment debtor to make specified installment payments to the United States if it is shown that he is receiving or will receive substantial nonexempt disposable earnings from self employment that are not subject to garnishment or is diverting or concealing substantial earnings from any source or property received in lieu of earnings.

A court may issue a writ of garnishment against property (including nonexempt disposable earnings) in which a debtor has a substantial nonexempt interest and which is in the possession, custody, or control of a person other than the debtor to satisfy a judgment against a debtor. Co-owned property is subject to garnishment under the law of the state where the property is located. The act also prescribes the general requirements for a writ of garnishment and procedures applicable to it.

Fraudulent Transfers Involving Debts and Miscellaneous. The act defines various terms including asset, creditor, and lien, and describes insolvency, value for transfer or obligation, and fraudulent transfers. It also sets out remedies of the United States and defenses, liability, and protection of transfers.

Discussion

By creating a uniform federal framework for collecting federal debts in the federal courts, the act improved efficiency and expedited collections. The uniform framework overcame obstacles presented by differences and conflicts in various

provisions of state law which formerly determined the nature, availability, and timing of executing various collection remedies.

Selected Source Reading

Congress. House of Representatives. Committee on the Judiciary. Federal Debt Collection Procedures Act of 1990. H.Rept. 101-736. 101st Congress, 2nd session. Washington: GPO, 1990.

Congress. House. Committee on Government Reform and Oversight, Subcommittee on Government Management, Information, and Technology. Federal Debt Collection Practices. Hearing. 105th Congress, 1st session. Washington: GPO, 1998.

_____. Brooks, Representative Jack. "Federal Debt Collection Procedures Act of 1990." Remarks in the House. Congressional Record, daily edition, vol. 136 (September 27, 1990), pp. 26231-26254.

Thomas Nicola

P. Debt Collection Improvement Act of 1996

Statutory Intent and History

The Debt Collection Improvement Act of 1996 (DCIA; P.L. 104-134; 110 Stat. 1321-358; 31 U.S.C. §§ 3711 et seq.), Section 31001 of the Omnibus Appropriations Act, FY1996, amends several sections of Title 31 that were enacted in the Federal Claims Collection Act of 1966 and the Federal Debt Collection Act of 1982, as well as some sections of Titles 5, 26, 28, and 42 of the United States Code.[911] It is intended to enhance authorities for administrative, salary, and tax refund offsets and collections, as well as to increase delinquent debt collections, limit costs of collecting debts, and reduce losses from debt management activities.

Major Provisions

Coverage. The act extends authorities relating to claims of the United States and claims against the United States to judicial agencies and instrumentalities, to make the judicial branch consistent with the executive and legislative branches. It also adds administrative offset authority and requirements for charging interest and penalties to debts owed to the United States by states and units of local governments.

Administrative Offset Authority. The act enhances administrative offset authority by requiring its use except when a statute explicitly prohibits using it. With some exceptions, a disbursing official of the Department of the Treasury, Department of Defense, the United States Postal Service, or any other government corporation, or any disbursing official of the United States designated by the Secretary of the Treasury, is required to offset at least annually the amount of a payment that a that certifying agency has certified to an official for disbursement, by an amount equal to the amount of a claim which a creditor agency has certified to the Secretary.

The act gives the Secretary of the Treasury discretion to apply administrative offset authority to any past-due, legally enforceable debt owed to a state if the appropriate state disbursing official requests an offset and there is a reciprocal agreement with a state that meets certain requirements.

Salary Offset Authority. The act requires agencies to which debts are owed and which have outstanding delinquent debts to participate at least annually in a

---

[911] The act was originally introduced in H.R. 2234 in 1995. An earlier version passed the House in the Seven Year Balanced Budget Reconciliation Act of 1995, H.R. 2491, as amended by the substitute of the House Committee on the Budget, H.R. 2517. (Congressional Record, daily edition, vol. 141 (Oct. 26, 1995), part II, pp. H10995, H11031H11040). The act did not appear in the conference report on the Reconciliation Act, H.Rept. 347, 104th Cong., 1st sess., 1995 (Congressional Record, daily edition, vol. 141 (Nov. 15, 1995), part II, p. 12509.

computer match of their delinquent debt records with records of federal employees to identify those employees who are delinquent in repaying these debts. The computer match requirement does not apply to debts under the Internal Revenue Code.

Taxpayer Identifying Numbers. The act directs the head of each federal agency to require each person doing business with the agency to furnish it with the person's taxpayer identifying number. It defines doing business with a federal agency and requires each agency to disclose its intent to use the identifying number for purposes of collecting and reporting on any delinquent amounts arising out of the person's relationship with the government. Creditor agencies are authorized to match their debtor records with records of the Department of Health and Human Services and Department of Labor records. Taxpayer identifying records may be disclosed only if disclosure is not otherwise prohibited by the Internal Revenue Code. It amends the definition of included federal program in the Internal Revenue Code.

Barring Delinquent Federal Debtors from Federal Loans, Loan Insurance, or Loan Guarantees. Unless the head of an agency or delegatee, i.e. the chief financial officer or deputy chief financial officer, waives this authority, a person who has an outstanding debt (other than a debt under the Internal Revenue Code) in delinquent status with any federal agency may not obtain a loan (other than a disaster loan) or loan insurance or loan guarantee administered by the agency. Such person may obtain additional loans or loan guarantees only after the delinquency is resolved. At the request of an agency, the Secretary of the Treasury may exempt any class of claims. An amendment excludes, in addition to disaster loans, a marketing assistance loan or loan deficiency payment under Subtitle C of the Agricultural Market Transition Act (7 U.S.C. §§ 7231 et seq.).

Disclosures to Consumer Reporting Agencies and Commercial Reporting Agencies. The head of an agency must require, as a condition for insuring or guaranteeing any loan, financing, or other extension of credit under any law to a person, that the lender provide information relating to the extension of credit to consumer reporting agencies and commercial reporting agencies, as appropriate. Under certain circumstances, the head of an agency may provide information that a claim is current in payment, i.e., not delinquent, to a consumer reporting agency or a commercial reporting agency.

Contracts for Collection Service. Under appropriate conditions, an agency head may enter into a contract with a person for collection service to recover indebtedness owed, or to locate or recover assets, of the United States government. This authority may not be used to locate or recover assets of the United States held by a state government or financial institution unless an agency has established procedures approved by the Secretary of the Treasury to identify and recover such assets.

Cross-Servicing Agreements and Centralization of Debt Collection Activities in the Department of the Treasury. If a nontax debt or claim owed to the United States has been delinquent for 180 days, the head of the agency that administers the program giving rise to the debt or claim is required to transfer it to the Secretary of the Treasury. Upon such transfer, the Secretary is required to take appropriate action to collect or terminate collection actions on the debt or claim. These authorities do not apply to certain categories of debts or claims. The Secretary may designate and withdraw designations of debt collection centers operated by other federal agencies.

Garnishment. The act authorizes the head of an agency, notwithstanding any provision of state law, to garnish the disposable pay of an individual to collect the amount owed, if the individual is not currently making required payment in accordance with an agreement between the agency head and the individual.

Adjustment of Administrative Debt and Dissemination of Information Regarding Identity of Delinquent Debtors. The head of any agency is authorized to increase an administrative claim by a cost of living adjustment instead of charging interest and penalties.

The act authorizes any agency head, with the review of the Secretary of the Treasury, for the purpose of collecting any delinquent nontax debt owed by any person, to publish or otherwise disseminate information regarding the identity of the person and the existence of the nontax debt.

Federal Civil Monetary Penalties Inflation Adjustments and Electronic Funds Transfer. The act amends the Federal Civil Penalties Inflation Adjustment Act of 1990 (P.L. 101-410; 104 Stat. 890; 28 U.S.C. § 2461 nt) to direct the head of each agency, not later than 180 days after the enactment of the Debt Collection Improvement Act, and at least once every four years thereafter, to adjust by regulation each monetary civil penalty provided by law within the jurisdiction of the agency (with some exceptions). The initial increase could not exceed 10%.

The Federal Financial Management Act of 1994 (P.L. 103-356; 108 Stat. 3410, 3412; 31 U.S.C. § 3301 nt) is amended to mandate electronic funds transfer for all payments to a recipient who becomes eligible to receive them more than 90 days after enactment of the Debt Collection Improvement Act of 1996. This requirement may be waived for any individual who does not have an account with a financial institution. All payments made after January 1, 1999, must be made by electronic funds transfer.

Expanding Use of Private Attorneys. The act expands use of private attorneys by amending requirements relating to the number of contracts in each district and repealing termination dates for the pilot program.

Discussion

The Debt Collection Improvement Act of 1996 is intended to improve federal debt collection by, among other things, adding a new administrative offset authority, revising salary offset authority, permitting non-delinquent consumer debt to be reported to credit bureaus, allowing agencies to retain a portion of annual collections of delinquent debts, expanding tax refund offset authority, and requiring electronic disbursements.

Two bills to amend federal debt collection procedures passed the House and one was introduced in the Senate in the 105th Congress. No further action occurred on any of the bills. Among other provisions, H.R. 4243 and H.R. 4857 would have (1) permitted a private collection contractor to verify information about an individual's employer and compensation; (2) denied to individuals with delinquent debt eligibility for the award or renewal of a federal benefit, including access to federal loans; required agency heads to establish programs to sell nontax debt; and (3) authorized agency heads to accept electronic payments, including debit and credit cards, to satisfy nontax debts. S. 2571 would have permitted agencies administering benefit programs to verify the information provided to them by applicants for these benefits and would have authorized the Secretary of Health and Human Services to disclose information to another agency from the National Directory of New Hires. (Similar provisions were in H.R. 2347 and H.R. 2063 and were discussed during the consideration of H.R. 4243.) Additionally, S. 2571 would have authorized the administrator of the General Services Administration, on behalf of federal agencies, to acquire commercial services to accept electronic payments for grants or loans and electronic claims submissions from the general public.

In the 106th Congress, H.R. 436 and H.R. 1441 passed the House and were referred to the Senate Committee on Governmental Affairs, but no further action occurred. H.R. 436 was identical to H.R. 4857 (105th Congress) and H.R. 1441 was similar to it. During the 106th Congress, H.R. 4181, a bill to prohibit delinquent federal debtors from being able to enter into federal contracts and to amend the Internal Revenue Code to provide for disclosure to federal agencies of certain information to relating to delinquent taxpayers, was considered in committee.

A subcommittee of the House Committee on Government Reform (the Subcommittee on Government Management, Information, and Technology, now renamed the Subcommittee on Government Efficiency and Financial Management) has conducted regular oversight hearings on DCIA since its enactment. Generally, those hearings have found that the DCIA provisions (especially those on administrative offset and cross-servicing) have not been fully implemented in executive agencies, that the amounts of delinquent nontax debts and debts written off remain significant, and that agencies have experienced difficulties in identifying and referring eligible debt to the Department of the Treasury's Financial Management Service (FMS) and in identifying debt that is collectible. Agencies were encouraged to include debt collection as a

performance goal for purposes of the Government Performance and Results Act of 1993 (P.L. 103-62; 107 Stat. 285).

General Accounting Office (GAO) evaluations of the implementation of DCIA have focused on many of the issues stated above and have frequently been featured at the House hearings. In its October 2003 evaluation of the cross-servicing program, GAO recommended that the Department of the Treasury help to ensure that debts returned from private collection agencies be examined to make sure that all appropriate collection action has been taken and that the Office of Management and Budget work to improve agency compliance with the standards and policies for writing off and closing out debts. In a December 2001 evaluation, GAO found that the Department of Agriculture (USDA) had not yet fullyimplemented keyprovisions of DCIA. An increased commitment by USDA to implement DCIA was reported by GAO in November 2002, but GAO cautioned that a sustained commitment would be necessary to address problems, including those relating to identifying and referring eligible debts to FMS.

The FMS' Fiscal Year 2003 Report to Congress showed that $70.061 billion of nontax debt was delinquent as of September 30, 2003. Of this total, $7.780 billion was debt written off, $55.273 billion was delinquent debt greater than 180 days old and $14.916 billion was delinquent debt determined to be currently not collectible. The report also showed that $18.2 billion of nontax debt has been collected through the Treasury Offset Program and Cross-Servicing Program since the enactment of DCIA; $3.1 billion was collected through these programs in FY2003. The Departments of Education ($32.166 billion) and Agriculture ($6.613 billion) have the most delinquent debt. As of September 30, 2003, private collection agencies under contract with the Departments of Education, Health and Human Services, and Treasury had been referred $14.375 billion in debt and collected $546.8 million.

Selected Source Reading

Davis, Representative Thomas III, et al. "Government Waste, Fraud, and Error Reduction Act of 1998." Remarks in the House. Congressional Record, daily edition, vol. 144 (October 20, 1998), pp. H11672-H11679.

Horn, Representative Stephen. "Government Waste, Fraud, and Error Reduction Act of 1998." Remarks in the House. Congressional Record, daily edition, vol. 144 (October 14, 1998), pp. H10850-H10855.

Horn, Representative Stephen. "Government Waste, Fraud, and Error Reduction Act of 1999." Remarks in the House. Congressional Record, daily edition, vol. 145 (August 2, 1999), pp. H6780-H6784.

Horn, Representative Stephen. Remarks in the House. Congressional Record, daily edition, vol. 142 (April 25, 1996), pp. H4087-H4091.

Lieberman, Senator Joseph I. "Federal Benefit Verification and Integrity Act." Remarks in the Senate. Congressional Record, daily edition, vol. 144 (October 7, 1998), pp. S11708-S11711.

Sessions, Representative Pet, et al. "Government Waste, Fraud, and Error Reduction Act of 1999." Remarks in the House. Congressional Record, daily edition, vol. 145 (February 24, 1999), pp. H743-H749.

U.S. Congress. House. Committee on Government Reform. Government Waste, Fraud, and Error Reduction Act of 1999. Report to Accompany H.R. 436. H.Rept. 106-9, Part 1. 106th Congress, 1st session. Washington: GPO, 1999.

——. Subcommittee on Government Management, Information, and Technology. Federal Debt Collection Practices. Hearing. 105th Congress, 1st session. Washington: GPO, 1998.

——. H.R. 4243, Government Waste, Fraud, and Error Reduction Act of 1998; H.R. 2347, The Federal Benefit Verification and Integrity Act; and H.R. 2063, The Debt Collection Wage Information Act of 1997. Hearing. 105th Congress, 2nd session. Washington: GPO, 1998.

——. Oversight Hearing on Improving Federal Debt Collection Practices at the Department of Agriculture. Hearing. 105th Congress, 2nd session, March 20, 1998. Unpublished [available from author].

——. Oversight of the Implementation of the Debt Collection Improvement Act. Hearing. 106th Cong., 2nd session. Washington: GPO, 2001.

——. What Is the Federal Government Doing to Collect the Billions of Dollars in 1st
Delinquent Debts It Is Owed? Hearing. 106th Congress, session. Washington: GPO, 2000.

——. Subcommittee on Government Efficiency, Financial Management, and Intergovernmental Relations. The Debt Collection Improvement Act of 1996: How Well Is It Working? Hearing. 107th Congress, 1st session, October 10, 2001, and December 5, 2001. Washington: GPO, 2002.

——. Federal Debt Collection: Is the Government Making Progress? Hearing. 107th Congress, 2nd session. Washington: GPO, 2003.

——. Federal Debt Management — Are Agencies Using Collection Tools Effectively? Hearing. 108th Congress, 1st session. Washington: GPO, 2003.

Department of Justice and U.S. Department of the Treasury. Federal Claims Collection Standards, 4 C.F.R. Parts 900-904. Washington: GPO, 2003.

Department of the Treasury. Financial Management Service. Fiscal Year 2003 Report to the Congress. U.S. Government Receivables and Debt Collection Activities of Federal Agencies. Washington: FMS, no date.

General Accounting Office. Debt Collection, Improved Reporting Needed on Billions of Dollars in Delinquent Debt and Agency Collection Performance. GAO/AIMD-97-48. June 1997.

——. Major Management Challenges and Program Risks: Department of the Treasury. GAO/OGC-99-14. November 1998.

——. Debt Collection; Opportunities Exist for Improving FMS's Cross-Servicing Program. GAO-04-47. October 2003.

——. Debt Collection; Treasury Faces Challenges in Implementing Its Cross-Servicing Initiative. GAO/AIMD-00-234. August 2000.

——. Debt Collection Improvement Act of 1996; Agencies Face Challenges Implementing Certain Key Provisions. GAO-02-61T. October 10, 2001.

——. Debt Collection Improvement Act of 1996: Major Data Sources Inadequate for Implementing the Debtor Bar Provisions. GAO-02-462. March 2002.

——. Debt Collection; Agriculture Making Progress in Addressing Key Challenges. GAO-03-202T. November 13, 2002.

Thomas Nicola
Barbara L. Schwemle

Q. Improper Payments Information Act of 2002

Statutory Intent and History

Toward the end of the 107th Congress, the Improper Payments Information Act (IPIA) of 2002 was enacted as P.L. 107-300.[912] The intent of the law is to increase financial accountability in the federal government, and thereby reduce wasteful spending, thus augmenting previous financial management reform laws. The law requires agencies each year to identify programs that are vulnerable to improper payments and to estimate the amount of overpayments or underpayments. As explained in the next section, improper payments generally include any payments by the federal government that should not have been made or were made in an incorrect amount.

Previously, there was no government-wide requirement for agencies to estimate or report in any systematic way on improper payments, although it is generally acknowledged that billions of dollars are involved. For example, after reviewing audited financial statements for the 24 Chief Financial Officers (CFO) Act agencies, GAO concluded that improper payments voluntarily reported by the agencies declined slightly, from $ 20.7 billion in FY1999 to $19.6 billion in FY2001.[913] In 2003, the Office of Management and Budget (OMB) testified that overpayments for major benefit programs alone were approaching $35 billion each year.[914]

H.R. 4878, to provide for estimates and reports of improper payments by federal agencies, was introduced on June 6, 2002, by Representative Stephen Horn, with a group of bipartisan cosponsors, and referred to the House Committee on Government Reform. The Subcommittee on Government Efficiency, Financial Management, and Intergovernmental Relations held markup on the measure on June 18, 2002, and approved the bill, as amended, by unanimous voice vote. On July 9, 2002, H.R. 4878 was considered under suspension of the rules and passed the House, as amended, by voice vote. On October 9, 2002, the Senate Committee on Governmental Affairs ordered H.R. 4878 to be reported favorably, with a substitute amendment. On October 17, 2002, the bill, as amended, passed the Senate by unanimous consent, and on November 12, under suspension of the rules, the House agreed to the Senate amendment byvoice vote. The President signed H.R. 4868 into law on November 26, 2002 (P.L. 107-300).

---

[912] 116 Stat. 2350; 31 U.S.C. § 3321 note.

[913] U.S. General Accounting Office, Financial Management: Coordinated Approach Needed to Address the Government's Improper Payments Problems, GAO-02-749, Aug. 2002, p. 11.

[914] Cited in U.S. General Accounting Office, Financial Management: Challenges Remain in Addressing the Government's Improper Payments, GAO-03-750T, May 13, 2003, p. 1.

The problem of improper payments received attention in previous Congresses. During House floor debate on H.R. 4878, Representative Horn noted that hearings held in the past "clearly demonstrated the need" for such legislation:

Since the 104th Congress, the subcommittees I have chaired have held approximately 100 hearings on wasteful spending within the Federal Government. Time and again witnesses from the General Accounting Office and agency inspectors general have told the subcommittee that poor accounting systems and procedures have contributed to the government's serious and long-term problems involving improper payments.[915]

In the written report of the Senate Committee on Governmental Affairs to accompany H.R. 4878, the measure was also specifically linked to GAO recommendations offered in a best practices guide for agencies in managing improper payments, prepared at the request of the committee chairman, Senator Joseph Lieberman. The guide suggested that determining the nature and extent of risks for improper payments was a key step in the process, and H.R. 4868 would address this by requiring agencies to estimate total improper payments made each year in their programs and also to consider ways to reduce these amounts.[916] In August 2002 GAO also provided an update of previous reports on improper payments at the request of the ranking minority member, Senator Fred Thompson.[917]

Major Provisions

The act directs each executive branch agency, in accordance with OMB guidance, to review all of its programs and activities each year, identify those that may be susceptible to significant improper payments, estimate the amount of improper payments, and report this information to Congress by March 31 of the following applicable year. OMB determines the method of reporting, which is to be used by all agencies.

With respect to any program or activity with estimated annual improper payments exceeding $10 million, the agency is required to provide along with the estimate a report on agency actions to reduce such improper payments. The report is to discuss the causes of the improper payments and the results of the

---

[915] Rep. Stephen Horn, remarks in the House, Congressional Record, daily edition, vol. 148, July 9, 2002, p. H4379.

[916] See GAO Report GAO-02-749, issued initially as GAO Report GAO-01-703G [exposure draft] (Washington: May 2001). Cited in U.S. Congress, Senate Committee on Governmental Affairs, Improper Payments Information Act of 2002, report to accompany H.R. 4878, 107th Cong., 2nd sess., S.Rept. 107-333 (Washington: GPO, 2002), p. 2.

[917] See GAO Report GAO-02-749, Aug. 2002.

actions taken to address them, to state whether the agency has information systems and other necessary infrastructure to reduce such payments to minimal cost-effective levels, to describe budgetary resources requested by the agency to accomplish any needed changes in information systems and infrastructure, and to identify steps the agency has taken to ensure that managers are held accountable for reducing improper payments.

Improper payment is defined as any payment that should not have been made or that was made in an incorrect amount. The definition includes payments to ineligible recipients or for ineligible services, duplicate payments, and payments for services not received or that do not reflect applicable discounts. The act covers payments made by a federal agency, a federal contractor, or a governmental or other organization administering a federal program.

Discussion

IPIA. The IPIA codified and expanded efforts underway in the executive branch to reduce improper payments. The Bush Administration in 2001 designated improving financial performance as one of five government-wide initiatives in the President's Management Agenda.[918] The establishment of a baseline on the extent of erroneous (improper) payments in major federal benefit programs was a key component of the financial management initiative.[919] Agencies were to include available information on erroneous payment rates for benefit and assistance programs over $2 billion as a part of their FY2003 budget submissions. In July 2001, revisions to OMB Circular No. A-11 in Section 57, implemented this objective, requiring 15 federal agencies to include improper payment information, covering nearly 50 programs, with initial FY2003 budget materials to OMB.[920] Enactment of the IPIA extended and augmented the erroneous payment reporting requirements, originally contained in OMB Circular No. A-11 for the 15 agencies designated therein, to all executive branch departments and agencies.

In May of 2003, OMB distributed a guide to instruct agencies on the implementation of the IPIA.[921] The guide provides a detailed definition of

---

[918] See U.S. Office of Management and Budget, The President's Management Agenda — FY2002 (Washington: OMB, 2001), pp. 19-21. For an overview of the PMA, see CRS Report RS21416, The President's Management Agenda: A Brief Introduction, by Virginia A. McMurtry.

[919] Ibid.

[920] GAO Report GAO-02-749, pp. 7, 56.

[921] OMB, "Improper Payments Information Act of 2002 (Public Law No: 107-300)," Memorandum for Heads of Executive Departments and Agencies from Mitchell E. Daniels Jr., May 21, 2003, M-03-13., available at: [http://www.whitehouse.gov/omb/memoranda/print/m03-13.html], visited Jan. 22, 2004.

improper or erroneous payments and of program and activity and then outlines four action steps to be followed by the agencies. First, agencies must systematically review all their programs and activities and identify those which are susceptible to significant erroneous payments, defined as "annual erroneous payments in the program exceeding both 2.5 percent of the program payments and $10 million." Second, agencies shall determine an annual estimated amount of erroneous payments made in those programs and activities found susceptible to significant errors; this calculation is based on a statistical random sample sufficiently large "to yield an estimate with a 90 percent confidence interval" within 5% precision. The third step is to determine why the particular programs are at risk, and then put in place a plan to reduce the erroneous payments. The last step in implementation for the agency is reporting to the President (via OMB) and Congress on the estimates of the annual amount of erroneous payments in its programs and activities and on progress in reducing them.

The House Subcommittee on Government Efficiency and Financial Management held oversight hearings on improper payments in May and July 2003.[922] A GAO report to the subcommittee on the initial implementation under the IPIA followed in October 2003.[923] There has been some criticism about the OMB guidance to the agencies in implementing the IPIA, particularly about defining "significant [emphasis added] improper payments" to include at least 2.5 % of payments, in addition to the estimated improper spending over $10 million. According to a recent news article, the chairman and ranking minority member of the Senate Finance Committee, in a January 9, 2004, letter to OMB Director Joshua Bolten, stated:

> *...OMB should not have established the 2.5 percent threshold and should have simply required agencies to report all programs generating estimated improper payments of more than $10 million. Because of the 2.5 percent threshold, some programs wasting more than $10 million could slip through the cracks, the senators explained. 'The improper payments figures that will*

---

[922] U.S. Congress, House Committee on Government Reform., Subcommittee on Government Efficiency and Financial Management, Show Me the Tax Dollars — How Much Is Lost to Improper Payments Each Year?, hearing, 108th Cong., 1st sess., May 13, 2003, available at [http://reform.house.gov/GEFM/Hearings/EventSingle.aspx?EventID=385], visited Jan. 22, 2004; and Show Me the Tax Dollars Part II — Improper Payments and the Tenncare Program, July 14, 2003, available at: [http://reform.house.gov/GEFM/Hearings/EventSingle.aspx?EventID=401], visited Jan. 22, 2004.

[923] U.S. General Accounting Office, Financial Management: Status of the Governmentwide Efforts to Address Improper Payment Problems, GAO-04-99, Oct. 2003.

eventually be reported to the public will look better and feel better than they really are…' Grassley and Baucus said.[924]

Likewise, the chairman and ranking minority member of the House Subcommittee on Government Efficiency and Financial Management, Representative Todd Platts, and Representative Marsha Blackburn, sent a letter to OMB in August 2003, questioning the 2.5 % minimum threshold. OMB's Controller of the Office of Federal Financial Management, Linda Springer, has defended the guidelines as stringent enough, noting, "We're [at OMB] certainly not trying to take any steam out of the effort."[925]

New estimates from the agencies of improper payments, and of possible ways to reduce them, are due to Congress each year, providing useful oversight information. If dissatisfaction with OMB's guidelines should linger or increase, language in the IPIA might be revisited. Meanwhile, the control of improper payments remains a priority for OMB as a part of the President's Management Agenda.

Recovery Auditing. Another provision related to improper payments, enacted in the 107th Congress as Section 831 of the National Defense Authorization Act for FY2002,[926] provides a statutory mandate for agencies to identify and recover contract overpayments (one type of improper payments) by using recovery auditing. Recovery auditing is designed to identify and then recoup inadvertent overpayments by reviewing large volumes of purchase and contract records using ongoing, systematic procedures. Originating in the private sector around 1970, recovery auditing came to the federal government via a demonstration program first mandated in the National Defense Authorization Act for FY1996 (P.L. 104-106). The FY1998 Defense Authorization Act (P.L. 105-85) provided for continuation and expansion of the pilot program, and also called for a review of its results by the General Accounting Office (GAO). The GAO report reviewing the demonstration program in recovery auditing undertaken by the Department of Defense at the Defense Supply Center in Philadelphia was issued at the end of 1998[927] and provided an impetus for additional legislative attention to recovery auditing in the 106th Congress.

H. R. 1827 (106th Congress) was introduced by Representative Dan Burton on May 17, 1999, and was referred to the Committee on Government Reform. On

---

[924] Amelia Gruber, "OMB Defends Actions on Improper Payments," GovExec.com, Jan. 14, 2004.

[925] Cited ibid.

[926] P.L. 107-107, Dec. 28, 2001; 115 Stat. 1186.

[927] U.S. General Accounting Office, Contract Management: Recovery Auditing Offers Potential to Identify Overpayments, GAO/NSIAD-99-12, Dec. 1998.

June 29, 1999, hearings were held by the Subcommittee on Government Management, Information, and Technology.[928] On July 21, 1999, subcommittee consideration and markup of the measure occurred, with approval by voice vote, after which the bill, with an amendment in the nature of a substitute, was forwarded to the full committee. On November 10, 1999, the Government Reform Committee considered the measure and, by voice vote, approved the amendment in the nature of a substitute from the subcommittee, as further amended, and ordered that H.R. 1827 be favorably reported. It was reported on November 17, 1999, and placed on the House Calendar.[929] On March 8, 2000, H.R. 1827 passed the House by a vote of 375-0. On September 12, 2000, Senator Fred Thompson introduced S. 3030 (106th Congress) as a companion measure to H.R. 1827; the bill was referred to the Committee on Governmental Affairs. On September 27, 2000, the committee, by voice vote ordered S. 3030 reported favorably to the Senate, and the report was filed on October 12, 2000.[930] The Senate took no further action on S. 3030 or H.R. 1827 before the 106th Congress ended.

In the 107th Congress, Representative Burton introduced H.R. 2547, the Erroneous Payments Recovery Act, "To require certain executive agencies to carry out a cost-effective program for identifying any errors made in paying contractors and for recovering any amounts paid to contractors." This measure, similar to H.R. 1827 in the 106th Congress, was referred to the House Committee on Government Reform, but no further action occurred on the bill. Provisions relating to recovery auditing, however, were included in H.R. 2586, the National Defense Authorization Act for FY2002, as reported and passed by the House.[931] There were no similar provisions in the Senate bill, but the conference version contained the recovery auditing provisions from the House version, with modifications,[932] as Section 831. The measure was signed into law on December 28, 2001, becoming P.L. 107-107.

---

[928] U.S. Congress, House Committee on Government Reform, Subcommittee on Government Management, Information, and Technology, H.R. 1827, the Government Waste Corrections Act of 1999, hearing, 106th Cong., 1st sess., June 29, 1999 (Washington: GPO, 2000).

[929] U.S. Congress, House Committee on Government Reform, Government Waste Corrections Act of 1999, report to accompany H.R. 1827, 106th Cong., 1st sess., H.Rept. 106474 (Washington: GPO, 1999).

[930] U.S. Congress, Senate Committee on Governmental Affairs, To Amend Title 31, United States Code, to Provide for Executive Agencies to Conduct Annual Recovery Audits and Recovery Activities, and for Other Purposes, report to accompany S. 3030, 106th Cong., 2nd sess., S.Rept. 106-502 (Washington: GPO, 2000).

[931] U.S. Congress, House Committee on Armed Services, National Defense Authorization Act for Fiscal Year 2002, H.Rept. 107-195, 107th Cong., 1st sess. (Washington: GPO, 2001), pp. 342-343.

[932] See U.S. Congress, Conference Committee, National Defense Authorization Act for Fiscal Year 2002, H.Rept. 107-333, report to accompany S. 1438, 107th Cong., 1st sess. (Washington: GPO, 2001), p. 691.

Section 831 of P.L. 107-107 amends Chapter 35 of Title 31, United States Code, by adding a new Subchapter VI, "Recovery Audits." Section 3561 directs the head of each executive agency that enters into contracts in excess of $500 million in a fiscal year to carry out a cost-effective program for identifying any errors made in paying contractors and for recovering amounts erroneously paid. The OMB Director is required to issue guidelines for conducting the recovery audit programs, with specified protections and policies. Section 3562 provides for the disposition of recovered funds. Funds collected under the program may be used to reimburse the actual expenses incurred by the agency in administering the program or to pay contractors for recovery auditing services. Beyond funds needed for these purposes, amounts recovered may be credited to the appropriations from which the erroneous payments were made, or otherwise be deposited in the Treasury as miscellaneous receipts. Section 3563, sources of recovery services, requires each agency head to consider all available resources to carry out the program, including the agency itself, other departments and agencies, or private sector contractors. Section 3564 authorizes each agency head to carry out a program for improving contract payment management processes aimed at reducing payment errors and improving recovery of overpayments. Section 3565 clarifies the relationship of the subchapter to authority of inspectors general. Section 3566 deals with privacy protections. Section 3567 requires the OMB Director to report to the House Committee on Government Reform and the Senate Governmental Affairs Committee on implementation of the recovery auditing program.

In January 2003, OMB issued guidance to the agencies intended to assist them "to successfully implement recovery auditing and recovery activity as part of an overall program of effective internal control over contract payments." The guidance reiterates that the agencies required by statute to undertake recovery audit programs must report to OMB by December 31, 2004, on their activities during FY2003 and, likewise, for FY2004 and FY2005.[933]

Selected Source Reading

Congress. House. Committee on Government Reform. Subcommittee on Government Management, Information, and Technology. H.R. 1827, the Government Waste Corrections Act of 1999. Hearing. 106th Congress, 1st session, June 29, 1999. Washington: GPO, 2000.

[933] U.S. Office of Management and Budget, Programs to Identify and Recover Erroneous Payments to Contractors, Memorandum to Heads of Executive Departments and Agencies, from Mitchell E. Daniels Jr., Jan. 16, 2003, M-03-07, available at: [http://www.whitehouse.gov/omb/memoranda/print/m03-07.html], visited Jan. 22, 2004.

Congress. Senate. Committee on Governmental Affairs. Improper Payments Information Act of 2002. Report to accompany H.R. 4878. 107th Congress, 2nd session. S.Rept. 107-333. Washington: GPO, 2002.

——. To Amend Title 31, United States Code, to Provide for Executive Agencies to Conduct Annual Recovery Audits and Recovery Activities, and for Other Purposes. Report to accompany S. 3030. 106th Congress, 2nd session. S.Rept. 106-502. Washington: GPO, 2000.

U.S. General Accounting Office. Financial Management: Challenges Remain in Addressing the Government's Improper Payments. GAO-03-750T. May 13, 2003.

——. Financial Management: Effective Implementation of the Improper Payments Information Act of 2002 Is Key to Reducing the Government's Improper Payments. GAO-03-991T. July 14, 2003.

U.S. Office of Management and Budget. 2003 Federal Financial Management Report. Washington, Aug. 2003, pp. 7-9. At [http://www.whitehouse.gov/omb/financial/2003_report_final.pdf, visited January 22, 2004.

Virginia McMurtry

R. Cash Management Improvement Act (CMIA) of 1990

Statutory Intent and History

The Cash Management Improvement Act of 1990 (CMIA; 104 Stat. 1058; 31 U.S.C. § 3335) is intended to ensure greater efficiency, effectiveness, and equity in the exchange of funds between the federal government and the states. Its objective is to minimize the ability of the federal or a state government to engage in cash management practices that allow it to earn interest on cash reserves at the expense of the other.

Passage of the act was preceded by seven years of joint study by federal and state management officials of how federally funded programs were being managed in terms of the actual receipt and expenditure of program funds. The early deliberations of this group resulted in a June 1983 Memorandum of Understanding that stated the intention of each group to find an equitable approach to intergovernmental cash management. Pilot tests of new procedures were conducted in 1984-1985.

Major Provisions

The major provisions of the act mandate (1) that each head of a federal executive agency implement procedures designed to disburse federal funds in a timely manner through cash, checks, electronic funds transfer, or any other means identified by the agency head and that each state establish procedures for minimizing the elapsed time between transfer of funds from the United States Treasury and state expenditure of these funds for the intended federal purpose; (2) a method to calculate the interest owed — to a state when the federal government fails to disburse federal funds in a timely manner, and to the federal government when a state fails to spend federal funds in a timely manner; (3) procedures to net the interest charges each level of government owes to the other and to transfer the net interest owed; and (4) the source of the interest payment when a federal agency must pay interest to a state.

Discussion

This act is a response to both levels of government experiencing instances in which one level of government was perceived to be manipulating cash management practices in a manner designed to hold on to money for a longer period of time than necessary. Such behavior earns interest income on the cash being held, but in effect this interest income is being paid by the other level of government.

The issue is illustrated here with an example about Medicaid payments. A delayed federal Medicaid payment might require a state to utilize its own funds to pay the vendor, thereby causing the state to lose the interest income it could have earned had it been able to hold on to its own cash. The state perceives that the federal government's delay in making the cash payment is motivated by the

federal government's desire to earn interest income on its cash (or, equivalently, to delay borrowing the money to make the Medicaid payment, thereby avoiding interest expenses).

A state's drawing cash from a federal account prior to the date the state pays a Medicaid vendor's bill has the effect of reducing the interest income the federal government can earn on this cash. The federal government perceives that the state's early drawdown is motivated by the state's desire to earn interest income on this cash between the date of the drawdown and the date the Medicaid vendor must be paid (or, equivalently, to delay borrowing money for other state expenses, thereby avoiding interest expenses).

In May 2002, the Financial Management Service (FMS), the Bureau within the Department of the Treasury charged with implementing the CMIA, issued new clarifying regulations in the Federal Register (31 C.F.R. § 205). The regulations define the federal assistance programs covered by the CMIA and provide guidance on the mechanics of CMIA implementation.[934]

Selected Source Reading

Bruebaker, Gary and Jack Kiley. "Cash Management Improvement Act of 1990." Government Finance Review, vol. 8 (October 1992), pp. 29-31.

U.S. General Accounting Office. Financial Management: Implementation of the Cash Management Improvement Act. GAO/AIMD-96-4. January 1996.

Steven B. Maguire

[934] FMS's website provides more background information on the CMIA at [http://fms.treas.gov/cmia/index.html], visited Dec. 29, 2003.

S. User Fee Act of 1951

Statutory Intent and History

User fees — charges to recipients of goods and services provided by the government — have existed since the earliest days of the republic and, indeed, extend to the colonial period. Payment for mail delivery, use of toll roads, and certain customs services were among the first fees. In the contemporary era, there are several hundred such charges at the federal level, amassing nearly $158 billion in revenue in FY2002 alone.[935] These are authorized under a general user fee statute or, in most cases, agency-specific legislation. Such fees are usually defended as serving one or more purposes: (1) to help make a service or good self-sustaining; (2) to shift the burden of payment from the general taxpayer to an identifiable beneficiary; (3) to enhance revenue for the government; and (4) to regulate access to or determine availability of a good or service.[936]

Congressional Action. Despite the long heritage of such charges, a general user fee statute was not enacted until August 31, 1951: i.e., Title V of the Independent Offices Appropriations Act (IOAA) for Fiscal Year 1952.[937] This short provision, which was slightly modified in its 1982 codification, grants federal agencies the authority to levy charges on identifiable beneficiaries for government-provided goods and services. The law also establishes criteria to be followed in its implementation. Prior to this, an agency could impose fees only if it had specific statutory authority to do so.

In the early 1950s, several congressional panels advanced user fees on a broad scale. In 1950, the Senate Committee on Expenditures in the Executive Departments endorsed user charges for agencies under its jurisdiction and called for the "equitable transfer of many financial burdens from the shoulders of the

---

[935] U.S. Office of Management and Budget, Budget of the United States: Analytical Perspectives, Fiscal Year 2004 (Washington: GPO, 2003), p. 93.

[936] For background on the general user fee statute and a detailed survey of user charges under various public laws, see U.S. Congressional Budget Office, The Growth of Federal User Charges: An Update (Washington: CBO, 1995), along with the initial CBO study: The Growth of Federal User Charges (Washington: CBO, 1993). This effort was reinforced by a recommendation from the Representatives on the Joint Committee on the Organization of the Congress, calling upon CBO "to conduct a study of all Federal user fees and the effects of inflation on any user fees since such fees were last adjusted." U.S. Joint Committee on the Organization of the Congress, Organization of the Congress: Final Report of the House Members, H.Rept. 103-413, 103rd Cong., 1st sess. (Washington: GPO, 1993), p. 19. Further information on user charges and their implementation is available in U.S. General Accounting Office, Federal User Fees: Some Agencies Do Not Comply with Review Requirements, GGD-98-161, June 30, 1998.

[937] 65 Stat. 290. The original language and format of the statute were modified in 1982, when the authority was codified at 31 U.S.C. § 9701, by 96 Stat. 1051-1052.

taxpaying general public to the direct and special beneficiaries."[938] The next year, the House Appropriations Subcommittee on Independent Offices followed suit. Representative Yates, a member of the subcommittee, introduced its new legislation:

For the first time, our subcommittee went into a new question, the question as to whether or not there should be charges and fees made by regulatory agencies of the Government for many of the services which they render to those who come within their jurisdiction.[939]

The subcommittee emphasized that regulatory agencies, such as the Interstate Commerce Commission (ICC) and the Federal Communications Commission (FCC), must meet the expense of hearings, inspections, and other activities related to granting franchises, construction and other permits, and licenses. Continuing, Representative Yates stated:

The taxpayers pay every dollar of the charges and costs that go into that hearing. The companies pay nothing, other than taxes, and I think it is only fair that in exchange for the franchise that the Government gives the broadcasting company and the protection which the Government affords to such broadcasting company to assure its freedom from interference in the operation of its broadcasting facilities ... that it should pay some of the costs of the hearings.[940]

The subcommittee agreed and extended the doctrine to all federal agencies, not just the ones under its jurisdiction. To do this, the panel added an amendment to the appropriations bill that would permit each federal agency "to appraise its own operations to see whether or not it would be possible to recapture for the Government some of the costs that the Government incurs in connection with this regulation through the establishment of a schedule of fees."[941] In addition to this goal, Representative Yates noted that one agency official "expressed the viewpoint that such a practice would not only be feasible, but would deter and do away with superfluous applications."[942]

Executive Guidance. In 1959, the Bureau of the Budget, predecessor to the Office of Management and Budget (OMB), issued guidelines for implementing the user

---

[938] U.S. Congress, Senate Committee on Expenditures in the Executive Departments, Fees for Special Services, S.Rept. 2120, 81st Cong., 2nd sess. (Washington: GPO, 1950), p. 15.

[939] See statement by Rep. Sidney Yates, Congressional Record, vol. 97, May 3, 1951, p. 4809.

[940] Ibid.

[941] Ibid.

[942] Ibid.

fee statute.[943] Circular No. A-25 emphasized that such charges should be assessed only for special benefits provided to identifiable recipients. The circular has been revised in the interim, most recently in 1993.[944] The newest version, which rescinded the original, extended guidance to agencies operating under other statutory authority, not just the 1951 user fee statute, and made more explicit the factors that agencies should consider when assessing the government's costs in providing the good or service.

Judicial Interpretation. Federal courts have been involved in interpreting user fee legislation, both the general user fee statute as well as agency-specific authorizations.[945] The Supreme Court has determined that such charges are constitutional when they impose a true fee, which must meet certain criteria and standards for fairness and equity, among other things, and when they are an appropriate legislative delegation of authority to the executive (i.e., levying a fee for services rendered, rather than imposing a tax).

According to several Supreme Court decisions,[946] user fees are allowable under the 1951 IOAA if they recoup appropriate costs for goods or services rendered to individual beneficiaries; the charges must be based only on the costs of services or goods provided to the individual recipient, as opposed to being based on all costs of goods or services that also benefit the general public. IOAA-authorized user fees must also meet the standards of fairness and equity under the law and must not be arbitrary. Finally, such charges are acceptable if they are consistent with congressional policy and if the agency has not exceeded its authority and has not disregarded the statute's guidelines.

---

[943] U.S. Bureau of the Budget, "User Charges," OMB Circular No. A-25, Sept. 23, 1959.

[944] U.S. Office of Management and Budget, "User Charges," OMB Circular No. A-25, Revised, July 8, 1993.

[945] See CBO, The Growth of Federal User Charges, pp. 26-30; and Clayton P. Gillette and Thomas D. Hopkins, "Federal User Fees: A Legal and Economic Analysis," Boston University Law Review, vol. 67 (Nov. 1987), pp. 822-835.

[946] See, especially, Aeronautical Radio, Inc. v. United States, 379 U.S. 933 (1965). This ruling upheld the FCC fees as a constitutional delegation of authority to the executive. The Court found that they were fair and equitable; they were not arbitrary; they were consistent with congressional policy; and the agency had not exceeded its authority or disregarded the statutory guidelines. A later ruling, National Cable Television Association v. United States, 415 U.S. 336 (1974), however, struck down new and higher FCC fees; these charges were based on all costs, both direct and indirect, and were for services that benefitted the general public, not just recipients of certain services. A similar ruling resulted from a companion case, based on annual charges that the Federal Power Commission levied on natural gas companies and electric utilities. Here, the Supreme Court held that the IOAA authorized only specific charges for specific services to identifiable recipients. Federal Power Commission v. New England Power Company, 415 U.S. 345 (1974).

Major Provisions

Purposes. Current general user fee legislation directs that "each service or thing of value provided by an agency ... shall be self-sustaining to the extent possible." By comparison, the original 1951 version had provided an elaborate list of goods and services for which charges could be levied — "any work, service, publication, document, benefit, privilege, authority, use, franchise, license, permit, certificate, registration or similar thing of value or utility" — while the 1982 codification reduced it to the generic concept of "each service or thing of value."

Also, the original enactment called for such services to be "self-sustaining to the full extent possible," while the codified version omitted the word full. No other purpose — such as redirecting costs away from the general taxpayer and to the beneficiary — is specified in the legislation.

Eligible Agencies. The original 1951 enactment, when granting user fee authority to federal agencies, specifically included "wholly owned government corporations as defined in the Government Corporation Control Act of 1945." By comparison, the 1982 codification struck this language and instead specifically excluded mixed-ownership government corporations from federal agencies having authority to impose user fees.

Authority. The general user fee statute grants powers to both the head of the agency as well as to the President with regard to "executive agencies." The head of each eligible agency is authorized to issue regulations establishing the charge for a service or thing of value. The law adds that regulations issued "by the heads of executive agencies are subject to policies prescribed by the President and shall be as uniform as practicable."

Criteria and Standards. The law requires user fees to meet certain criteria and standards. Each charge, importantly, is to be "fair." The original language read "fair and equitable," but "equitable" was omitted in the codified version as being redundant and otherwise included in "fair." In addition to this requirement, the charges are to be based on:

- the costs to the government (with the original version specifying "direct and indirect" costs);
- the value of the service or thing to the recipient;
- public policy or interest served; and
- other relevant facts (with the original version reading "pertinent" facts).

Disposition of the Revenue. Revenue collected under the general user fee statute is paid into the U.S. Treasury as miscellaneous receipts. This is in contrast to some agency-specific user fee statutes, in which the revenue is deposited in dedicated accounts and earmarked to reimburse the collecting agency for certain expenses and activities.

Effect on Other Statutes. The 1951 general user fee statute and its codified current version leave intact other legislation that either proscribes or prescribes user charges. The law insists that nothing contained in it repeals or modifies other statutes prohibiting the collection or fixing of any fee, charge, or price. The enactment also states that the user fee legislation does not affect any law "prescribing bases for determining charges, but a charge may be redetermined under this section consistent with its prescribed bases."

Discussion

The general user fee statute, enacted in 1951 and modified in 1982, provides a means for standardizing user charges and specifying the basic criteria which should be met. The statute delegates broad authority and substantial discretion and flexibility to agencies to establish fees for goods and services, in order to make them self-sustaining. This legislative initiative, in turn, has been endorsed and supported by the Bureau of the Budget and its successor, the Office of Management and Budget, through regulations, most recently in 1993. Contributing to the 1993 revision of OMB Circular No. A-25, moreover, was an earlier recommendation from the Administrative Conference on the United States (ACUS). Based on a major study of user fees that it had commissioned, in 1987, ACUS recommended general principles to guide the setting and implementation of user fees.[947]

The general user fee statute, however, has failed to standardize user fees and most of these charges result from specialized grants of authority to particular agencies. Several reasons explain this situation.

One is that the language of the general user fee law is vague, and its provisions have been viewed as inconsistent. Most open-ended, for instance, is the allowance that "other relevant facts" be considered when establishing a charge. In addition, charges that are set to make a service "self-sustaining" may not be "fair" to the parties who must pay. Furthermore, the requirement to consider public policy or other interests might result in costs that differ from the actual costs of providing a good or service. Regulating or reducing the volume of traffic at congested national parks, if that were a public policy goal, for instance, might require higher prices for parking and admission than would otherwise be justified in terms of the actual costs to the government and the value of the service to the recipient.

Other reasons help to explain a reluctance to use the across-the-board authority and instead rely on specific legislation to establish particular charges for goods or services. Operating under the general user fee statute requires an agency to act

---

[947] U.S. Administrative Conference of the United States, "User Fees," Recommendation 874, adopted June 12, 1987.

alone, without the immediate support of Congress for the specific charge. This means that the agency incurs the objections directly and solely from adversely affected parties, that is, the individuals and industries who must pay a new or higher price (for a good or service that they had received previously for free or at a lower price). This development may result in public criticism of the agency's planned charges, intense opposition to them before Congress as well as other parts of the executive, or in potentially costly court challenges to the fees.[948]

Besides these disincentives to using the general user fee statute, agencies lack a financial or budgetary incentive to impose fees under the IOAA: its revenue is deposited in the general treasury and is not dedicated for use by the agency itself. In short, the agency would have to do the work (e.g., argue on behalf of a charge, establish the proper fee amount, and collect the revenue) but receive no direct budget benefit. In contrast, some agency-specific user fee statutes establish special accounts in the treasury and earmark the revenue for the agency's own use, for instance, to reimburse it for collection expenses and/or to support certain operations and activities. In addition to determining the disposition of the revenue, specialized user fee statutes, by comparison to the general authority, allow Congress to control virtually all other aspects of such charges. Legislation can be used to erect a fee structure, set the fees themselves, identify and charge particular beneficiaries or recipients of a service, and provide for exemptions among specific recipients and exceptions to certain fees.

Selected Source Reading

Gillette, Clayton P. and Thomas D. Hopkins. "Federal User Fees: A Legal and Economic Analysis." Boston University Law Review, vol. 67 (November 1987), pp. 795-874.

Kaiser, Frederick M. "U.S. Customs Service User Fees: A Variety of Charges and Countercharges." Public Budgeting and Finance, vol. 8 (autumn 1988), pp. 78 95.

Sperry, Roger L. "Gold Rush." Government Executive, vol. 30 (March 1998), pp. 13-17.

U.S. Administrative Conference of the United States. Federal User Fees: Data Compilation with Addendum. Washington: ACUS, 1988.

——. Federal User Fees: Proceedings of a Symposium, edited by Thomas D. Hopkins. Washington: GPO, 1988.

[948] See CBO, The Growth of Federal User Charges, pp. 15-31; Gillette and Hopkins, "Federal User Fees," pp. 869-873; Frederick M. Kaiser, "U.S. Customs Service User Fees: A Variety of Charges and Countercharges," Public Budgeting & Finance, vol. 8 (autumn 1988), pp. 78-95; and Roger L. Sperry, "Gold Rush," Government Executive , vol. 30 (Mar. 1998), pp. 13-17.

U.S. Congressional Budget Office. The Growth of Federal User Charges. Washington: CBO, 1993.

——. The Growth of Federal User Charges: An Update. Washington: CBO, 1995.

U.S. General Accounting Office. Federal User Fees: Budgetary Treatment, Status, and Emerging Management Issues, GAO/AIMD-98-11. December 1997.

——. Federal User Fees: Some Agencies Do Not Comply with Review Requirements. GAO/GGD-98-161. June 1998.

CRS Report 89-625E. Federal User Fees: An Overview, by Julius Allen (1989). (This CRS report is archived and available from the author of this entry in the compendium.)

U.S. President's Council on Integrity and Efficiency, Audit Committee. Audit of the Establishment and Collection of User Charges. Washington: OMB, 1989.

Frederick M. Kaiser

IV. Organization

A. Government Corporation Control Act

Statutory Intent and History

In 1945, partly in response to the proliferation of corporate bodies created during the Depression and World War II, Congress enacted the Government Corporation Control Act (59 Stat. 841; 31 U.S.C. §§ 9101-9110).[949] The intent of the act was (1) to establish consistent treatment and appropriate accountability and control of revenue producing business enterprises organized as corporate bodies; and (2) to assure reasonable financial autonomy and flexibility in carrying out authorized programs.[950]

The Control Act does not define what constitutes a government corporation or how corporations may or may not differ from other categories of agencies. The charter for each federal government corporation is the separate enabling legislation passed by Congress. The Control Act simply lists corporate organizations covered by the act, a list that is subject to occasional additions and deletions.[951] The act provides for two types of government corporations: "wholly owned government corporations," and "mixed-ownership government corporations." In the absence of a criteria-based definition, the number of government corporations may differ from one source to another. The most commonly used estimates suggest a figure between 22 and 44, both figures derived from General Accounting Office (GAO) reports.[952]

Despite the Control Act's silence on the matter, a working definition of government corporation has emerged.[953] The distinguishing characteristics of a federal government corporation are that it is an agency of government, established by Congress to perform a public purpose, which provides a market-

---

[949] Hereafter, "the Control Act."

[950] In 1982, P.L. 97-258 codified the 1945 act's provisions as 31 U.S.C. §§ 9101-9110 and technically repealed the 1945 act. These sections of the United States Code constitute the basic corporate control law.

[951] For example, in 1945 the Control Act listed the Reconstruction Finance Corporation. After this corporation was abolished in 1957, it was removed from the list.

[952] In a 1988 report, GAO profiled some 44 government corporations. See U.S. General Accounting Office, Profiles in Existing Government Corporations, GAO/AFMD-89-43FS, Dec. 1988. In 1995, using a more precise and narrow definition, GAO concluded that there were actually 22 government corporations. U.S. General Accounting Office, Government Corporations: Profiles of Existing Corporations, GAO/GGD-96-14, Dec. 1995.

[953] National Academy of Public Administration, Report on Government Corporations (Washington: NAPA, 1981).

oriented service that produces revenue that meets or approximates its expenditures. Corporations cover the spectrum in size and function from large, well-known corporations, such as the Federal Deposit Insurance Corporation, to small, low-visibility corporate bodies, such as the Federal Prison Industries in the Department of Justice. The absence of a statutory definition has led to some agencies being designated "corporations" although they perform no commercial function (e.g., Legal Services Corporation), and to confusion with "government-sponsored enterprises" (e.g., Federal National Mortgage Association, "Fannie Mae") that are instrumentalities, not agencies of the United States.

The courts have deemed government corporations to be agencies of the United States (Cherry Cotton Mills v. United States, 327 U.S. 536 (1946)) and, therefore, subject to laws generally applicable to agencies, unless otherwise exempted by a general statute or a statute applicable to the individual corporation. In practice, application of government-wide statutes tends to vary widely among the corporations, and it is necessary to review the status of each corporation to appreciate the full scope of the exceptions.

Major Provisions

The major provisions of the Control Act provide for (1) establishing and acquiring of corporations; (2) business type budgeting; (3) audits and management reports; and (4) accounts and obligations, and standards for depository institutions holding government corporation securities.

Some agencies (such as the Department of Agriculture, the National Credit Union Administration, and the Department of Housing and Urban Development, to name a few) have established or acquired government corporations.[954] However, under the Control Act an agency may only do so if specifically authorized by Congress.

Once established, a government corporation annually must prepare and submit to the President a business-type budget. The budget, which contains estimates and statements of financial condition, income, and expenses, is then submitted to Congress in the President's budget proposal. Although government corporations are usually expected to earn sufficient revenues to cover costs, Congress may supplement the government corporation's budget and provide for its debts.

The inspector general of every government corporation must annually audit the corporation's financial statements and submit audit reports to the head of the corporation, the Chairman of the House Committee on Government Reform and

[954] Most government corporations, though, are established independent of federal departments.

the Chairman of the Senate Committee on Governmental Affairs.[955] The Comptroller General of the United States may review the audit and report his findings to the Director of the Office of Management and Budget (OMB) and the head of the corporation. The Control Act also requires a government corporation to provide management reports each year to the President, the Director of OMB, the Comptroller General, and Congress. Management reports must include statements of financial position, operations, cash flows, the results of the inspector general's audit, and other items as required in the corporation's charter.

Government corporations, unlike most government agencies, are permitted to issue obligations. However, a corporation must first seek the approval of Secretary of the Treasury, who may decide many particulars of the obligation (e.g., interest rate, maturity). The Control Act also empowers a government corporation to consolidate its cash into an account kept by the Secretary of the Treasury at a Federal Reserve bank or other bank or fiscal agent as designated by the Secretary.

Discussion

The government corporation is an attractive option to policymakers for three reasons. First, government corporations possess significant revenue streams not available to other government agencies: commercial activities and government obligation issuance. Second, government corporations are largely exempted from government management laws (including personnel and compensation ceilings). Finally, government corporations can be used as transition organizations toward eventual privatization of some government agency or program (e.g., U.S. Enrichment Corporation). On the whole, then, the government corporation option offers policymakers some of the attractions of a private entity without sacrificing governmental control.[956]

---

[955] The inspector general may also assign this responsibility to an independent external auditor or the head of the corporation.

[956] Government corporations, no matter what function they perform or how "private" they may appear to the public or to themselves, are agents of the state subject to constitutional limitations. As the Supreme Court concluded in the 1995 Lebron case involving the status of AMTRAK, a government corporation has certain inherent legal characteristics that cannot be shed simply by legislative language or by corporate fiat. In the Lebron case, the Supreme Court decided that, while Congress can determine AMTRAK's governmental status for purposes within Congress's control (e.g., whether it is subject to general management laws, such as the Administrative Procedure Act), Congress cannot make the final determination of AMTRAK's status as a governmental entity for purposes of determining constitutional rights of citizens affected by its actions. To do so, in the Court's view, would mean that the government could evade its most solemn constitutional obligations by simply resorting to the corporate form of organization. (Michael A. Lebron v. National Railroad Passenger Corporation, 513 U.S. 374 (1995).)

Selected Source Reading

Mitchell, Jerry. The American Experiment with Government Corporations. Armonk, NY: M.E. Sharpe, 1999.

National Academy of Public Administration, Report on Government Corporations, vol. 2. Washington: National Academy of Public Administration, 1981.

Congress. Senate. Committee on Governmental Affairs. Managing the Public's Business: Federal Government Corporations, by Ronald C. Moe. S.Prt. 104-18. 104th Congress, 1st session. Washington: GPO, 1995.

General Accounting Office. Government Corporations: Profiles of Existing Government Corporations. GAO/GGD-96-14. December 1995.

CRS-199 CRS Report RL30365. Federal Government Corporations: An Overview, by Ronald C. Moe.

Kevin R. Kosar

B. Reorganization Act of 1977, as Amended

Statutory Intent and History

Although reorganization authority expired in 1984 and has not been renewed since, it is still part of the United States Code.[957] The authority to reorganize federal agencies has been delegated by Congress to the President from time to time since 1932. In 1949, the President submitted to Congress the reorganization bill that would form the basis of reorganization authority through 1977. The Reorganization Act of 1949 provided that the President could submit a reorganization plan involving any agency. This plan would go into effect as law after 60 days unless a resolution of disapproval was passed by a majority in either House (a one-house veto). Over time, Congress periodically renewed the President's reorganization authority, although the length of extensions varied and on occasion the authority was allowed to lapse.

As renewals were sought and debated, amendments were adopted altering the original law. For the most part, these amendments limited the President's authority. In most instances, specific incidents led to the limitations on presidential authority. For example, after failing to obtain a Department of Housing and Urban Development through legislation, President Kennedy employed the reorganization plan process. The plan was approved and the department established. Congress, however, found fault with the reorganization authority, and when it came up for renewal in 1963, Congress let the authority lapse. In 1965, when President Johnson once more requested the authority, Congress granted it but inserted a provision prohibiting the use of the reorganization authority to create new executive departments.

One of President Carter's first legislative proposals was a request that Congress renew the President's authority to submit reorganization plans. The Reorganization Act of 1977, as finally enacted, represented a procedural compromise. The approval process remained the same as in the 1949 Reorganization Act, except that a resolution of disapproval, subject to certain expedited procedures, was automatically introduced in both chambers. This ensured a congressional up-or-down vote. In addition, the President was permitted to amend a plan within 30 days after its submission, thus allowing for modifications in response to congressional concerns.

A major blow was struck against the reorganization plan procedure in 1983, when the Supreme Court ruled in INS v. Chadha that the legislative veto process was unconstitutional.[958] The Court held that exercises of legislative power must fulfill the constitutional requirement of consideration by both houses of Congress and

---

[957] 5 U.S.C. §§ 901-912.

[958] 462 U.S. 919 (1983).

"presentment" to the President. Inasmuch as legislative vetoes frequently provided for consideration by only one house and, by definition, did not involve the President, the mechanism was found to be constitutionally deficient. One consequence of the Chadha ruling was that Congress passed legislation in 1984 that had the effect of ratifying reorganization plans previously approved (P.L. 98-532; 98 Stat. 2705).

Congress approved the Reorganization Act Amendments of 1984, which extended the reorganization plan authority from November 1984 to December 31, 1984. Although it was never used and has expired, this version of reorganization authority remains "on the books," and maybe found in Chapter 9 of Title 5 of the United States Code. The 1984 amendments, an effort to address the constitutional issues raised by the Chadha decision, required that a joint, rather than concurrent, resolution be introduced in both the House and Senate upon receipt of a reorganization plan. Another significant innovation in the 1984 amendments was the requirement that an implementation section be included in the President's message accompanying the reorganization plan.

In the absence of presidential reorganization authority, reorganizations of federal agencies are accomplished through the regular legislative process.[959] Prominent examples of such reorganizations include the creation of the Department of Veterans Affairs[960] in 1988 and the creation of the Department of Homeland Security in 2002.[961]

Major Provisions

Under provisions of the Reorganization Act of 1977, as amended through 1984, the President could submit to Congress a reorganization plan providing for the transfer, in whole or in part, of an agency or its functions to another agency, "except that no enforcement or statutory program shall be abolished by the plan."[962] A plan could not "create a new department," continue an agency or function beyond the period authorized by law, or authorize an agency to perform a function not expressly provided in law.[963]

---

[959] Certain agency heads are statutorily vested with the authority to conduct limited reorganizations within their own organizations. For example, such authority is vested in the Secretary of Defense in Title 10, Section 125, of the United States Code.

[960] P.L. 100-527, 102 Stat. 2635.

[961] P.L. 107-296, 116 Stat. 2135.

[962] 5 U.S.C. § 903(a)(2).

[963] 5 U.S.C. § 905(a). The statute includes several other limitations on what can be achieved by a reorganization plan.

Once the President submitted a reorganization plan, Congress had 90 days to act upon the following joint resolution: "That the Congress approves the reorganization plan numbered _____ transmitted to the Congress by the President on _____, 19___."[964] The President had to provide an "implementation plan" meeting the requirements of the law when submitting a plan. As a joint resolution, this vehicle had to be approved by the President to have the force of law.

Discussion

The original rationale for delegating to the President broad authority to propose executive reorganization plans was the widely held view that the President, as chief manager of the executive branch, ought to have powers to make organizational and management changes without having them subject to so-called "political pressures" from Congress. Reorganization was viewed in large measure as a technical exercise best left to the experts in the executive branch.

Reorganization is now not usually regarded as merely a technical exercise. Reorganizations may lead to increased organizational efficiency, economy, and effectiveness, but they also often have significant institutional and political consequences. From the early 1960s on, questions were raised in congressional deliberations as to both the constitutional bases for reorganization authority and processes and the political wisdom of assigning this broad authority to the White House. The successive reorganization acts were founded upon the concept of permitting the President to submit to Congress what were, in fact, laws that would go into effect unless either house prevented activation by passing a motion of disapproval. Despite modifications of the process, this "legislative veto" was increasingly criticized as the years passed.

The reorganization process began to be questioned in terms of both its utility and its potential for increasing conflict and distrust between the branches. Congress, in successive reorganization acts, gave the President authority to circumvent the regular legislative process. Yet, when Presidents invoked the authority, they opened themselves to the accusation of violating the established system. Plans were sometimes submitted that probably would not have been accepted using the regular legislative process, thus increasing tension between the branches. After each presidential "misuse," Congress responded by adding restrictions and exemptions, gradually circumscribing the power until the reorganization plan process (provided in the 1977 act, as amended) was a mere shadow of the original Reorganization Act of 1949. With the 1983 Chadha decision striking down the legislative veto, the utility and desirability of using the reorganization act, compared to following the regular legislative process, came into question.

[964] The quotation is taken from the statute, which has not been updated to reflect the new century.

Nonetheless, the drawbacks of reorganization authority might be outweighed, for some, by the perceived difficulty of reforming government organization through the conventional legislative process. It could be argued that the need for modernization of the federal bureaucracy warrants the renewal of the President's reorganization authority, with appropriate modifications and safeguards for congressional prerogatives.

Selected Source Reading

Arnold, Peri E. Making the Managerial Presidency: Comprehensive Reorganization Planning, 1905-1996, 2nd ed. Lawrence, KS: University Press of Kansas, 1998.

CRS Report RL30876. The President's Reorganization Authority: Review and Analysis, by Ronald C. Moe.

Emmerich, Herbert. Federal Organization and Administrative Management. Tuscaloosa, AL: University of Alabama Press, 1971.

Fisher, Louis and Ronald C. Moe. "Presidential Reorganization Authority: Is It Worth the Cost?" Political Science Quarterly, vol. 96 (summer 1981), pp. 301 318.

U.S. Congress. House. Committee on Government Operations. Reorganization Act Amendments of 1983. H.Rept. 93-128. 98th Congress, 1st session. Washington: GPO, 1984.

Henry B. Hogue

C. Federal Vacancies Reform Act of 1998

Statutory Intent and History

The Federal Vacancies Reform Act of 1998[965] (Vacancies Reform Act) replaces the Vacancies Act of 1868,[966] as amended (5 U.S.C. §§ 3345-3349d). The purpose of the 1868 act and the 1998 act is the same: to provide for the temporary filling of certain positions in the executive branch to which the President makes appointments, subject to the advice and consent of the Senate.

The 1868 act, which applied only to executive departments — no independent agencies existed at the time — provided that when an incumbent in an advice and consent position died or resigned, or was absent or sick, the first assistant thereof was to perform the duties of the office, unless the President designated someone else who was occupying a position for which he or she had been confirmed by the Senate. Whoever assumed the duties of the position could do so for no longer than 10 days when the vacancy was caused by death or resignation. An 1891 amendment extended the time period to no more than 30 days.[967] In 1988, the act was amended once again, extending the time period to no more than 120 days. In addition, several new provisions were added to the act. The 120-day time period was suspended if a first or second nomination to fill the vacancy was before the Senate, but would begin to run again if the nomination was rejected or withdrawn. For the first time, the heads of executive agencies were brought under the act. Finally, a temporary appointment or designation could be made only under provisions of the act, except for recess appointments.[968]

The Vacancies Reform Act addresses a number of issues raised in the administration of the prior act. These include, but are not limited to, (1) extending the act's coverage to all advice and consent positions in single-headed executive independent agencies; (2) extending the President's authority to make temporary appointments to include officials who are not in positions for which they were confirmed by the Senate; (3) lengthening the time a first assistant or acting or designated officer may serve; (4) stipulating that the act is the exclusive means for temporarily filling vacant positions, except for recess appointments and instances in which express statutory authority provides otherwise; (4) providing for the Comptroller General to report to Congress regarding agency adherence to the act; (5) temporarily suspending the now 210-day time period during a presidential inaugural transition; and (6) specifying that positions in

---

[965] The act is found in P.L. 105-277 (Omnibus Consolidated and Emergency Supplemental Appropriations for FY1999) under Division C, Title 1, Sec. 151.

[966] Act of July 23, 1868, Ch. 227, 15 Stat. 168.

[967] Act of Feb. 6, 1891, Ch. 113, 26 Stat. 733.

[968] P.L. 100-398, Sec. 7; 102 Stat. 988.

independent multi-headed regulatory boards and commissions, as well as certain other positions, are not covered by the act.

Major Provisions

Section 3345. Acting Officer. Provides that if an officer in an advice and consent position dies, resigns, or is unable to perform his or her duties, the office may be filled temporarily in one of two ways: (1) the first assistant to the office assumes the duties of the office, unless he or she has been nominated for the vacant position and has served as first assistant for fewer than 90 of the preceding 365 days; or (2) the President selects either (a) an official from another position to which he or she has been confirmed, or (b) an official from the affected agency, whose pay rate is at least equal to GS-15, and who has been at the agency for at least 90 of the preceding 365 days.

Section 3346. Time Limitation. Establishes a 210-day time period after a vacancy occurs during which an acting officer may serve. If the vacancy occurs during an adjournment sine die, the time period begins when the Senate first reconvenes. If on the last day of the 210-day period the Senate is not in session, the second day the Senate is next in session shall be deemed to be the last day of such period (Section 3348). The 210-day restriction is suspended if a nomination is pending, but begins anew if the nomination is rejected, returned, or withdrawn. A second nomination again suspends the time restriction, which does not begin again unless the second nomination is rejected, returned, or withdrawn. (See also Section 3349a for additional time limitation provisions.)

Section 3347. Exclusivity. Provides that Sections 3345 and 3346 are the exclusive means for temporarily filling a vacant advice and consent position in an executive department or agency, unless (1) a statutory provision specifically authorizes the President, a court, or the head of an executive department to temporarily fill a specific position, or designates an officer or employee to temporarily fill a specific position; or (2) the President makes a recess appointment. The section specifically nullifies the previously held position of the Justice Department that the statutory vesting of general agency authority in the head of an agency, and allowing this authority to be delegated, provides an alternative way to fill vacant advice and consent positions.

Section 3348. Vacant Office. Provides that a vacant advice and consent position may not be filled temporarily except in conformity with the Vacancies Reform Act, and that an action taken by any person who is not acting under the provisions of the act shall have no force or effect and may not be ratified. Provides further that the head of a department or agency may perform the functions and duties of a vacant, subordinate, advice and consent position. The head of the agency may not perform these functions and duties, however, for the following positions: General Counsel of the National Labor Relations Board, General Counsel of the Federal Labor Relations Authority, any inspector general or chief financial officer in an advice and consent position, or any executive

agency position, if a statutory provision expressly prohibits the head of the agency from performing the functions and duties of such office.

Section 3349. Reporting of Vacancies. Directs each agency head to notify the Comptroller General and each house of Congress when a covered vacancy occurs, including the name of the acting officer, the name of the nominee for the position, and the date a nomination is rejected, withdrawn, or returned. If the Comptroller General determines that an acting officer is serving longer than the 210-day period, including the applicable exceptions, he is to report this fact to specified committees of Congress, to the President, and to the Office of Personnel Management.

Section 3349a. Presidential Inaugural Transitions. Provides that for any vacancy that exists during the first 60 days after a new President assumes office, the 210-day time period does not begin until 90 days after the inauguration date, or 90 days after the vacancy occurs, whichever is later.

Section 3349b. Holdover Provision. The act does not affect any statute that authorizes a person to continue serving in a fixed-term position after a term expires, until a successor is appointed or a specified period of time has expired.

Section 3349c. Exclusion of Certain Officers. The act does not cover any advice and consent officer on a board, commission, or similar entity that is composed of multiple members and governs an independent establishment or government corporation; or any member of the Federal Energy Regulatory Commission or the Surface Transportation Board; or any judge on an Article I court.

Section 3349d. Notification of Intent to Nominate. Provides that if, during a recess or adjournment of the Senate of at least 15 days, the President sends a written notification of intent to nominate a specific individual to a specific office, this notice shall be considered a nomination for purposes of the act. If the President does not submit the nomination within two days after the end of the recess or adjournment, the nomination shall be treated as a withdrawn nomination for purposes of the act.

The Vacancies Reform Act became effective on November 20, 1998, and applies to any vacancy occurring after that date. The 210-day limitation applies to any office that was vacant on the effective day as if the vacancy had occurred on that date.

Discussion

The Vacancies Reform Act was largely inspired by evidence that, by early 1998, as many as 25% of the 320 advice and consent positions in executive departments were being filled by temporary designees, most of whom had served beyond the 120day limitation period of the old act and had not been nominated by the President. In addition, it was found that this evasion of the Senate's

constitutional confirmation prerogative was being supported by the Department of Justice (DOJ). The department had developed a legal construction of the enabling legislation of the 14 departments that effectively superceded the requirements of the old act. The Attorney General was interpreting general housekeeping provisions found in the enabling statutes of all the departments as authority for the head of the department to designate an acting official to occupy, for an indefinite term, a vacant position requiring Senate confirmation. These provisions[969] vest department heads with the powers and functions of their agencies, and with authority to delegate some of their authority to their subordinates.[970] The Comptroller General had rejected Justice's interpretation and issued a series of opinions on the matter.[971] The Vacancies Reform Act makes clear that its requirements are exclusive and specifically rejects the DOJ position. To assure that the executive branch will comply with the act, the Comptroller General is now required to report to Congress if any acting officer is serving longer than the 210-day period (including the applicable extensions). In addition, the statute now stipulates that the acts of any person who is not acting under its provisions have no force or effect and may not be ratified.

The Vacancies Reform Act also addresses some of the President's concerns, particularly regarding the amount of time taken to fill positions through the regular advice and consent appointment process. Aware of the problem, Congress extended the time limit for a temporary appointment from 120 to 210 days. In addition, the 210-day time limit is suspended for a specific period during the inaugural transition period of a new President. Finally, the President now has wider choice when designating an acting official.

The Vacancies Reform Act vests the Comptroller General with the task of monitoring agency compliance, by establishing requirements for reporting, to the Congress and the Comptroller General, action related to vacancies in advice and consent positions, as well as setting standards for who can be named to act in these positions when they are vacant and how long they can remain. In performance of this duty, since 1999, the General Accounting Office (GAO) has issued a series of reports that examined agencies' performance in implementing the act. It found substantial lags between the time a reportable event, such as the

---

[969] See, e.g., such provisions for DOJ at 28 U.S.C. §§ 509-510.

[970] The assertion of DOJ's position at that time is found in two letters to Senator Strom Thurmond from Andrew Fois, Assistant Attorney General, Office of Legislative Affairs, dated May 2, and July 10, 1997.

[971] See, e.g., 65 Comp. Gen. 626-635, issued on June 9, 1986. An analysis of the issue, which supports the Comptroller General's position, is found in CRS Congressional Distribution Memorandum, Validity of Bill Lann Lee as Acting Assistant Attorney General for Civil Rights, by Morton Rosenberg, in U.S. Congress, Senate Committee on Governmental Affairs, Oversight of the Implementation of the Vacancies Act, hearing on S. 1764, 105th Cong., 2nd sess., Mar. 18, 1998, S.Hrg. 105-495 (Washington: GPO, 1998), pp. 62-100.

naming of an acting officer, occurred and the time it was reported, as well as instances that were not reported at all. It also identified instances in which an acting officer exceeded the legally allowed maximum period for service in this capacity.[972] In 2003, GAO issued a report identifying approaches that would facilitate prompt and accurate compliance with the act's provisions that could be applied throughout the executive branch. The report identified five critical elements essential to agency compliance with the act:

(1) clear identification of the agency components responsible for each requirement under the act; (2) frequent communication between the responsible agency components; (3) maintaining up-to-date lists of the first assistants to each covered advice and consent position; (4) documentation of an agency's Vacancy Reform Act procedures to guide responsible persons when a triggering vacancy occurs; and (5) assigning Vacancy Reform Act responsibilities to career employees so as to assure continuity of an agency's compliance activities. (See the GAO report listed under "Selected Source Reading" below.)

Selected Source Reading

U.S. General Accounting Office. Federal Vacancies Reform Act: Key Elements for Agency Procedures for Complying with the Act. GAO-03-806. July 2000.

CRS Report 98-892A. The New Vacancies Act: Congress Acts to Protect the Senate's Confirmation Prerogative, by Morton Rosenberg (1998).

CRS Congressional Distribution Memorandum. Validity of Bill Lann Lee as Acting Assistant Attorney General for Civil Rights, by Morton Rosenberg. In U.S. Congress. Senate. Committee on Governmental Affairs. Oversight of the Implementation of the Vacancies Act. Hearing on S. 1764. 105th Congress, 2nd session, March 18, 1998. S.Hrg. 105-495, pp. 62-100.. Washington: GPO, 1998.

Morton Rosenberg
Henry B. Hogue

---

[972] For example, see U.S. General Accounting Office, Violations of the 210-Day Limit Imposed by the Vacancies Reform Act, B-286265, Sept. 15, 2000; Implementation of the Federal Vacancies Reform Act of 1998, GAO/GGD-00-210R, Sept. 29, 2000; Eligibility Criteria for Individuals to Temporarily Fill Vacant Positions Under the Federal Vacancies Reform Act of 1998, GAO-01-468R, Feb. 23, 2001; and Presidential Appointments: Agencies' Compliance with Provisions of the Federal Vacancies Reform Act of 1998, GAO 01-701, May 31, 2001.

V. Procurement and Real Property Management

A. Public Buildings Act of 1959

Statutory Intent and History

Until 1926, each federal building was approved and funded in separate legislation. With exceptions, this remained the practice until enactment of the Public Buildings Act of 1926 (44 Stat. 630). This act provided the basic authority for construction of federal buildings by congressional authorizations and appropriations. Congress later enacted the Public Buildings Act of 1949 (63 Stat. 176) to authorize the acquisition of sites and design plans for federal buildings located outside Washington, DC, and for improvement to existing federal buildings. The same year, Congress enacted the Federal Property and Administrative Services Act of 1949 (63 Stat. 377). This act established the General Services Administration (GSA) and gave the GSA Administrator responsibility for administering federal real property. In 1954, Congress amended the Public Buildings Act of 1949 to authorize the GSA Administrator to acquire titles to real property and to construct federal buildings through lease-purchase contracts (68 Stat. 518). Under this procedure, a building was financed by private capital, and the federal government made installment payments on the purchase price in lieu of rent payments. Title to the property vested in the federal government at the end of the contract period, generally between 10 and not more than 30 years. When authority for lease-purchase contracts expired in 1957, Congress approved a successor statute, the Public Buildings Act of 1959 (40 U.S.C. § 3301 et seq.). The 1959 act re-established earlier requirements to provide for direct federal construction of public buildings through the congressional appropriations and authorizations process. This act, as amended and re-codified over the years, remains the basic statute authorizing the construction and renovation of federal civilian facilities.

The Public Buildings Act Amendments (86 Stat. 216) were enacted in 1972 to address a backlog of congressionally authorized building projects which had not received appropriations since 1959. The legislation authorized the GSA Administrator to use lease-purchase contracts for a three-year period to construct 68 federal buildings in an attempt to reconcile the urgent need for new federal facilities with budgetary constraints. The Federal Buildings Fund (FBF) was also established within GSA to be used for acquisition and maintenance of real property. Revenue to the FBF was supplied from rent payments charged to federal agencies occupying GSA's office space.

The Public Buildings Act Amendments of 1988 (102 Stat. 4049) were enacted to permit the GSA Administrator to enter into five-year contracts to realize greater savings in the operations and maintenance of federal facilities. The 1988 act increased to $1.5 million the threshold for projects not requiring approval of the congressional authorizing committees.

Major Provisions

The Public Buildings Act, as amended, codifies existing law and establishes a uniform method for meeting the building needs of the federal government. The act vests with the Administrator of General Services sole authority to acquire, construct, alter, repair, remodel, improve, or extend most federal buildings, and to acquire the sites or additions to sites for such buildings It also requires GSA to submit to the congressional authorizing committees a detailed prospectus of all proposed building projects costing over $1.5 million prior to the appropriation of funds, and requires GSA to submit an annual report to Congress on all projects and conduct an ongoing survey of federal building needs.

Discussion

Since 1972, the FBF has financed GSA's real property activities through reimbursements for purchases of goods and services or as rent paid for space in GSA-owned and leased buildings. While revenue to the FBF is the principal source of funding, Congress annually authorizes how GSA may allocate its FBF revenues as new obligational authority in appropriations funding. In its early years, the revenues from the FBF proved inadequate to provide operating capital for federal buildings. As a result of insufficient revenues, GSA turned increasingly to the leasing of space to meet federal agency needs, which totaled nearly $1.2 billion in FY1988.

In response, Congress authorized a total of $2.8 billion in new appropriations to the FBF for construction of new federal facilities between 1990 and 1997. The following year, Congress authorized $450 million to be deposited into the FBF from GSA's rent revenues, and also authorized a new appropriation of $492 million for the acquisition and construction of new federal facilities. Since that time, Congress has generally remained supportive in its funding of new construction projects, while requiring GSA to justify and monitor all proposed building costs.

Most recently, the December 2003 conference report (H.Rept. 108-401) to accompany the FY2004 omnibus appropriations bill (H.R. 2673) recommended that an additional $446 million be deposited into the FBF, for a total of $6,758 million. Of this total, $708 million is to be used for new construction, and an additional $991 million is to remain available until expended for repairs and alterations.

GSA's Public Buildings Service (PBS) provides property and asset management, as well as acquisition and property disposal services. GSA has constructed nearly 1,800 buildings, and leases space in approximately 6,500 privately-owned buildings. Adequate funding for repairs and alterations continues to be of major concern for the PBS, so that it can maintain and improve these properties that are in the government's inventory. A June 2003 General Accounting Office report

noted that more than $10 billion would be needed for repairs and renovations to the federal facilities constructed over 50 years ago.[973]

In both the 106th and 107th Congresses, legislation was introduced to reform property management by providing greater flexibility to GSA and executive branch agencies to manage their personal property assets more effectively. Past legislative proposals included the transfer and exchange of property with other agencies and qualifying private-sector entities, the use of subleases on unexpired portions of government leases, and the leasing of certain federal assets to the private sector. In the 108th Congress, two bills have been introduced in the House to revise federal property management policies (H.R. 2548 and H.R. 2573). If enacted, the proposed legislation would authorize the GSA Administrator to enter into agreements with non-federal entities to sell or sublease real property that is no longer needed by the federal government. These proposed changes to existing law are intended to give greater flexibility to GSA and federal agencies to manage more effectively and oversee federal property assets based on changing mission requirements.

Selected Source Reading

Congress. House. Committee on Government Reform and Oversight. Subcommittee on Government Management, Information, and Technology. Oversight of Federal Real Property Policy. Hearings. May 4, 1998. 105th Congress, 2nd session. Washington: GPO, 1999.

Congress. House. Committee on the Judiciary. Revision of Title 40, United States Code, "Public Buildings, Property, and Works." S.Rept. 107-479. 107th Congress, 2nd session. Washington: June 2002.

General Accounting Office. Federal Real Property: Executive and Legislative Actions Needed to Address Long-standing and Complex Problems. GAO-03839T. June 5, 2003.

Stephanie Smith

---

[973] U.S. General Accounting Office, Federal Real Property: Executive and Legislative Actions Needed to Address Long-standing and Complex Problems, GAO-03-839T, Washington: June 5, 2003, p. 1.

B. Federal Acquisition Streamlining Act of 1994

Statutory Intent and History

The 103rd Congress enacted the Federal Acquisition Streamlining Act of 1994 (FASA; 108 Stat. 3243), a comprehensive procurement reform effort designed to streamline the civilian and military acquisition process, which totaled $234.9 billion in FY2002. The new law was based in large part on recommendations contained in the 1993 National Performance Review (NPR) report.[974] These reforms included the revision and consolidation of existing procurement statutes, increased use of commercially available items, and adoption of a simplified acquisition purchase threshold of $100,000. Immediately after signing FASA into law, President William Clinton issued E.O. 12931, requiring executive branch agencies to make their administrative procurement procedures more effective and innovative "over and above those required by statute."[975]

By way of background, the Federal Property and Administrative Services Act of 1949 (41 U.S.C. § 251 et seq.) established a statutory basis for the postwar procurement procedures of civilian agencies. The legislation created the General Services Administration (GSA) to procure supplies and services, including federal buildings as well as their management, and to set records management standards. Since 1949, the enabling law's original provisions have been frequently and substantially amended. Enactment of FASA was a comprehensive attempt to revise and consolidate duplicative federal regulations that often hindered an agency's ability to procure the highest quality goods at the lowest cost. Potential vendors also complained of the frustrating complexity of federal specifications that controlled the design and production of goods.

The Federal Acquisition Regulation (FAR) is the codification of uniform policies and procedures for executive branch acquisitions, and is the primary regulation used in the acquisition of supplies and services. The FAR is maintained and revised by the Federal Acquisition Regulatory Council, which is composed of the GSA Administrator, the Secretary of Defense, and the Administrator of the National Aeronautics and Space Administration. The FAR is published as Chapter One of Title 48 of the Code of Federal Regulations. It can also be accessed online at [http://www.arnet.gov/far]. The Office of Federal Procurement Policy (OFPP), established within the Office of Management and Budget (OMB) in 1974, provides oversight of federal procurement policies for executive branch agencies (41 U.S.C. § 404). The OFPP Administrator is responsible for oversight of the council, and provides the final approval on

---

[974] U.S. Office of the Vice President, National Performance Review, From Red Tape to Results: Creating a Government That Works Better & Costs Less (Washington: GPO, 1993), pp. 26-31.

[975] 3 C.F.R., 1995 Comp., pp. 925-926.

revisions to the FAR, in the event the three member agencies fail to agree in a timely manner.

Until 1996, GSA also had responsibility for technology procurement. The Information Technology Management Reform Act (110 Stat. 679), which was incorporated as an amendment into the National Defense Authorization Act for FY1996, transferred authority for information technology acquisitions from GSA to OMB (40 U.S.C. § 1401). Later retitled the Clinger-Cohen Act (110 Stat. 3009-393), this comprehensive legislation provided federal agency procurement officials greater flexibility to acquire information technology systems through the use of multi-agency contracts.

Major Provisions

Enactment of FASA revised existing procurement law in an effort to simplify the government's 55-year-old acquisition system that had become cumbersome and duplicative. New FASA requirements authorize the use of multiple award contracts for goods and services, thus minimizing the burden on contracting officials to negotiate and administer contracts. Encouraging a more active relationship between the federal government and suppliers, FASA authorizes procurement officials to buy goods quickly and economically through the simplified acquisition purchase threshold of $100,000, and through greater reliance on commercially available items. Micro-purchases, under $2,500, are authorized by FASA to be made with the use of purchase cards. Procurement officials are also encouraged to conduct bid requests, quote specifications, and award contracts electronically, whenever possible.

Generally, federal agencies acquire their goods and services through contracts that mandate specific requirements. An agency can now consider a contractor's past performance, management skills, and workmanship in its decision to award supply and services contracts based on best-value procurement, instead of lowest price. In addition, the use of fixed-price performance-based contracting is also encouraged to eliminate audits and cost overruns often associated with cost-reimbursement contracts.

Discussion

FASA contained 204 sections that amended procurement law, and established September 1995 as the deadline for final implementing regulations. Two years later, the General Accounting Office (GAO) reported that the actual implementation of FASA requirements was a "complex process," involving major revisions of the FAR, as well as individual agency directives and FAR

supplements.[976] The Federal Acquisition Regulatory Council, in conjunction with 11 interagency drafting groups, initially proposed 29 FAR revisions to implement the act. While only 13 regulations were published in final form by the FASA deadline, an additional 11 regulations were published the following month. GAO found that the FAR drafting groups emphasized crafting language that would be useful to contracting officers, and addressing public comments on the more complex or controversial regulations.[977]

In the decade following enactment of FASA, federal procurement officials have been able to emphasize performance-based requirements in proposed contracts, and to allow greater flexibility to potential vendors on the methods used to accomplish their work more effectively. Agency procurement officials have also been authorized to negotiate procurements with the use of time-and-materials contracts. In this type of contract, the vendor assumes the full burden of performing and completing the entire scope of work, within the contract's maximum not-to-exceed price for wages and materials. Title XIV of the FY2004 National Defense Authorization Act (P.L. 108-136), the Services Acquisition Reform Act of 2003 (described in more detail elsewhere in this compendium), amends FASA to provide that contracts may be used by federal agencies for the acquisition of commercial services. Agency procurement officials are required to make a determination that a time-and-materials contract is more appropriate than a traditional fixed-price contract, and include in the proposed contract a maximum, not-to-exceed price that the contractor exceeds at his own risk. Procurement officials also have the flexibility to authorize any subsequent change in the cost of the contract, if it is determined to be in the best interest of the procuring agency.

The significance of procurement in the federal government is reflected in the $234.9 billion that civilian and defense agencies spent on goods and services in FY2002. Growth in procurement spending is likely to continue as the President and Congress address homeland security and defense issues, as well as the need to acquire updated information and technology systems within the federal government.

Selected Source Reading

Congress. House. Committee on Government Reform and Oversight. Subcommittee on Government Management, Information, and Technology. Simplifying and Streamlining the Federal Procurement Process. Hearings. 104th Congress, 1st session. Washington: GPO, 1996.

---

[976] U.S. General Accounting Office, Acquisition Reform: Regulatory Implementation of the Federal Acquisition Streamlining Act of 1994, GAO/NSIAD-96-139, June 1996, p. 1.

[977] Ibid., pp. 2-3.

General Accounting Office. Acquisition Reform: Implementation of Title V of the Federal Acquisition Streamlining Act of 1994. GAO/NSIAD-97-22BR, October 1996.

——. Acquisition Reform: Regulatory Implementation of the Federal Acquisition Streamlining Act of 1994. GAO/NSIAD-96-139. June 1996.

Stephanie Smith

C. Federal Activities Inventory Reform (FAIR) Act of 1998

Statutory Intent and History

Office of Management and Budget (OMB) Circular No. A-76, which was first issued in 1966, provides guidance for federal agencies to use in determining who — a government agency or a private business — will perform commercial activities.[978] A commercial activity is defined as "a recurring service that could be performed by the private sector."[979] The circular does not require agencies in the executive branch to conduct cost comparison studies. The voluntary nature of the A-76 program is manifested by varying levels of participation by executive agencies.

Concerned that civilian executive agencies infrequently consulted Circular No. A-76,[980] and supportive of the federal government's stated policy of relying on the private sector for commercial activities,[981] the 105th Congress responded with new legislation. As introduced in the Senate, S. 314 would have required executive agencies to procure "from sources in the private sector all goods and services that are necessary for or beneficial to the accomplishment of authorized functions of the agency," except for inherently governmental goods and services.[982] The version of the bill passed by Congress and signed by the President differed substantially from the original bill. The Federal Activities Inventory Reform Act of 1998 (FAIR; P.L. 105-270)[983] requires agencies to compile and submit lists of their commercial activities to OMB, but does not require them to conduct cost comparison studies.

---

[978] The circular is available at [http://www.whitehouse.gov/omb/circulars/a076/a76_ incl_ tech_correction.pdf], visited Dec. 4, 2003.

[979] U.S. Office of Management and Budget, Circular A-76 (Revised), May 29, 2003, p. D-2.

[980] U.S. Congress, Senate Committee on Governmental Affairs, Federal Activities Inventory Reform Act of 1998, report to accompany S. 314, 105th Cong., 2nd sess., S.Rept. 105-269 (Washington: GPO, 1998), pp. 5-6, 11.

[981] In acknowledgment of the Administration's emphasis on public-private competition, the 2003 revision to the circular restated the policy: "The longstanding policy of the federal government has been to rely on the private sector for needed commercial services. To ensure that the American people receive maximum value for their tax dollars, commercial activities should be subject to the forces of competition" (U.S. Office of Management and Budget, Circular No. A-76 (Revised), p. 1).

[982] This version of S. 314, and all other versions, are available at the Legislative Information System website, [http://www.congress.gov], visited Dec. 18, 2003.

[983] 112 Stat. 2382, 31 U.S.C. § 501 note.

Major Provisions

This statute requires the compilation of lists of commercial activities performed by executive agencies, establishes an appeals process, and defines what is an inherently governmental function. FAIR requires executive agencies to compile an inventory of commercial activities and submit the list to OMB annually. After OMB review and consultation, the agency head sends a copy of the list to Congress and makes the list available to the public. Interested parties, such as a contractor or federal employee labor union, may appeal the omission or inclusion of certain activities. If appeals or challenges occur, they are handled by the agency. In lieu of defining commercial activity, the legislation defines inherently governmental function(s). An inherently governmental function is one "that is so intimately related to the public interest as to require performance by Federal Government employees." Because this definition is included in the FAIR Act, an inherently governmental function now is statutorily defined.[984]

Discussion

Agencies first compiled FAIR inventories and submitted them to OMB in 1999. Agencies identified approximately 850,000 full-time equivalents (FTEs)[985] as commercial on the 2000 inventories. Figures have changed only slightly since then.

Competitive sourcing is a component of the President's Management Agenda (PMA), and OMB has led the effort to promote competitive sourcing among federal agencies. The agency released a revision to Circular No. A-76 in May 2003 and has issued guidance on inventories and related competitive sourcing activities. The definition of inherently governmental included in the circular differs from the definition found in FAIR. It is unclear whether the differences possibly could lead to different results when agencies classify activities as inherently governmental. Since 2001, OMB has required agencies to submit inventories of their inherently governmental activities. The 2003 revision of Circular No. A-76 permits interested parties to challenge the classification of an activity as inherently governmental and the application of reason codes to commercial activities.[986] Neither type of inventory challenge is included in FAIR.

---

[984] Beginning with the 2003 revision of the circular, Circular No. A-76 includes criteria for an inherently governmental function (U.S. Office of Management and Budget, Circular No. A-76 (Revised), pp. A-2-A-3).

[985] A full-time equivalent represents the "staffing of Federal civilian employee positions, expressed in terms of annual productive work hours (1,776) rather than annual available hours that includes non-productive hours (2,080 hours)" (U.S. Office of Management and Budget, Circular No. A-76 (Revised), p. D-5).

[986] Reason codes apply only to commercial activities. Each function listed in a FAIR inventory is assigned a reason code, which indicates whether the function is eligible for public-private

Beginning in 2001, OMB issued competitive sourcing targets for agencies. For example, agencies were required to compete 5% of their commercial activities by the end of FY2002.[987] However, in July 2003, OMB abandoned government-wide targets in favor of goals tailored to each agency.[988]

Selected Source Reading

CRS Report RL32017. Circular A-76 Revision 2003: Selected Issues, by L. Elaine Halchin.

CRS Report RL31024. The Federal Activities Inventory Reform Act and Circular A-76, by L. Elaine Halchin.

CRS Report RL32079. Federal Contracting of Commercial Activities: Competitive Sourcing Targets, by L. Elaine Halchin.

Congress. House. Committee on Government Reform. Subcommittee on Government Management, Information, and Technology. The Implementation of the Federal Activities Inventory Reform Act. Hearing. 106th Congress, 2nd session, October 28, 1999. Washington: GPO, 2000.

Congress. Senate. Committee on Governmental Affairs. Federal Activities Inventory Reform Act of 1998. Report to accompany S. 314. 105th Congress, 2nd session. S.Rept. 105-269. Washington: GPO, 1998.

General Accounting Office. Competitive Contracting: Agencies Upheld Few Challenges and Appeals under the FAIR Act. GAO/GGD/NSIAD-00-244. September 2000.

General Accounting Office. Competitive Contracting: The Understandability of FAIR Act Inventories Was Limited. GAO/GGD-00-68. April 2000.

Office of Management and Budget. The Federal Activities Inventory Reform Act (FAIR), P.L. 105-270. Available at [http://www.whitehouse.gov/omb/procurement/fair-index.html], visited December 16, 2003. (This website includes

---

competition. OMB's 2003 inventory guidance is available at [http://www.whitehouse.gov/omb/memoranda/m03-09.html], visited Dec. 16, 2003.

[987] U.S. Office of Management and Budget, "Performance Goals and Management Initiatives for the FY2002 Budget," Memorandum M-01-15, Mar. 9, 2001, p. 1, available at [http://www.whitehouse.gov/omb/memoranda/2001.html], visited Dec. 15, 2003.

[988] U.S. Office of Management and Budget, Competitive Sourcing: Conducting Public-Private Competition in a Reasoned and Responsible Manner, July 2003, available at [http://www.whitehouse.gov/omb/procurement/comp_sourcing_072403.pdf], visited Dec. 15, 2003.

resources and guidance involving FAIR, and information on where to find agency inventories.)

L. Elaine Halchin

D. Services Acquisition Reform Act (SARA) of 2003

Statutory Intent and History

The Services Acquisition Reform Act of 2003 (SARA),[989] enacted as Title XIV of the National Defense Authorization Act for Fiscal Year 2004, joins two other major pieces of legislation enacted within the past 20 years aimed at reforming the federal government's procurement policies and processes — the Competition in Contracting Act of 1984 and the Federal Acquisition Streamlining Act of 1994 — which are discussed in this compendium.

Major Provisions

SARA focuses on the federal government's acquisition workforce; the use of business acquisition practices by the federal government; the procurement of commercial items; measures related to the American occupation of Iraq; and preparing for, or responding to, terrorist attacks.

A provision in SARA directs the Administrator of General Services to establish, and manage through the Federal Acquisition Institute, an acquisition workforce training fund. Five percent of the fees collected by federal agencies under certain contracts (e.g., government-wide contracts for the acquisition of information technology, popularly known as "GWACs") is to be credited to the training fund.

Among the business management practices instituted by SARA are the requirement for agency heads to appoint or designate chief acquisition officers (CAOs) and the creation of a chief acquisition officers council. This step follows the establishment of agency-level chief financial officers by the Chief Financial Officers Act of 1990,[990] and agency-level chief information officers by the Information Technology Reform Act of 1996 (National Defense Authorization Act for Fiscal Year 1996).[991] Other major provisions require the administrator of the Office of Federal Procurement Policy (OFPP), an official in the office of Management and Budget, to establish an advisory panel to review all acquisition laws and regulations, which is to report, no later than one year after its creation, on findings, conclusions, and recommendations; extend the authority for franchise funds from October 1, 2003, to December 31, 2004; and authorize telecommuting for employees of federal contractors.

---

[989] 117 Stat. 1663; P.L. 108-136; H.R. 1588. The initial version of the Services Acquisition Reform Act in the 108th Congress was a separate piece of legislation, H.R. 1837.

[990] 31 U.S.C. §§ 901-903; P.L. 101-576, §§ 205-207; 104 Stat. 2838.

[991] 40 U.S.C. § 1425; P.L. 104-106, Div. E, § 5125; 110 Stat. 186, at 679. This law was later renamed the Clinger-Cohen Act of 1996 by P.L. 104-208 (110 Stat. 3009-393).

With regard to the acquisition of commercial items, a provision in SARA permits federal agencies to treat the procurement of services under a performance-based contract as a procurement of commercial items. Certain conditions apply; for example, the value of the contract cannot exceed $25 million. This provision also allows agencies to use, under certain conditions, a time-and-materials contract or a labor-hour contract for the purchase of commercial services.

The final portion of SARA responds to circumstances in the aftermath of the September 11, 2001, terrorist attacks. The heads of civilian agencies may exercise the same authority, under the same conditions and limitations, that the Secretary of Defense has to enter into certain transactions (popularly referred to as "other transactions" because they do not involve, for example, contracts or grants) for research and development projects.[992] In civilian agencies, eligible projects are those related to helping defend against, or recover from, biological, nuclear, chemical, or radiological attack. Congressional interest in the use of other than full and open competition procedures by federal agencies awarding contracts for the reconstruction of Iraq led to a disclosure provision on these contracts. Information about noncompetitive contracts must be published in the Federal Register. For procurements in support of a contingency operation, or used to facilitate preparation for, or recovery from, nuclear, biological, chemical, radiological attack, the simplified acquisition threshold was increased; the threshold for simplified acquisition procedures was increased; and agencies may treat such items or services as commercial items.

Discussion

This statute represents an effort to continue streamlining federal procurement processes. As such, it is consistent with efforts over the past 20 years to enhance the efficiency of procurement activities while giving agency personnel greater flexibility in making procurements. However, some parties are concerned that greater flexibility could lead to problems. It is too early to tell how agency personnel will use procurement flexibilities, whether these statutory changes will enhance procurement of goods and services, and whether unintended consequences will occur.

Selected Source Reading

Congress. House. Committee on Government Reform. Better Training, Efficiency and Accountability: Services Acquisition Reform for the 21st Century. Hearing on H.R. 1837. 108th Congress, 1st session, April 30, 2003. Washington: GPO, 2003.

Office of Management and Budget. Office of Federal Procurement Policy.

[992] Authority for the Secretary of Defense to enter into other transactions is found in Sec. 845 of the National Defense Authorization Act for Fiscal Year 1994 (P.L. 103-160; 10 U.S.C. § 2371 note).

Emergency Procurement Flexibilities, A Framework for Responsive Contracting and Guidelines for Using Simplified Acquisition Procedures, May 2003. Available at [http://www.whitehouse.gov/omb/procurement/emergency_procurement_flexibilities.pdf], visited December 16, 2003.

L. Elaine Halchin

E. Competition in Contracting Act

Statutory Intent and History

The last full-scale statutory changes made to the competitive contracting procedures concerning federal procurement occurred in 1984. The Competition in Contracting Act of 1984 (CICA or the Competition Act; 98 Stat. 1175; 41 U.S.C. § 251 et seq.), enacted as Title VII of the Deficit Reduction Act of 1984 (98 Stat. 494), made broad changes in the two major procurement statutes that had served as basic authority for federal government purchases of supplies and services since the late 1940s. Specifically, CICA changed the Federal Property and Administrative Services Act (40 U.S.C. § 475 et seq.), the major civilian agency procurement statute, and the Armed Services Procurement Act (10 U.S.C.§ 2301 et seq.), the major military procurement statute. Additional statutory provisions to increase competition were included in the Small Business and Federal Procurement Competition Enhancement Act of 1984 (41 U.S.C. § 251 note), which is applicable to civilian agencies, and the Defense Procurement Reform Act of 1984 (98 Stat. 2588), which is applicable to the Defense Department.

Major Provisions

Before CICA, the procedures involving federal contracting were based on "formal advertising" or "competitive negotiation." After passage of CICA, competitive procedures became defined as "procedures under which an executive agency enters into a contract pursuant to full and open competition."[993] The Office of Federal Procurement Policy Act states that "full and open competition means that all responsible sources are permitted to submit sealed bids or competitive proposals."[994] The two most important competitive procedures set forth in CICA are sealed bids, corresponding to the former competitive procedure of formal advertising, and competitive proposals,[995] corresponding to the former competitive procedure of negotiation. CICA also states that "competitive procedures means procedures under which an executive agency enters into a contract pursuant to full and open competition" and defines what the term includes.[996]

When selecting a competitive procedure, the major question concerns whether to use sealed bids or competitive proposals. Before CICA, all contracts over $10,000 required formal advertising unless one of the exemptions allowed negotiation and advertising was not feasible and practicable. Under CICA,

---

[993] 41 U.S.C. § 259(b) and 10 U.S.C. § 2302(2).

[994] 41 U.S.C. § 403(6).

[995] 41 U.S.C. § 253(a)(2)(B) and 10 U.S.C. § 2304(a)(2)(B).

[996] 41 U.S.C. § 259(b) and 10 U.S.C. § 2302(2).

however, an executive agency which is conducting a procurement for property or services is required to "use the competitive procedure or combination of competitive procedures that is best suited under the circumstances of the procurement."[997]

"Procedures other than competitive," known as "sole-source" or "limited competition," depending upon the circumstances, may be used only if meeting one of the enumerated seven exceptions. These exceptions are as follow: (1) when "the property or services needed by the executive agency are available from only one responsible source and no other type of property or services will satisfy the needs of the executive agency"; (2) when "the executive agency's need for the property or services is of such an unusual and compelling urgency that the government would be seriously injured unless the executive agency is permitted to limit the number of sources from which it solicits bids or proposals"; (3) when "it is necessary to award the contract to a particular source or sources in order (A) to maintain a facility, producer, manufacturer, or other supplier available for furnishing property or services in case of a national emergency or to achieve industrial mobilization, or (B) to establish or maintain an essential engineering, research, or development capability to be provided by an educational or other nonprofit institution or a federally funded research and development center"; (4) when "the terms of an international agreement or treaty between the United States Government and a foreign government or international organization, or the written directions of a foreign government reimbursing the executive agency for the cost of the procurement of the property or services for such government have the effect of requiring the use of procedures other than competitive procedures";[998] (5) when "a statute expressly authorizes or requires that the procurement be made through another executive agency or from a specified source, or the agency's need is for a brand-name commercial item for authorized resale"; (6) when "the disclosure of the executive agency's needs would compromise the national security unless the agency is permitted to limit the number of sources from which it solicits bids or proposals"; and (7) when "the head of the executive agency — (A) determines that it is necessary in the public interest to use procedures other than competitive procedures in the particular procurement concerned, and (B) notifies the Congress in writing of such determination not less than 30 days before the award of the contract."

Discussion

Since passage of the Competition in Contracting Act, Congress has continued to examine the procurement process. Perhaps the most significant changes since

---

[997] 41 U.S.C. § 253(a)(1)(B) and 10 U.S.C. § 2304(a)(1)(B). All remaining quotations are from 41 U.S.C. § 235 et seq. and 10 U.S.C. § 2304 et seq.).

[998] 41 U.S.C. § 253(c)(4) and 10 U.S.C. § 2304(c)(4).

1984 occurred in the Federal Acquisition Reform Act of 1996.[999] Although the provisions are not a full-scale revamping of the procurement requirements, the changes are significant. The general effect of the act is to eliminate or to simplify certain of the contracting procedures. It is likely that Congress will continue to examine whether additional changes to the procurement laws are warranted.

Selected Source Reading

U.S. Congress. House. Conference Report No. 104-450. 104th Congress, 2nd session. Washington: GPO, 1996.

——. House. Conference Report No. 98-861. 98th Congress, 2nd session. Washington: GPO, 1996.

——. House. Committee on Ways and Means. Report No. 98-432. 98th Congress, 2nd session. Washington: GPO, 1983 and 1984.

Michael Seitzinger

[999] Division D of the 1996 Defense Authorization Act, P.L. 104-106 (110 Stat. 642).

F. Federal Contract Labor Standards Statutes

Statutory Intent and History

Through the early decades of the 20th century, federal procurement law required the government to accept the lowest responsible bid for federal contract work. Since contracts normally specified the type, style, and quality of the construction or goods to be purchased, economies were often achieved through reduced labor costs as firms engaged in competitive bidding. The result, many policymakers believed, was a system that undercut the local market to the disadvantage of contractors and workers alike. It was argued that the system also disadvantaged the government. Low-wage workers often lacked first-rate skills and allegedly produced substandard work which resulted in increased cost to the taxpayer over the long term. And, it made government, at least indirectly, a party to adverse (and often sweatshop) working conditions.

After several tentative proposals during the late 1920s, Congress adopted the Davis-Bacon Act (40 U.S.C. §§ 3141-3148) in 1931. Enacted at the urging of the Hoover Administration, in part as an effort to bring stability to the construction industry and to cope with the collapsing national economy, the act required that persons employed on federal contract work must be paid not less than the locally prevailing wage for comparable work in the locality of the project. In 1935, the scope of the act was broadened to include both public buildings and public works, together with painting and decorating. In 1964, Congress expanded the concept of prevailing wage to include the value of fringe benefits (other than those mandated by law) paid to workers employed in comparable work in the locality. Through the years, Davis-Bacon provisions have been added to more than 50 federal program statutes.

In 1936, following roughly the pattern set by the Davis-Bacon Act, Congress adopted the Walsh-Healey Act (41 U.S.C. §§ 35-45), which set basic standards with respect to goods produced under contract for the federal government. Nearly three decades later, in 1965, Congress adopted the McNamara-O'Hara (Service Contract) Act (41 U.S.C. §§ 351-358), similarly setting basic labor standards for services provided, under contract, to the federal government. These three primary federal contract labor standards statutes are supplemented, inter alia, by the Fair Labor Standards Act of 1938 (FLSA, 29 U.S.C. §§ 201-219), the Contract Work Hours and Safety Standards Act of 1969 (40 U.S.C. §§ 327-333), and the Occupational Safety and Health Act of 1970 (29 U.S.C. §§ 651-678), among others.

Major Provisions

The three statutes deal only with federal contract procurement: respectively, construction (Davis-Bacon), goods (Walsh-Healey), and services (McNamaraO'Hara). Although similar in purpose, they differ in certain details. For Davis-Bacon, the coverage threshold is $2,000; for Walsh-Healey, $10,000; and for McNamara-O'Hara, $2,500. For Davis-Bacon and McNamara-O'Hara,

the basic wage rate is that prevailing for the same type of work in the locality. For Walsh-Healey, the wage floor is, in practice, the minimum wage under the FLSA. Work under each of the contract labor standards statutes is subject to the overtime pay requirements of the FLSA (or reflects a comparable standard): that is, 1½ times a worker's regular rate of pay for hours worked in excess of 40 per week. Child labor is restricted under Walsh-Healey — but also restricted in many forms under the more comprehensive FLSA. Through not addressed in Davis-Bacon, industrial homework is restricted under Walsh-Healey, McNamara-O'Hara and the FLSA — as is convict labor under Walsh-Healey. For Davis-Bacon and McNamara-O'Hara, wage rate calculations are locality based. For Walsh-Healey, in practice, they are the same national rates as those of the FLSA.

Discussion

Of the contract labor standards statutes, the Davis-Bacon Act has been the most visible — and the most controversial. Some view the act as a vital protection for contractors, workers and the public alike — as important now as when it was originally enacted. They assert that the act ensures fairness and equity for workers, that it encourages higher standards in construction, saving the government money in the long run, and that it encourages the training of construction industry professionals through recognized apprenticeship programs. Others argue that the act inflates the cost of public construction, that it is difficult and cumbersome to enforce and perhaps impossible equitably to enforce, and that its complexity works to the disadvantage of small contractors. The Davis-Bacon literature appears to be inconclusive with respect to the act's impact.

Concerning the McNamara-O'Hara Act, proponents hold that it protects workers from what would otherwise be a cycle of wage/benefit reductions as one service provider after another sought government contracts based upon the lowest possible labor costs. It also provides stability for industry and for government (as a consumer), it is argued, preventing a revolving movement of contractors as an award is made first to a low bidder and then to a still lower bidder — each competing upon the basis of ever lower wages and, often, with nonunion labor. Conversely, critics argue that the market, unrestrained, would produce a less expensive service bill for government. The statute is, they argue, difficult to administer, cumbersome, and needlessly inflates wages above market levels. The Walsh-Healey Act, perhaps because its standards are largely the same as those of the national FLSA, has been, at least through recent decades, less subject to controversy.

Historically, each of these statutes was adopted as a means of dealing with specific abuses that had arisen in the workplace and in federal procurement. There is nothing to suggest, some argue, that these abuses would not reappear were the statutes substantially modified or repealed. Conversely, others question whether, at a minimum, some consolidation of the federal contract labor standards statutes and the more general FLSA might not be appropriate.

Selected Source Reading

CRS Report RL32086. Federal Contract Labor Standards Statutes: An Overview, by William G. Whittaker.

CRS Report 94-408. The Davis-Bacon Act: Institutional Evolution and Public Policy, by William G. Whittaker.

CRS-225 CRS Report 94-908. Davis-Bacon: The Act and the Literature, by William G. Whittaker. William Whittaker

G. Prompt Payment Act

Statutory Intent and History

The Prompt Payment Act (PPA) was originally enacted in 1982 (96 Stat. 85; 31 U.S.C. § 3901) in response to what was perceived as a pervasive problem of federal agencies not paying their bills on time.[1000] While this act did lead to improvement in the timeliness of government bill paying, the 100th Congress saw the need for amendment, revision, and general tightening up of the PPA to bring about more uniform compliance with its purposes. Congress responded by enacting the PPA amendments of 1988 (102 Stat. 2455). The basic structure of the PPA is relatively simple and straightforward. If a bill is not paid on time, interest must be paid on the delinquency. The funds for the interest must come from funds already appropriated for the program which has incurred the interest.

Major Provisions

The PPA applies to all types of federal contracts, including leases (31 U.S.C. § 3901(a)(6)) for the procurement of property or services by agencies covered by the act (OMB Circular No. A-125, § 2(a); see also: 48 C.F.R. § 32.901). Agency is defined to include each authority of the government of the United States, whether or not it is within or subject to review by another agency, but it does not include Congress, the United States courts, governments of territories or possessions, the government of the District of Columbia, courts martial, military commissions, and military authority exercised in the field in time of war or in occupied territory (31 U.S.C. § 3901(a)(1) which incorporates by reference 5 U.S.C. § 551(1)). Agency also includes any entity that is operated exclusively as an instrumentality of such an agency for the purpose of administering one or more programs of that agency, and that is so identified for this purpose by the head of such agency (OMB Cir. A-125, § 1(b)). The PPA specifically applies to the Tennessee Valley Authority and the United States Postal Service.[1001] The head of an agency acquiring property or service from a business concern, who does not pay the concern for such complete delivered item of property or service by the required payment date, shall pay an interest penalty to the concern on the amount of the payment due. The interest rate to be used is the interest rate established by the Secretary of the Treasury under the Contracts Disputes Act (41 U.S.C. § 611), which is in effect when the obligation to pay PPA interest arises (31 U.S.C. § 3902(d)). The temporary unavailability of funds to make timely payment does

---

[1000] U.S. Congress, House, H.Rept. 97-461, 97th Cong., 2nd sess. (Washington: GPO, 1982). See also U.S. General Accounting Office, "The Federal Government's Bill Paying Performance Is Good but Should Be Better," FGMSD-78-16, 1978, in which GAO found that 30% of the federal government's bills, covering 18% of the dollar total, were paid late.

[1001] 31 U.S.C. § 3901(b) and (c). The United States Postal Service was not included under the 1982 PPA. Coverage was added by the 1988 amendment, P.L. 100-496, § 2(c)(1), and is applicable to all obligations incurred on or after Jan. 1, 1989.

not relieve the agency of the obligation to pay such penalty (31 U.S.C. § 3902(d)). The PPA interest penalty is to be paid automatically, whether or not it has been requested by the contractor. Failure to pay such interest may result in an additional penalty. This additional penalty is equal to 100% of the original penalty and is limited to $5,000, but cannot be less than $25. These limitations apply to each invoice (OMB Circular No. A-125, § 8(b) and (c)). In the case of construction contracts, the regulations shall provide for the payment of interest on late progress payments and retainages (31 U.S.C. § 3903(a)(6)(A)).[1002] The regulations are also required to include provision for prompt review of invoices submitted to agencies. Agencies are to have seven days to return invoices found to be not proper.[1003]

Every construction contract awarded by an agency must include a clause which requires the contractor to include two clauses, a payment clause and an interest penalty clause, in each of its subcontracts. The payment clause must specify that the prime contractor is obligated to pay the subcontractor for satisfactory performance under its subcontract out of payments received from the agency, within seven days of such receipt. The interest penalty clause is to require that the contractor will pay an interest penalty, computed at the same rate as applied to the government under the PPA, to the subcontractor if the seven day deadline is not met (31 U.S.C. § 3905(b)). These protections are extended to all tiers of subcontractors by requiring the prime contractor to require all subcontractors to include these same two clauses in their sub-subcontracts (31 U.S.C. § 3905(c)). A contractor's obligation to pay an interest penalty to a subcontractor under any of these required clauses may not be passed along to the federal government by any means, including contract modifications or cost reimbursement claims (31 U.S.C. § 3905(k)).

Discussion

The PPA greatly reduced the problem of federal agencies not paying their bills in a timely fashion. While the problem has not been entirely eradicated, the PPA has not generally been the subject of proposed legislation since its amendment in 1988.

Selected Source Reading

Donnaly, Robert A. and Mark W. Stone. "The Prompt Payment Act in 1987:

[1002] A period longer than 14 days may be included in the solicitation only if required to afford the agency a practicable opportunity to inspect the work adequately and to determine the adequacy of the contractor's performance under the contract (see A-125, § 10(a)(1)).

[1003] The limit is shorter for meat and meat product contracts (three days), and for perishable agricultural commodities (dairy products, edible fats or oils, and food products prepared from edible fats or oils, five days) (A-125, § 7(a)(7)).

Collecting from Uncle Sam." National Contract Management Journal, vol. 21 (1987), pp. 45-55.

Renner, Michael J. "Prompt Payment Act: An Interesting Remedy for Government Late Payment." Public Contract Law Journal, vol. 21 (1992), pp. 177-278.

John R. Luckey

VI. Intergovernmental Relations Management

A. Intergovernmental Cooperation Act

Statutory Intent and History

Congress approved the Intergovernmental Cooperation Act of 1968 (ICA)[1004] to improve administrative relationships among federal, state, and local governments, particularly with regard to the grant-in-aid system. The legislation, as enacted, was a composite of government reform proposals that had been considered over a number of years. Recommendations from a variety of organizations, including the Kestnbaum Commission of 1955, the Advisory Commission on Intergovernmental Relations (ACIR),[1005] as well as public interest groups representative of state and local governments, were incorporated in the legislation.

Proponents argued for the legislation out of concern with the duplication of effort and lack of coordination in the federal domestic assistance system, in part because of the rapid expansion of categorical grant-in-aid programs in the 1960s.[1006] While few, if any, spoke against the intent of the legislation, some debate occurred over the proposed inclusion of a uniform relocation assistance provision in the legislation (the language was ultimately deleted from the bill) and the proposed "sunset" language (also ultimately not included).[1007]

Major Provisions

As originally enacted, the Intergovernmental Cooperation Act consisted of six titles. Title I set out definitions. Title II established administrative requirements for grants-in-aid, and Title III authorized federal agency heads to provide technical assistance to state or local governments. Title IV required that the President issue program regulations to help state and local governments attain urban and rural community development objectives regarding land use, transportation systems, environmental protection, and other related areas. Also,

---

[1004] P.L. 90-577, 82 Stat. 1098, et seq.

[1005] The Advisory Commission on Intergovernmental Relations (ACIR) was established by Congress in 1959 (5 U.S.C. § 2372) for continuing study of the American federal system. The commission ceased operations when Congress no longer appropriated funds after FY1996.

[1006] Categorical grants provide aid for specified activities and generally require adherence to rigorous guidelines and regulations.

[1007] Sunset provisions specify that program authority must terminate by a date certain. Advocates of sunset provisions argued that the inclusion of such language in legislation would ensure that committees of jurisdiction would conduct oversight hearings on programs and evaluate their usefulness on a regular basis. Instead of sunset language, Congress required quadrennial review by committees of jurisdiction of program administration and implementation.

Title IV required that federal aid be consistent "to the maximum extent possible" with non-federal comprehensive planning, and that units of general local government be favored to received federal aid over special purpose governments. Title V amended the Federal Property and Administrative Services Act[1008] to ensure that federal acquisition, use, or disposal of land in urban areas did not conflict with local zoning, land use, and planning practices. Finally, Title VI required that congressional committees with jurisdiction evaluate programs not scheduled to terminate every four years. Also, Title VI required that the Comptroller General and the ACIR conduct studies of grant-in-aid programs.

The ICA has been amended several times, most notably in 1982, when it was recodified.[1009] In its current form, the act sets out definitions[1010] and enables state officials to obtain information on the purpose and amount of grants received in the states.[1011] Concerning fund transfers and associated requirements, the act requires that federal officials make funds available to the states in an expedited fashion; establishes requirements concerning interest payments received on deposited federal funds; and requires state officials to make reports on the funds.[1012] Provisions have been retained from the original statute that authorize federal agency heads to waive statutory requirements concerning designation of a single state contact[1013] and to make specialized or technical services available to state and local governments.[1014] Also, the provisions of Title IV that require coordination between federal expenditures and state and local community development objectives remain in force,[1015] as do those concerning quadrennial congressional committee review.[1016]

Discussion

[1008] 63 Stat. 377; 40 U.S.C. § 475 et seq.

[1009] In 1982, the ICA was technically repealed, reenacted, and recodified at 31 U.S.C. § 6501 et seq. (see P.L. 97-258, 96 Stat. 1005-1010). Previously, it had been codified at 42 U.S.C. § 4201-4243.

[1010] 31 U.S.C. § 6501.

[1011] 31 U.S.C. § 6502.

[1012] 31 U.S.C. § 6503.

[1013] 31 U.S.C. § 6504.

[1014] 31 U.S.C. § 6505.

[1015] 31 U.S.C. § 6506. E.O. 12372, signed by President Reagan July 14, 1982, and amended by E.O. 12416 on April 8, 1983, allowed states to design their own procedures for reviewing federal financial assistance and directing federal development.

[1016] 31 U.S.C. § 6507.

Intergovernmental relations have undergone considerable change in recent years. Some of these changes resulted from actions required by the ICA. For example, the authority of federal agency heads to waive federal requirements concerning a single state contact, at the request of state officials, first appeared in the ICA. In recent years, such waivers have been used in a number of policy areas to improve intergovernmental relations as well as the administration of federal grant-in-aid funding. Another significant effect of the ICA was the assignment of increased responsibilities to the Office of Management and Budget (OMB). Implementation of the ICA was included in OMB's Federal Assistance Review efforts during the Nixon Administration.

During the Reagan Administration, officials sought to modify past patterns of federal involvement in domestic assistance programs. Although provisions of the ICA were modified, the act was not repealed. At present, though most provisions of the 1968 act remain in effect, they are largely dormant.

Selected Source Reading

U.S. Congress. Senate. Committee on Governmental Affairs. Office of Management and Budget: Evolving Roles and Future Issues. Committee print. 99th Congress, 2nd session. Washington: GPO, 1986, pp. 335-358.

Keith Bea

B. Intergovernmental Personnel Act of 1970

Statutory Intent and History

The Intergovernmental Personnel Act of 1970 (IPA)[1017] authorized programs to improve state and local government personnel management operations and procedures. Congress approved the IPA at the urging of federal managers, Members of Congress, and others who voiced concern over a perceived need to strengthen the core management capabilities of state and local general purpose governments. In the late 1960s, when Congress first debated the legislation, federal agencies were expanding to meet new federal policy objectives, and agency heads were competing with state and local governments to attract employees at upper management levels. Congress viewed enactment of the IPA has a means of improving the pool of public management candidates in the nation.

Two types of management needs figured in the enactment of the IPA:[1018]
Policy Management — identification of needs, analysis of options, and selection of programs throughout non-federal units of government.

Resource Management — establishment of basic administrative support systems such as budgeting, financial management, procurement and supply, and personnel administration.

Major Provisions

The congressional declaration of findings and policy in the act notes that the effective management of federal funds by state and local governments is in the national interest. The IPA identified state and local manpower issues that required attention and additional resources. The issues include the interchange and retention of government employees, training, quality of public service, merit system requirements, and personnel management. Sponsors of the act sought to address these issues by authorizing the following types of assistance:

- grants-in-aid to help states and localities meet the costs of strengthening such personnel management activities as recruitment, selection, pay administration, training and employee development, and labor-management relations;
- invitations to state and local government employees to participate in federal training courses;

[1017] P.L. 91-648, 84 Stat. 1909, et seq.

[1018] U.S. Executive Office of the President, Strengthening Public Management in the Intergovernmental System (Washington: GPO, 1975), p. vii.

- technical assistance in personnel management on a reimbursable, non-reimbursable, or partly reimbursable basis;
- cooperative recruiting efforts;
- temporary exchange of personnel between different levels of governments and institutions of higher education (the "mobility program"); and
- transfer of responsibility for prescribing and maintaining merit system standards required under various federal assistance programs to a single agency.

The mobility program and the merit systems administration program were amended by Section 602 of the Civil Service Reform Act of 1978 (92 Stat. 11881189). In 1996, the 104th Congress approved technical amendments to the provision authorizing reimbursement for employees and families in transit (110 Stat. 2758). Since 1996, Congress has taken no further action on the IPA.

Discussion

The statutory authority for IPA remains on the books. Most of the IPA programs, however, have not been implemented for years. Funding for the grant program ended in FY1981. Currently, the only IPA program in existence is the Intergovernmental Mobility Program, discussed below.[1019]

Congressional approval of the IPA was based on three assumptions: effective state and local governments are essential in the federal system of governance; a national interest in state and local management practices exists, since federal funds are involved; and public service at all levels of governance can be improved through better personnel administration.[1020] These assumptions remained unchallenged until 1981, when the Reagan Administration proposed termination of the grant program and all the act's other provisions, except for its merit system principles, declarations of policy concerning public service, and provisions on interstate compacts.[1021] To support this proposal, the Administration contended that the IPA had achieved its objectives as a demonstration program and could be eliminated. The proposed abolition of much of the IPA statutory authority paralleled other Reagan Administration efforts to reduce federal involvement in "what should be primarily a state and local government responsibility."[1022]

[1019] The mobility program is codified at 5 U.S.C. §§ 3371-3376.

[1020] U.S. Advisory Council on Intergovernmental Personnel Policy, More Effective Public Service (Washington: GPO, 1973), p. 1.

[1021] U.S.Congress, Senate Committee on Governmental Affairs, Amending the Intergovernmental Personnel Act of 1970, hearings, 97th Cong., 1st sess. (Washington: GPO, 1981), p. 136.

[1022] Donald J. Devine, Letter Transmitting Legislation to Abolish the Intergovernmental Personnel Act, Congressional Record, daily edition, vol. 127, Apr. 29, 1981, p. S 4141.

The administration proposal came at a time when many domestic assistance programs were being cut or eliminated. General management assistance usually does not have a large or effective constituency, and federal programs with such a focus were largely repealed or allowed to lapse during this period. In FY1981, the IPA grant assistance program was terminated.[1023] In November 1981, the Office of Intergovernmental Personnel Programs in OPM, which had administered the programs, was abolished. The merit system provisions, which had been administered by this office, no longer received budgetary support from OPM, thus bringing the IPA grant assistance program to an end.

As noted above, the Intergovernmental Mobility Program is the only statutory provision that continues to be implemented, largely to facilitate temporary details of scientific and technical staff. The program allows federal, state, and local government employees to be voluntarily assigned to a public agency or to an organization oriented toward public service for no more than two years. Federal employees may be assigned to state, local, or tribal agencies, public or private institutions of higher education, or nonprofit or professional government associations. The reverse holds as well: employees of these entities may volunteer to be temporarily assigned to federal agencies. Through such assignments, scarce or technical expertise may be shared; program operational experience may be gained, or the management of federal grant programs improved. Assignments generally cannot exceed two years, although extensions might be approved. Assignment costs, including the salary of the employee, may be shared by the agencies or borne entirely by one entity, subject to agreement between the organizations. Since 1981, the IPA authority and the mobility program have been given little attention or publicity.

Selected Source Reading

Congress. House Committee on Post Office and Civil Service. Subcommittee on Human Resources. Intergovernmental Personnel Act Mobility Program. Hearings. 101st Congress, 1st session. Washington: GPO, 1989.

General Accounting Office. An Evaluation of the Intergovernmental Personnel Act of 1970. FPCD-80-11. December 19, 1979.

——. Intergovernmental Personnel Act of 1970: Intergovernmental Purpose no Longer Emphasized. GAO/GGD-89 — 95. June 19, 1989.

Keith Bea

[1023] U.S. Office of Management and Budget, Budget of the United States Government, Fiscal Year 1983 (Washington: GPO, 1982), p. I-V127.

C. Unfunded Mandates Reform Act of 1995

Statutory Intent and History

After considerable debate and some legislative action in the 103rd Congress, the Unfunded Mandates Reform Act (P.L. 104-4; 109 Stat. 48-71; 2 U.S.C. §§ 15011571) was enacted early in the 104th Congress. Generally, unfunded intergovernmental mandates include responsibilities or duties that federal programs, standards, or requirements impose on governments at other levels without providing for the payment of the costs of carrying out these responsibilities or duties. The intent of the mandate legislation was to limit the ability of the federal government to impose costs on state and local governments through unfunded mandates.

Legislation to restrain unfunded mandates was proposed regularly from 1984 through 1990 (98th-101st Congresses), but none of the proposals received action. During the 102nd and 103rd Congresses (1991-1994), increased pressure developed as state and local interest groups united in an effort to bring about mandate reform. Although some of this effort was concentrated on specific laws considered to impose mandates (e.g., safe drinking water, motorcycle helmet requirements, national education standards), much attention focused on overall unfunded mandate reform legislation. The Clinton Administration supported the concept of mandate reform, though not necessarily the specifics of all reform legislation.

Thirty-four mandate reform bills were introduced in the 103rd Congress, and a bipartisan compromise bill (S. 993/H.R. 5128) came close to floor action. Unfunded mandate reform was a component of the House Republican "Contract with America" in the 1994 election, and election of a Republican majority in both houses ensured early action in the 104th Congress. Mandate reform legislation was introduced as S. 1 and H.R 5 on January 4, 1995, and the Unfunded Mandates Reform Act was signed into law on March 22, 1995.

Major Provisions

The Unfunded Mandates Reform Act has three components: revised congressional procedures regarding future mandates; new requirements for federal agency regulatory actions; and authorization for a study of existing mandates to evaluate their current usefulness. The primary objective was to create procedures that would retard and spotlight, if not stop, congressional authorization of new unfunded mandates on state and local governments.

Point of Order in Congress. The act amended Title IV of the Congressional Budget and Impoundment Control Act of 1974 (P.L. 93-344; 88 Stat. 297-339), as amended, to require the Congressional Budget Office (CBO) to estimate the costs to state, local, and tribal governments and the private sector of the unfunded intergovernmental mandates established by each reported bill exceeding $58 million (in calendar year 2002, the latest year available; the threshold is adjusted

for inflation). The act requires that the cost information be printed and available before a vote is taken. If the information is not available, or if the bill does not provide that all mandates it establishes will be funded, a point of order may be raised against considering the bill. For this purpose, a mandate is considered unfunded unless the bill establishes a mechanism to ensure that, if in any year funding is not provided, the mandate will be reviewed or abolished. An affirmative vote by a majority of those present is necessary to override the point of order.

These requirements do not apply to provisions that are a condition of federal assistance or a duty arising from voluntary participation in a federal program (except that certain large entitlement programs are subject to the special procedures). Other provisions exempt from the requirements are:

- provisions affecting constitutional rights of individuals;
- statutory rights that prohibit discrimination;
- accounting and auditing requirements attached to federal assistance; and
- emergency assistance, national security, and emergency legislation.

Federal Agency Regulations. The second component affects federal agencies. The act requires agencies to develop a process through which state, local, and tribal governments and the private sector can participate in the development of regulations. In addition, agencies must identify the federal law that authorizes the regulation; estimate the costs and benefits, including whether federal assistance is available to pay the costs; and describe consultation with state, local, or tribal officials. Finally, the agencies must establish plans to involve local governments in the development of regulations affecting them, as well as pilot programs on local government flexibility.

Study of Existing Mandates. While the first two components of the act address proposed new mandates, the third relates to those that existed before its enactment. The act required the Advisory Commission on Intergovernmental Relations (ACIR) to study a number of things, including existing unfunded mandates. ACIR was directed to make recommendations reflecting flexibility in compliance; reconciling conflicting mandates; terminating duplicative, obsolete, or impractical mandates; suspending certain mandates not vital to public health and safety; consolidating and simplifying reporting and planning requirements; and establishing common federal definitions and standards.

Discussion

Origins. The term unfunded federal mandates refers to a host of flaws in the operation of the federal system perceived by some observers from the late 1970s into the 1990s. It summarized the concerns of those who asserted that there was excessive federal intrusion into state and local affairs, too much regulation, too many direct orders, too little respect for the role of state and local governments, and too little control by states and localities of their own affairs. Federal demands

on state and local resources were sometimes established as conditions of federal aid, but increasingly took the form of direct requirements, although no federal funds were made available to help carry out these directives. All of this came at a time when federal funds to state and local governments were being cut back.

The Unfunded Mandates Reform Act represented a response to a coordinated campaign by state and local officials and their supporters who had protested for years against these perceived federal demands at a time when federal assistance was diminishing. The exact magnitude of the costs to state and local governments of complying with federal mandates is not clear. Various estimates were made during debate on the legislation, ranging from a high of $500 billion to a low of $8.9 billion.

Use of Congressional Procedures. To some extent, the focus on unfunded mandates diminished after the legislation was enacted. Many of the individual grievances and criticisms that had fueled the mandate issue were separately addressed by the 104th Congress, which enacted the Unfunded Mandates Reform Act. Many Members of the new majorities had been elected with an agenda paralleling that of the mandate opponents; consequently, a number of issues were addressed directly and, in some cases, favorably. For example, the National Highway System Designation Act of 1995 (P.L. 104-59; 109 Stat. 568-634) repealed several items that regularly appeared on mandate reform agendas, including the national speed limit, the requirement that motorcyclists wear helmets, and requirements that crumb rubber be used in highway construction.

Since the point-of-order procedures took effect, the record on their usefulness as an anti-mandate tool could be described as mixed. On the one hand, state and local organizations used the process successfully to promote or secure changes in telecommunications legislation mandates, but on the other, the new procedures were not successful in preventing enactment of immigration legislation containing a number of provisions described as unfunded mandates. From 1996 through 2003, 13 points of order under the Unfunded Mandates Reform Act were raised in the House, and none in the Senate. The first time the procedure was invoked, the House voted against considering a proposal to amend a bill to include an increase in the minimum wage. Otherwise, the House has always voted to consider the measures against which the points of order were raised, dealing with the minimum wage as well as bankruptcy, nuclear waste, internet taxation, prescription drugs, and several welfare issues.

Advisory Commission Report. In January 1996, ACIR released a preliminary version of the report on federal mandates directed by the act. After considerable opposition was expressed to these preliminary findings, a revised report was presented to the commission for final action. This final version of the report included recommendations for modifying each of 13 mandates studied in detail and six recommendations common to all mandates. On July 23, 1996, a majority of the ACIR rejected these revised recommendations on the grounds that they

proposed too great a reduction in the federal role. Congress terminated funding for the ACIR in FY1996.

Private Sector Mandates. As attention to federal intergovernmental mandates grew in the 1980s and 1990s, supporters of regulatory reform began to assert a parallel between these mandates and federal laws regulating the private sector, on grounds that such laws also impose enforceable duties that entail costs of compliance. As a result, the Unfunded Mandates Reform Act includes a requirement that CBO provide information on the costs of these private sector mandates in proposed legislation, where the costs exceed $116 million (adjusted for inflation in calendar year 2002). The act does not, however, extend the points of order against consideration to private sector mandates. Subsequently, in both the 105th and 106th Congresses, legislation to apply to private sector mandates procedural protections similar to those now in effect for unfunded intergovernmental mandates passed the House, but it received only committee consideration in the Senate. In some versions, this Mandates Information Act would have established points of order against consideration of all private sector mandates, whether funded or not, including taxes.

Selected Source Reading

Ray, Maracella Ridlen and Timothy J. Conlan. "At What Price: Costs of Federal Mandates Since the 1980s." State and Local Government Review, vol. 28 (winter 1996), pp. 7-16.

Advisory Commission on Intergovernmental Relations. The Role of Federal Mandates in Intergovernmental Relations: A Preliminary ACIR Report for Public Review and Comment. Washington: GPO, 1996.

Congressional Budget Office. A Review of CBO's Activities in 2002 Under the Unfunded Mandates Reform Act. Washington: GPO, 2003.

Congress. House Committee on Government Reform, Subcommittee on Energy Policy, Natural Resources and Regulatory Affairs, and House Committee on Rules, Subcommittee on Technology and the House. Unfunded Mandates — A Five-Year Review and Recommendations for Change. Joint Hearing. 107th Congress, 1st session. Serial No. 107-19. Washington: GPO, 2001.

Keith Bea
Richard S. Beth

D. Single Audit Act

Statutory Intent and History

The Single Audit Act of 1984 (98 Stat. 2327; 31 U.S.C. §§ 7501-7507) established uniform audit requirements for state and local governments receiving federal financial assistance. It generally requires entity-wide audits instead of the previous program-by-program audits that had been criticized as an inefficient use of audit resources and an ineffective means of assuring accountability for federal funds.

The Single Audit Act Amendments of 1996 (110 Stat. 1391) extended the act's coverage to nonprofit agencies.[1024] The amendments also raised the thresholds that require compliance under the act, focused audits on riskier programs, improved audit reporting, and allowed more administrative flexibility. The only other amendments have been technical in nature (108 Stat. 1363 and 111 Stat. 2634).

As amended, the Single Audit Act has five purposes:

- to promote sound financial management (including effective internal controls) with respect to federal awards administered by non-federal entities;
- to establish uniform requirements for audits of federal awards administered by these entities;
- to promote the efficient and effective use of audit resources;
- to reduce burdens on state and local governments, Indian tribes, and nonprofit organizations; and
- to ensure that federal departments and agencies, to the maximum extent practicable, rely upon and use the audit work.

Regulatory guidance on single audits is contained in Office of Management and Budget (OMB) Circular No. A-133, Audits of States, Local Governments, and Non-Profit Organizations.

Major Provisions

The Single Audit Act generally requires each non-federal entity that expends $300,000 or more in federal awards during a fiscal year to have a single audit made for that year. A "single audit" covers both the entity's financial statements and a schedule of its federal awards. An entity subject to this provision may elect to have a program-specific audit if it has only one federal program and is not

---

[1024] Nonprofit organizations receiving federal financial assistance were previously subject to similar single-audit requirements in earlier versions of OMB Circular No. A-133, at that time named Audits of Institutions of Higher Education and Other Non-Profit Organizations.

otherwise required to have a financial statement audit. An entity with federal award expenditures less than the threshold is exempt from the act's audit requirements as well as from financial audit requirements of other federal laws, but must comply with federal requirements to maintain and allow access to records. These provisions do not preclude federal agencies from conducting or arranging for other audits as needed. Every two years, the Director of OMB may adjust the threshold amount, though not below $300,000. (For fiscal years ending after December 31, 2003, the Director has determined that the threshold should be raised to $500,000.)

Prior to the 1996 amendments, the act required single audits for state and local governmental entities that received (rather than expended) $100,000 or more of federal assistance a year; entities that received $25,000 or more but less than $100,000 could choose to have either a single audit or the financial and compliance audit required for particular programs. Only if entities received less than $25,000 in federal assistance were they exempt from the act. The 1996 amendments extended coverage to federal awards, which include cost-reimbursement contracts as well as financial assistance.

Entities subject to the act generally must conduct annual audits, although in some cases biennial audits are allowed. Audits must be conducted by independent auditors in accord with generally accepted government auditing standards, except that performance audits need not be included unless authorized by the Director of OMB. (Prior to the 1996 amendments, performance audits were expressly excluded.) Auditors must determine whether the financial statements are fairly presented in all material aspects in conformity with generally accepted accounting principles and whether the schedule of expenditures for federal awards is fairly presented in all material respects in relation to these statements.[1025]

For each major program, the act requires auditors to obtain an understanding of internal controls relating to compliance requirements, assess control risk, and perform tests of controls (unless they are deemed ineffective). The auditors must also determine whether the entity has complied with provisions of laws, regulations, and other requirements that have a direct and material effect on the program. Selection of major programs is based upon risk-based selection criteria developed by the Director of OMB. (Prior to the 1996 amendments, the act defined major programs simply by dollar thresholds.) The number of programs selected for audit testing using risk-based criteria is generally limited to the number of programs that exceed certain dollar thresholds for the non-federal entity; however, auditors must test programs that represent at least 50% of the

[1025] In auditing, materiality is determined by whether the magnitude of an omission or misstatement is such that a reasonable person relying on the assertion would be influenced by its inclusion or correction.

entity's federal expenditures, or whatever lower percentage the Director determines.

The Single Audit Act specifies various responsibilities for the Director of OMB, including (1) designating a clearinghouse to receive copies of audit reports, identifying recipients that failed to have audits required by the act, and undertaking analyses that assist the Director; (2) developing criteria to determine appropriate charges to federal awards for audit costs; (3) developing implementation guidance; and (4) developing criteria to determine which federal agency is to provide technical and other assistance for a given non-federal entity. The Director may also authorize pilot projects to test alternative methods of achieving the purposes of the act.

Under OMB Circular No. A-133, recipients expending more than $25 million a year ($50 million for fiscal years ending after December 31, 2003) shall have a "cognizant agency for audit responsibilities" that shall provide technical advice and liaison to auditees and auditors, consider requests for extensions, obtain or conduct quality control reviews, inform other federal agencies and law enforcement officials of irregularities and illegal acts, advise auditors and auditees of audit deficiencies requiring corrective action, coordinate other audits or reviews made by or for federal agencies, coordinate management decisions for audit findings, coordinate audit work and reporting responsibilities among auditors to achieve cost-effective audits, and consider auditee requests to qualify as low-risk. The cognizant agency for audit shall be the federal awarding agency that provides the predominant amount of direct funding for a recipient, determined every fifth year. Recipients that do not expend more than the threshold amounts just identified shall instead have an "oversight agency for audit responsibilities" that shall provide technical assistance and may, at its option, assume some of the other responsibilities of the cognizant agencies.

In addition, the act assigns monitoring responsibilities to the Comptroller General and establishes reporting and other requirements for federal agencies that provide financial assistance, for non-federal entities that receive the assistance (or pass it through to other entities), and for auditors. For example, if there are audit findings or reports of internal control weaknesses, the non-federal entity must submit plans for corrective action or describe why they are not needed.

Discussion

The Single Audit Act has improved the amount and quality of information that is available about federal financial assistance to state and local governments. By requiring entity-wide audits conducted in accordance with generally accepted government auditing standards and employing generally accepted accounting principles, the act has led to more comprehensive and reliable audit reports. More important, it has encouraged financial management reforms: new accounting systems have been installed; new ways of tracking federal funds have

been devised; and stronger administrative controls have been adopted. Federal agency oversight has improved.

The 1996 amendments were aimed at making the Single Audit Act more effective and less burdensome. Their most important change may be increased attention to federal award programs that pose the greatest financial risk — not only those with the largest expenditures but also those with ill-defined objectives, complicated administrative procedures, and minimal political review and oversight.

As is true of any audit, the effectiveness of single audits depends on timely completion and on the ability and willingness of decision makers to act on information made available. One study has shown that single audit reports have not always been received in accordance with OMB's reporting requirements and that the agency in question did not effectively use the reports to oversee and monitor program recipients.[1026] Another study showed that some agencies did not issue required written management decisions or have documentary evidence of their evaluations and conclusions on recipient actions to correct audit findings.[1027] For some issues, the effectiveness of single audits may also be limited because they do not as a rule include performance measures.

Selected Source Reading

Foelster, Mary McKnight and George A. Scott. "Single Audit Overhaul." Journal of Accountancy, vol. 185 (May 1998), pp. 75-79.

Miller, Gerald J. and Relmond P. VanDaniker. "Impact of the Single Audit Act on the Financial Management of State and Local Governments." The Government Accountants Journal, vol. 44 (spring 1995), pp. 55-63.

Melton, Robert W. "Optimizing Audit and Monitoring Effectiveness under Changes to OMB Circular A-133" Government Finance Review, vol. 14 (August 1998), pp. 29-32.

Bureau of the Census. Federal Audit Clearinghouse. Information about single audits can be obtained through the Federal Audit Clearinghouse at [http://harvester.census.gov/sac], visited December 18, 2003.

[1026] U. S. General Accounting Office, NIH Research — Improvements Needed in Monitoring Extramural Grants, GAO/HEHS/AIMD-00-139, May 2000.

[1027] U.S. General Accounting Office, Actions Needed to Ensure That Findings Are Corrected, GAO-02-705, June 2002.

Congress. House. Committee on Government Reform and Oversight. Single Audit Act Amendments of 1996. H.Rept. 104-607. 104th Congress, 2nd session. Washington: GPO, 1996.

Congress. Senate. Committee on Governmental Affairs. Single Audit Act Amendments of 1996. S.Rept. 104-266. 104th Congress, 2nd session. Washington: GPO, 1996.

Executive Office of the President. Council on Integrity and Efficiency. Standards Subcommittee. Improving the Single Audit Process. Washington: GPO, 1993.

Executive Office of the President. Office of Management and Budget. Audits of States, Local Governments, and Non-Profit Organizations. Circular No. A

133. Washington: GPO, 2003.

——. OMB Circular A-133 Compliance Supplement March 2003. Washington: GPO, 2003.

U.S. General Accounting Office. Single Audit — Actions Needed to Ensure That Findings Are Corrected. GAO-02-705. June 2002.

——. Single Audit — Single Audit Act Effectiveness Issues. GAO-02-877T. June 26, 2002.

——. Single Audit — Survey of CFO Act Agencies. GAO-02-376. March 2002.

——. Single Audit — Update on the Implementation of the Single Audit Act Amendments of 1966. GAO/AIMD-00-293. September 2000.

——. Government Auditing Standards (the Yellow Book). Links to current audit standards and related information are available through the GAO website at [http://www.gao.gov], visited December 18, 2003.

Bob Lyke

VII. Human Resources Management and Ethics

A. Title 5: The Federal Civil Service

Title 5 of the United States Code is the codification of laws on government organization and employees.[1028] It is divided into three parts. Part I, entitled "The Agencies Generally," includes seven chapters that cover the organization of departments, agencies, independent establishments, and government corporations; the powers of departments and agencies; administrative procedure; regulatory functions; judicial review; congressional review of agency rulemaking; and executive reorganization. "Civil Service Functions and Responsibilities" are the subject of Title 5's Part II, which includes four chapters on the Office of Personnel Management; the Merit Systems Protection Board, and the Office of Special Counsel; special authorities (rules, regulations, and investigations); and political activities of certain state and local employees.

Part III, entitled "Employees," presents the various policies related to management of the federal workforce. It is divided into nine subparts: Subpart A, "General Provisions," includes chapters on definitions for terms used in Title 5 and merit system principles; Subpart B, "Employment and Retention," includes chapters on examination, selection, and placement and retention and reemployment; Subpart C, "Employee Performance," includes chapters on training and performance appraisal; Subpart D, "Pay and Allowances," includes chapters on classification and pay rates and systems; Subpart E, "Attendance and Leave," includes chapters on hours of work and leave; Subpart F, "Labor-Management and Employee Relations," includes chapters on labor-management relations and adverse actions; Subpart G, "Insurance and Annuities," includes chapters on retirement and health insurance; Subpart H, "Access to Criminal History Record Information," covers access to criminal history records for national security and other purposes; and Subpart I, "Miscellaneous," includes chapters on personnel flexibilities for the Internal Revenue Service, a human resources management system for the Department of Homeland Security, and the National Security Personnel System for the Department of Defense.

The laws codified in Title 5 encompass policies related to how the federal government manages the executive branch workforce. Over the last several years, that process has been referred to as the management of human capital. Other terms that have frequently been used to describe the process are personnel administration and personnel management and human resources management. Each of these terms is discussed briefly below.

[1028] This compendium does not address personnel laws in other titles of the United States Code, including the United States military (Title 10), the Foreign Service (Title 22), the Veterans Health Administration (Title 38), and the Postal Service (Title 39).

The terms personnel administration and personnel management relate to "that aspect of management concerned with the recruitment, selection, development, utilization, and compensation of the members of an organization…. The former is mainly concerned with the technical aspects of maintaining a full complement of employees within an organization, while the latter concerns itself as well with the larger problems of the viability of an organization's human resources."[1029] Personnel management evolved from personnel administration. Human resources management (HRM) is a term that "although often used synonymously with personnel management … transcends traditional personnel concerns, taking the most expansive view of the personnel department's mandate. Instead of viewing the personnel function as simply that collection of disparate duties necessary to recruit, pay, and discharge employees, a[n] HRM approach assumes that personnel's appropriate mission is the maximum utilization of its organization's human resources."[1030] In the late 1970s and early 1980s, textbooks on the federal workforce began to emphasize HRM. The term has been especially used in discussing federal workforce management since the publication in September 1993 of the reports prepared under Vice President Albert Gore's National Performance Review (NPR).

The term human capital management refers to "a concept that views employees as assets in the same sense as financial capital. It presupposes that an investment in human potential will yield significant returns for the organization."[1031] Human capital also "describe[s] what an organization gains from the loyalty, creativity, effort, accomplishments, and productivity of its employees."[1032] The economist Lester C. Thurow further defined human capital as:

> *an individual's productive skills, talents, and knowledge. It is measured in terms of the value (price multiplied by quantity) of goods and services produced. Since consumption is the ultimate goal of our economic system, the value of a man's capital is the same as the value of the consumption goods and services which he directly or indirectly produces. When the value of goods and*

[1029] Facts on File Dictionary of Personnel Management and Labor Relations (New York: Facts on File, Inc., 2nd ed., 1985).

[1030] Ibid.

[1031] Ibid.

[1032] The Human Resources Glossary (New York: American Management Association, 1991).

services rises, the value of human capital rises. When the value of goods and services falls, the value of human capital falls.[1033]

On September 6, 1966, Title 5 was recodified with the enactment of P.L. 89-554 (80 Stat. 378). Information on the derivation of laws in the title is provided in the United States Code Annotated under the "Historical and Revision Notes" accompanying each section. Among the laws codified in the title are the Pendleton Act of 1883; the Retirement Acts of 1920, 1930, and 1956; the Classification Acts of 1923 and 1949; the Hatch Acts of 1939 and 1940; the Ramspeck Act of 1940; the Veterans' Preference Acts of 1944 and 1953; the Federal Employees' Pay Acts of 1945 and 1946; the Annual and Sick Leave Act of 1951; the Federal Employees' Group Life Insurance Act of 1954; the Fringe Benefits Act of 1954; the Federal Employees Salary Increase Act of 1958; the Government Employees Training Act of 1958; the Federal Employees Health Benefits Act of 1959; and the Federal Salary Reform Act of 1962.

Other laws codified in Title 5 include the Intergovernmental Personnel Act of 1970; the Job Evaluation Policy Act of 1970; the Federal Pay Comparability Act of 1970; the Equal Employment Opportunity Act of 1972; the Federal Wage System Act of 1972; the Civil Service Reform Act of 1978; the Alternative Work Schedule Act of 1978; the Spouse Equity Act of 1984; the Federal Employees' Retirement System Act of 1987; the Federal Employees Leave Sharing Acts of 1988 and 1993; the Whistleblower Protection Act of 1989; the Federal Employees Pay Comparability Act (FEPCA) of 1990; the Hatch Act Reform Amendments of 1993; and the Federal Workforce Restructuring Act (FWRA) of 1994.

This compendium's treatment of civil service issues is organized by chapters as they appear in Title 5. The chapter entries include discussion of selected laws on managing the federal executive branch workforce and their major amendments.[1034]

Twenty years of effort to establish a civil service for the executive branch of the federal government that was based on law and featured competitive examinations, relative security of tenure, and political neutrality culminated with

---

[1033] Lester C. Thurow, Investment in Human Capital (Belmont, CA: Wadsworth Publishing Co., Inc., 1970).

[1034] Several chapters of in Parts II and III of Title 5 are not included in this edition of the compendium. The omitted chapters include Chapter 29 ("Commissions, Oaths, Records, and Reports"); Chapter 81 ("Compensation for Work Injuries"); Chapter 85 ("Unemployment Compensation"); and Chapter 91 ("Access to Criminal History Records for National Security and Other Purposes").

enactment of the Pendleton Act of 1883.[1035] The act established the Civil Service Commission, which continued with largely the same mandate until 1978, when the Office of Personnel Management (OPM) was created in its stead. Although over the years many statutes (including those listed above) have been enacted to, among other things, expand the civil service, regulate political activities, classify and grade federal jobs, and set pay rates or establish mechanisms for pay setting, none so changed the original character of the civil service as did the Civil Service Reform Act (CSRA) of 1978 (92 Stat. 1111).[1036]

In addition to creating OPM, the CSRA of 1978 established the Office of Special Counsel (OSC), the Merit Systems Protection Board (MSPB), and the Federal Labor Relations Authority (FLRA) as independent organizations charged with protecting the merit system and adjudicating disputes between agencies and employees. The law also created a Senior Executive Service (SES) to enable department and agency heads to be assisted by experienced managers, some of whom were career civil servants and others of whom were political appointees, who could be moved to fill positions as assignments required. For the first time, authority for labor-management relations within the federal government was established in statute. Finally, personnel research programs and demonstration projects were authorized as a means for experimenting with various HRM policies, including pay and classification of jobs.

Implementation of the provisions of the CSRA of 1978 (particularly those on pay for performance and personnel research programs and demonstration projects) and FEPCA of 1990 were among the issues focused on during the Administrations of Presidents Ronald Reagan and George H.W. Bush. Among the concerns of President William J. Clinton's Administration was implementation of the recommendations presented by the NPR of 1993[1037] (particularly those on creating a family-friendly workplace) and the FWRA of 1994, which sought to reduce the size and scope of government. During the 1990s, OPM downsized considerably and contracted out traditionally centralized functions such as training and investigations. Executive branch agencies used voluntary separation incentives (commonly referred to as buyouts) instead of reductions-in-force to reduce their workforces. Departments and agencies developed in-house HRM capacities or contracted with OPM or other vendors for administrative services

---

[1035] Paul P. Van Riper, History of the United States Civil Service (Evanston, IL: Row, Peterson, and Company, 1958). Although dated, this work is still widely considered the best history of the federal civil service.

[1036] Patricia W. Ingraham and Carolyn Ban, eds., Legislating Bureaucratic Change, The Civil Service Reform Act of 1978 (Albany, NY: State University of New York Press, 1984).

[1037] U.S. Office of the Vice President, From Red Tape to Results: Creating a Government That Works Better & Costs Less. Report of the National Performance Review (Washington: GPO, 1993).

such as review and rating of job applications, classification of federal jobs, training, payroll administration, implementation of affirmative action policies, and counseling services. During this period as well, OPM publicized the various HRM flexibilities provided government-wide under Title 5 and encouraged departments and agencies to use them. Congress authorized separate authorities for personnel management at the Federal Aviation Administration and the Internal Revenue Service that provide for greater HRM flexibilities than Title 5 generally permits.[1038]

Policies on federal workforce management in the Administration of President George W. Bush have been influenced significantly by the September 11, 2001 terrorist attacks on the World Trade Center and the Pentagon, and the discovery of anthrax in Washington, DC, and other cities. The President's term began with OPM's continued emphasis on the full use of already existing government-wide personnel flexibilities by departments and agencies and the incorporation of the management of human capital into agency strategic plans and processes (currently being implemented through the establishment of agency chief human capital officers (CHCOs) and a CHCO Council). In the wake of 9-11, however, new requirements for the federal government's HRM system have been stated by the White House and OPM. According to the President, the nation's efforts to fight terrorism require a system that is modern and flexible and puts the right people in the right place at the right time. In practice, this has been translated into law as authority for separate HRM systems for the Transportation Security Administration and the Departments of Homeland Security (DHS) and Defense (DOD) that provide the respective department heads with considerable discretion to establish their particular systems outside of many of the current Title 5 policies.[1039] Depending on how they are implemented, the DHS and DOD changes arguably could rival the CSRA of 1978 for impact on the civil service.

Both of the newly created systems at DHS and DOD have been described by the White House and some Members of Congress as demonstration projects whose various features could ultimately be applied to executive branch employees government-wide. Currently, the systems are authorized in separate chapters of Title 5 (Chapter 97 covers DHS and Chapter 99 covers DOD), and their implementation is expected to occur over several years. Whether the features of

---

[1038] For the Federal Aviation Administration (FAA), see P.L. 104-50, 109 Stat. 436 and subsequent amendments in P.L. 104-122, 110 Stat. 876; P.L. 104-264, 110 Stat. 3213; P.L. 105-339, 112 Stat. 3182; and P.L. 106-181, 114 Stat. 61. For the Internal Revenue Service (IRS), see P.L. 105-206, 112 Stat. 711. The FAA authority is codified in Title 49 of the United States Code. The IRS authority is codified in Title 5 of the United States Code as Chapter 95.

[1039] For the Transportation Security Administration (TSA), see P.L. 107-71, 115 Stat. 597; for the Department of Homeland Security (DHS), see P.L. 107-296, 116 Stat. 2229; and for the Department of Defense (DOD), see P.L. 108-136, 117 Stat. 1621. The TSA authority is codified in Title 49 of the United States Code. The DHS authority is codified as Chapter 97, and the DOD authority is codified as Chapter 99 in Title 5 of the United States Code.

one or both of the new systems are determined to be applicable to other federal agencies, or whether individual agencies continue to seek congressional approval for their own personnel flexibilities (a National Aeronautics and Space Administration proposal is currently pending in the 108th Congress), it seems likely that Congress will need to reconsider Title 5 (and the accompanying Title 5 Code of Federal Regulations that compiles the implementing regulations) as the Chapters 97 and 99 provisions are fully implemented.

Approaches that might be examined include recodification of the title into chapters that reflect HRM policies that apply government-wide; recodification of the title into chapters arranged by the general principles governing a particular policy, followed by all the exceptions to the policy; or continuation of the current amendment process that establishes separate chapters in Title 5 or other titles of the United States Code for individual departments granted separate authority. Issues that could be considered include which approach would provide for the administration of policies on government organization and employees in an efficient, understandable, coordinated, and fair manner; which approach would facilitate ongoing oversight of agency systems to ensure conformance with merit system principles and avoidance of prohibited personnel practices; and whether OPM or another organization or organizations would centrally administer HRM policies and exercise the authority for overseeing these policies.

Barbara L. Schwemle

(1) Office of Personnel Management (Chapter 11; in Part II).

Statutory Intent and History

The Office of Personnel Management (OPM), established pursuant to the Civil Service Reform Act of 1978 (92 Stat. 1119) succeeded the Civil Service Commission (CSC) established in 1883. The original objective in creating the CSC was to remove the selection and management of federal personnel from partisan political influence. With the passage of time, the leadership provided by the CSC, a multi-headed agency, was judged critically by some in the executive branch and in Congress. It was hoped that a new single-headed agencywould provide more effective leadership. By giving OPM the leadership role in federal personnel management, it was believed that the agency would be able to concentrate on planning and administering an effective government-wide program of personnel management. "Without the demands generated by a heavy day-to-day workload of individual personnel actions, OPM should provide the President, the civil service, and the Nation with imaginative public personnel administration."[1040]

In a 1993 assessment of the agency, the Clinton Administration's National Performance Review (NPR) identified OPM as a leader and source of expert advice concerning a broad range of human resources management matters. For the immediate future, the NPR envisioned OPM advising the President on issues affecting the management of federal employees; demonstrating commitment to diversity; planning for development of the workforce of the future; identifying strategies for providing the training essential to achieve a cultural shift toward more entrepreneurial management; conducting research, providing consulting services, and advising agencies on best practices; coordinating and sponsoring interagency cooperation on common issues; influencing government-wide change; and leading by example. The NPR indicated that achievement of this role would require OPM to overhaul its structure and change its internal culture. OPM privatized its investigations function, while training programs were transferred to the U.S. Department of Agriculture Graduate School. The OPM Director assured Congress that the agency would retain government-wide training policy and leadership responsibilities.

Significant reorganization of the agency, based on OPM's strategic plan, occurred in December 2002 when OPM's 12 departments were combined into 4 central divisions: Strategic Human Resources Policy, Human Resources Products and Services, Management and Chief Financial Officer, and Human Capital Leadership and Merit Systems Accountability. In the Homeland Security Act of 2002 (116 Stat. 1229) and the National Defense Authorization Act for FY2004

[1040] U.S. Congress, House Committee on Post Office and Civil Service, Legislative History of the Civil Service Reform Act of 1978, committee print, 96th Cong., 1st sess., Committee Print 96-2 (Washington: GPO, 1979), vol. II, p. 1470.

(P.L. 108-136; 117 Stat. 1621), Congress authorized the OPM Director, along with the Secretaries of the Departments of Homeland Security (DHS) and Defense (DOD), respectively, to jointly prescribe regulations to establish new human resources management (HRM) systems at DHS and DOD. (See the discussions of the 5 U.S.C. Chapter 97 and Chapter 99 provisions in this compendium.)

Major Provisions

Established as an independent agency in the executive branch, OPM's management structure comprises a director, deputy director, and the four associate directors mentioned above. The director executes, administers, and enforces civil service laws, rules, and regulations and oversees other OPM activities, including retirement and classification, except functions for which the Merit Systems Protection Board or the Special Counsel (the agency head for the Office of Special Counsel) are primarily responsible. The director aids the President as requested in preparing civil service rules, and otherwise advises the President on actions which may be taken to promote an efficient civil service and a systematic application of the merit system principles, including recommending policies relating to the selection, promotion, transfer, performance, pay, conditions of service, tenure, and separation of employees. The director also conducts or provides studies and research on improvements in personnel management. The director's duties may be delegated, except those regarding competitive examinations for positions with requirements common to all federal agencies. OPM maintains an oversight program to ensure that delegated authorities are in accordance with merit system principles and standards.

The Homeland Security Act of 2002 (116 Stat. 2289) at Section 1304 amended the director's functions to mandate that OPM design a set of systems, including appropriate metrics, for assessing the management of human capital by federal agencies. The systems must be defined in OPM regulations and include standards for (A) aligning agency human capital strategies with their missions, goals, and organizational objectives and integrating those strategies into agency budget and strategic plans; (B) closing skill gaps in mission critical occupations; (C) ensuring continuity of effective leadership through implementation of recruitment, development, and succession plans; (D) sustaining a culture that cultivates and develops a high-performing workforce; (E) developing and implementing a knowledge management strategy supported by appropriate investment in training and technology; and (F) holding managers and human resources officers accountable for efficient and effective human resources management in support of agency missions in accordance with merit system principles. The provision became effective on May 24, 2003.

In January 1999, the director was designated as the Chair of the President's Task Force on Federal Training Technology, established to encourage the use of technology in training. The director also chairs the Chief Human Capital Officers Council. (See the discussion of the 5 U.S.C. Chapter 14 provision in this compendium.)

Discussion

In the 104th Congress, legislation (H.R. 3483) was considered, but not enacted, which would have substantially altered the OPM Director's responsibilities. The thrust of the legislation, and the recent internal management activities of OPM, supported by the NPR, have been to delegate to the departments and agencies as many personnel functions as possible. OPM has been envisioned as a catalytic and overseer agency, not as an agency performing personnel functions of an executive branch-wide nature. Concerns have been raised by a number of organizations, such as the Senior Executives Association, that the downsizing of OPM and dispersal of its authorities and operations have placed OPM's capacity to carry out its statutory responsibilities at risk.

OPM's human resources management initiatives for 1998 and 1999 emphasized its expertise and leadership and sought to amend the agency's authorization to reorganize and clarify the responsibilities of the OPM Director. Vice President Gore announced in January 1999 that OPM would be proposing new hiring options to permit alternative selection procedures, to authorize agencies to make direct job offers in critical areas like information technology, to establish additional means for recruiting a diverse workforce, and to use non-permanent employees, with appropriate benefits, but a legislative proposal was not submitted to the 106th Congress.

Since enactment of P.L. 103-62, the Government Performance and Results Act (GPRA), oversight of OPM's role has especially focused on its administration of the civil service merit system and its human resources management leadership. The President's budget during the last three fiscal years of the Clinton Administration emphasized OPM's role as the administrator of the merit systems and designated it as a high impact agency. OPM announced an ambitious plan in its GPRA-mandated strategic plan for FY2000-FY2005. The strategic plan was revised in December 2002 and now covers the period 2002-2007. The plan has three strategic goals: (1) to have federal agencies adopt human resources management systems that improve their ability to build successful, high performance organizations; (2) to have federal agencies use effective merit-based human capital strategies to create a rewarding work environment that accomplishes the mission; and (3) to meet the needs of federal agencies, employees, and annuitants through the delivery of efficient and effective products and services. Various objectives accompany each goal. An annual performance plan accompanies the strategic plan. GAO concerns surrounding the agency's performance plans have been the inclusion of cost-based performance measures to provide an indication of how efficiently OPM is performing various activities and the credibility of agency performance information. OPM's FY2004 performance plan includes various instruments intended to permit program evaluation.

As part of the President's Management Agenda, OPM is leading the federal government's Strategic Management of Human Capital Initiative. (See [http://www.opm.gov], and choose "Strategic Management of Human Capital" on the home page menu.) OPM staff have been engaged in a joint effort with DHS and DOD to write the regulations creating new HRM systems at these departments since late 2002.

Significant workforce reductions have occurred at the agency. Especially troubling to some practitioners was the downsizing of the agency's library, which resulted in the loss of much of its well-regarded collection of materials on the Civil Service and all aspects of HRM. Questions about the agency's ability to carry out its statutory responsibilities despite the loss of staff persist. The Merit Systems Protection Board's (MSPB's) statutorily mandated evaluation of OPM's administration of the merit system found much improvement, but recommended increased leadership and coordination with the agencies. MSPB's December 2001 report included recommendations that OPM actively influence "broad-based regulatory or statutory changes where feasible" and "be an active participant in decisionmaking regarding HR [human resources] policies and programs." In a January 2003 report on OPM, GAO identified OPM's management challenges as: (1) leading strategic human capital management government-wide; (2) overseeing agency human capital management systems; (3) transforming OPM and managing its internal operations; and (4) administering the retirement and health insurance programs. A May 2003 GAO report suggested that OPM compile, analyze, and share information about personnel flexibilities that are being and should be used and "more vigorously identify new flexibilities that would help agencies better manage their human capital and then work to build consensus for the legislative action needed."

<u>Selected Source Reading</u>

Lane, Larry M. "The Office of Personnel Management: Values, Policies, and Consequences." In Patricia W. Ingraham and David H. Rosenbloom, eds. The Promise and Paradox of Civil Service Reform. Pittsburgh, PA: University of Pittsburgh Press, 1992.

Pfiffner, James P. and Douglas A. Brook, eds., The Future of Merit: Twenty Years After the Civil Service Reform Act. Washington: Woodrow Wilson Center Press, 2000.

Congress. Senate. Committee on Governmental Affairs. Major Management Challenges Facing Federal Departments and Agencies. 106th Congress, 2nd session. Washington: 2000.

Congress. House. Committee on Post Office and Civil Service. Legislative History of the Civil Service Reform Act of 1978. Committee print. 96th Congress, 1st session. Committee Print 96-2. Washington: GPO, 1979.

General Accounting Office. Human Capital; OPM Can Better Assist Agencies in Using Personnel Flexibilities. GAO-03-428. May 2003.

——. Major Management Challenges and Program Risks; Office of Personnel Management. GAO-03-115. January 2003.

——. Observations on the Office of Personnel Management's Fiscal Year 1999 Performance Report and Fiscal Year 2001 Performance Plan. GAO/GGD-00156R. June 30, 2000.

——. Results Act, Observations on the Office of Personnel Management's Annual Performance Plan. GAO/GGD-98-130. July 1998.

——. Results Act, Observations on the Office of Personnel Management's Fiscal Year 2000 Annual Performance Plan. GAO/GGD-99-125. July 1999.

U.S. Merit Systems Protection Board. Civil Service Evaluation, The Evolving Role of the U.S. Office of Personnel Management, A Report Concerning Significant Actions of the U.S. Office of Personnel Management. Washington: GPO, 1998.

——. The U.S. Office of Personnel Management in Retrospect; Achievements and Challenges After Two Decades. Washington: MSPB, 2001.

U.S. Office of Personnel Management. Congressional Budget Justification; Annual Performance Plan Fiscal Year 2004. Washington: OPM, 2003.

——. Fiscal Year 2002 Performance and Accountability Report. Washington: OPM [2003].

——. Strategic Plan 2002-2007. Washington: OPM [2002].

U.S. Office of the Vice President. National Performance Review. From Red Tape to Results: Creating a Government That Works Better & Costs Less. Office of Personnel Management: Accompanying Report of the National Performance Review. Washington: GPO, 1993.

Barbara L. Schwemle

(2) Merit Systems Protection Board; Office of Special Counsel; and Employee Right of Action (Chapter 12; in Part II).

Statutory Intent and History

The underlying statute for the Merit Systems Protection Board (MSPB) is the Civil Service Reform Act (CSRA) of 1978 (92 Stat. 1121). This same statute and the Whistleblower Protection Act of 1989 (103 Stat. 17) also established the Office of Special Counsel (OSC) and Employee Right of Action. These laws sought to create separate entities to perform personnel appellate and adjudicatory functions. The OSC, initially part of MSPB, became an independent agency with enactment of the whistleblower law, an action largely prompted by disputes over budget resources. In stating the need for reform, the CSRA legislative history noted that, "There is little doubt that a vigorous protector of the merit system is needed. The lack of adequate protection was painfully obvious during the civil service abuses only a few years ago. Establishment of a strong and independent Board and Special Counsel will discourage subversions of merit principles." MSPB and OSC were reauthorized through 2007 in P.L. 107-304 (116 Stat. 2364), enacted on November 27, 2002.

Major Provisions

The Merit Systems Protection Board was established with three members. The functions of the board are to (1) hear, adjudicate, or provide for the hearing or adjudication of personnel matters and take final action on such matters; (2) order any federal agency or employee to comply with any decision of the board and enforce compliance; (3) conduct special studies on the civil service and executive branch merit systems, and report to the President on protection of the merit system; and (4) review OPM rules and regulations.

The Office of Special Counsel was established to (1) protect employees, former employees, and applicants for employment from prohibited personnel practices; (2) receive and investigate allegations of prohibited personnel practices and bring petitions for stays and corrective actions, and file complaints or recommend disciplinary actions; (3) receive, review, and forward to the Attorney General (where necessary) disclosures of violations of any law, rule, or regulation, or gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety; (4) review OPM rules and regulations; and (5) investigate and bring actions concerning allegations of violations of laws.

An employee may seek corrective action from MSPB for a prohibited personnel action taken against him or her; MSPB may issue a stay of the personnel action involved.

If the Special Counsel does not transmit the information to the agency head, the Special Counsel shall inform the individual of the reasons why the disclosure may not be further acted on and other offices available for receiving disclosures, should the individual wish to pursue the matter further (added by P.L. 107-304, 116 Stat. 2364).

Discussion

As originally established by Congress, MSPB was granted a permanent authorization. Seeking "to maintain close scrutiny" of the agency, Congress changed this to a term authorization in 1989. Among the issues which have arisen in discussions of MSPB's mission are these: the agency's role in enforcing the Whistleblower Protection Act provisions; whether it has a bias toward management; the board's use, or lack thereof, of employee stays; its actions to hold agencies accountable; and the agency's interpretation of concepts such as burden of proof, reasonable belief, and eligibility.

An issue that has concerned both the authorizing and the appropriating committees is the process by which an employee appeals a personnel action. In a September 1995 issue paper, the Vice President's National Performance Review and MSPB recommended streamlining of the process. A draft version of H.R. 3841, an original bill offered during the 104th Congress, included language that would have provided for employee appeal rights to either MSPB or the Equal Employment Opportunity Commission, but not both. Lacking bipartisan agreement, this provision was removed during subcommittee markup of H.R. 3841. A similar provision, but one providing that MSPB would have the jurisdiction, was included in draft legislation, prepared but not introduced, in the 105th Congress, by the House Civil Service Subcommittee chair, Representative Mica. A National Academy of Public Administration study of the issue found that "MSPB is generally viewed in a positive light due to its timely and consistent decisions." A January 1999 symposium marking the 20th anniversary of MSPB heard renewed calls for improvement to the appeals process.

Other issues involving MSPB concern caseload, use of alternative dispute resolution procedures, and administrative judge pay. With regard to the latter, an agreement between the MSPB chair and the MSPB professional association would have amended Title 5 to establish an administrative judge pay system with four levels of pay referenced to Senior Executive Service pay and the application of locality pay. In the 106th Congress, Representative George Gekas introduced H.R. 2946, which included the provisions found in the agreement, but no further action was taken. Similar legislation (H.R. 1965) was introduced in the 107th Congress.

Congress changed the Office of Special Counsel from a permanent to a term authorization for the same reason as MSPB's authorization was changed. Much of the discussion about the OSC has focused on its alleged ineffectiveness and employee bypassing of the agency to seek relief in other forums. H.R. 5512,

introduced in the 106th Congress, would have provided that "except as provided in Section 518 of Title 28, relating to litigation before the Supreme Court, attorneys designated by the Special Counsel may appear for the Special Counsel and represent the Special Counsel in any civil action brought in connection with Section 2302(b)(8) [relating to prohibited personnel practices] or Subchapter III of Chapter 73 [relating to prohibitions on political activity], or as otherwise authorized by law." The bill also would have authorized the Special Counsel to obtain review of any final order or decision of the Merit Systems Protection Board by filing a petition for judicial review in the United State Court of Appeals for the Federal Circuit under certain circumstances. No further action occurred on H.R. 5512.

The Homeland Security Act of 2002 (P.L. 107-296; 116 Stat. 2229) and the National Defense Authorization Act for FY2004 (P.L. 108-136; 117 Stat. 1621) authorize the creation of new human resources management (HRM) systems for civilian employees of the Departments of Homeland Security and Defense. Both laws amend appellate procedures for these employees. (See the discussions of the 5 U.S.C. Chapter 77, Chapter 97, and Chapter 99 provisions in this compendium.)

In a December 5, 2003 memorandum to employees, MSPB announced that as part of a consolidation of agency operations, its Boston and Seattle field offices would be closed by March 31, 2004. The agency anticipates closing the Denver field office in 2005 and may close the New York City field office no earlier than 2005. Changes to the appellate procedures made by the Homeland Security and DOD Authorization Acts are reportedly part of the impetus for consolidation.

Selected Source Reading

CRS Report 97-787 A. Whistleblower Protections for Federal Employees, by L. Paige Whitaker and Michael Schmerling (1998).

National Academy of Public Administration. Facilitating Solutions to Multiple Appellate Processes: Alternatives for Change. Washington: NAPA, 1997.

Pfiffner, James P. and Douglas A. Brook, eds. The Future of Merit: Twenty Years After the Civil Service Reform Act. Washington: Woodrow Wilson Center Press, 2000.

"Symposium on the Civil Service Reform Act of 1978: An Evaluation." Policy Studies Journal, vol. 17 (winter 1988-1989), pp. 311-447.

Congress. House. Committee on Government Reform and Oversight. H.R. 3841, Omnibus Civil Service Reform Bill. Hearing. 104th Congress, 2nd session. Washington: GPO, 1996.

Congress. House. Committee on Government Reform and Oversight. Subcommittee on the Civil Service. Civil Service Reform IV: Streamlining Appeals Procedures. Hearing. 104th Congress, 1st session. Washington: GPO, 1995.

Congress. House. Committee on Post Office and Civil Service. Legislative History of the Civil Service Reform Act of 1978. Committee print. 96th Congress, 1st session. Committee Print 96-2. Washington: GPO, 1979.

General Accounting Office. Merit Systems Protection Board: Mission Performance, Employee Protections, and Working Environment. GGD-95-213. 1995.

Merit Systems Protection Board. Merit Systems Protection Board Annual Report Fiscal Year 2002. Washington: MSPB, no date.

——. Merit Systems Protection Board Performance and Accountability Report for FY2003. Washington: MSPB [2003].

——. Merit Systems Protection Board Performance Plan Fiscal Year 2003 (Revised Final) and Fiscal Year 2004 (Final). Washington: MSPB [2003].

——. Merit Systems Protection Board Strategic Plan FY2001-FY2006. Washington: MSPB [2002].

——. Removing Poor Performers in the Federal Service. Issue Paper. Washington: MSPB, 1995.

U.S. Office of Special Counsel. Annual Performance Plan FY2002. Washington: OSC, no date.
——. Annual Performance Report of the U.S. Office of Special Counsel for Fiscal Year 2002. Washington: OSC, no date. ——. OSC Strategic Plan FY2001-2006. Washington: OSC [2001]. ——. A Report to Congress from the U.S. Office of Special Counsel for Fiscal Year

2002. Washington: OSC, no date. Barbara L. Schwemle

(3) Special Authority (Chapter 13; in Part II).

Statutory Intent and History

The system of special authority i.e., drafting and issuing personnel rules and regulations, and controlling, supervising, and retaining records of and examinations for the competitive service, as well as investigating personnel security matters and issuing reports generally, was established by the Civil Service Act of 1883 (Pendleton Act; 22 Stat. 404) and the Veterans Preference Act of 1944 (P.L. 78-359; 58 Stat. 387). The intent was to remove partisan political influences from the selection and retention of civil servants, protect veterans' preference with respect to employment and retention, and authorize security investigations.

Major Provisions

The Office of Personnel Management (OPM), formerly the Civil Service Commission, is directed to aid the President, at his request, in preparing the rules he prescribes under Title 5 of the United States Code for administering the competitive service. OPM is required to prescribe regulations, control, supervise, and preserve records of and examinations for the competitive service. The agency is charged also with issuing and enforcing regulations to implement provisions of Title 5 of the United States Code and relevant executive orders that set forth the policy giving preference to eligibles (i.e., certain veterans) in the competitive service and the excepted service in the executive agencies and the government of the District of Columbia.

OPM is authorized to investigate and report on matters concerning enforcement and the effect of rules the President and the OPM prescribe under Title 5 of the United States Code for administering the competitive service.

OPM is directed to conduct investigations and issue reports required by cited sections of Titles 22 and 42 of the United States Code relating to security status of United States representatives appointed to some international organizations and individuals involved with the National Science Foundation. This investigative authority may be exercised by the Federal Bureau of Investigation (FBI), rather than OPM, under certain circumstances. A revolving fund is available to OPM without fiscal year limitation for financing investigations, training, and other functions the office is authorized or required to perform on a reimbursable basis. An agency may use available appropriations to reimburse OPM or the FBI for the cost of investigations, training, and functions performed for the agency or to make advances for their cost.

For the purposes of certain sections of Title 5 of the United States Code that relate to administrative law judges, OPM may and, for purposes of 5 U.S.C. § 7521 relating to administrative law judges, the Merit Systems Protection Board may investigate, require reports of agencies, prescribe regulations, appoint advisory

committees as necessary, recommend legislation, subpoena witnesses and records, and pay witness fees as established for the courts of the United States.

OPM is required to keep minutes of its proceedings and to publish annual reports on Chapter 83 (retirement), including the status of the Civil Service Retirement and Disability Fund, and to report annually to Congress on the operation of Chapters 87 (life insurance) and 89 (health insurance) of Title 5 of the United States Code.

Discussion

This chapter, which generally originated in the Civil Service Act of 1883, centralizes federal personnel functions in OPM. Some have argued that some functions granted herein should be exercised by agencies to permit them to design regulations and procedures suitable to their individual needs, while others believe that continuing the current centralized system is more effective.

Selected Source Reading

Bussey, Ellen M. Federal Civil Service Law and Procedures: A Basic Guide. Washington: Bureau of National Affairs, 1990.

U.S. Office of the Vice President. National Performance Review. From Red Tape to Results: Creating a Government That Works Better & Costs Less.
Accompanying Report of the National Performance Review "Office of Personnel Management." Washington: GPO, 1993.

Thomas J. Nicola

(4) Agency Chief Human Capital Officers (Chapter 14, in Part II).

Statutory Intent and History

Title XIII, Subtitle A of The Homeland Security Act of 2002 (116 Stat. 2287; P.L. 107-296) authorizes the establishment of chief human capital officer (CHCO) positions in federal executive branch agencies. The purpose of the provision is to raise the institutional profile of strategic human capital management within federal agencies.

Major Provisions

Section 1301 of the Homeland Security Act is entitled the Chief Human Capital Officers Act of 2002. Section 1302, amends Part II of Title 5 United States Code by adding a new Chapter 14 — Agency Chief Human Capital Officers. The new Section 1401 of Title 5 United States Code provides that the agency head must appoint or designate a CHCO who must advise and assist the agency head and other agency officials in carrying out the agency's responsibilities for selecting, developing, training, and managing a high-quality, productive workforce in accordance with merit system principles; implement the rules and regulations of the President and OPM and the laws governing the civil service within the agency; and carry out such functions as his or her primary duty.

The agencies covered by the CHCO provision are enumerated at 31 U.S.C. § 901(b)(1) and (2), which lists agencies subject to the Chief Financial Officers (CFO) Act, and include the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, Veterans Affairs, the Environmental Protection Agency, and the National Aeronautics and Space Administration. Other agencies covered are the Agency for International Development, the Federal Emergency Management Agency, the General Services Administration, the National Science Foundation, the Nuclear Regulatory Commission, the Office of Personnel Management, the Small Business Administration, and the Social Security Administration.

The Department of Homeland Security (DHS) is not covered by Chapter 14, although Section 103 of the Homeland Security Act (116 Stat. 2145) established a CHCO for DHS with responsibilities enumerated in Section 704 (116 Stat. 2219). The 108th Congress is considering legislation (H.R. 2886, S. 1567) that would, if enacted, include DHS among the CFO Act agencies and therefore make DHS subject to Chapter 14.

Under the new Section 1402, CHCOs have six functions, including (1) setting the workforce development strategy of the agency; (2) assessing workforce characteristics and future needs based on the agency's mission and strategic plan; (3) aligning the agency's human resources policies and programs with organization mission, strategic goals, and performance outcomes; (4) developing

and advocating a culture of continuous learning to attract and retain employees with superior abilities; (5) identifying best practices and benchmarking studies; and (6) applying methods for measuring intellectual capital and identifying links of this capital to organizational performance and growth. CHCOs must have access to all records, reports, audits, reviews, documents, papers, recommendations, or other materials that are the property of the agency or are available to the agency; and relate to programs and operations with respect to which the CHCO has responsibilities. The CHCO may request such information or assistance as may be necessary for carrying out the duties and responsibilities provided by Chapter 14 from any federal, state, or local governmental entity.

Section 1303 of the law establishes a CHCO Council consisting of the OPM Director who acts as chairperson; the OMB deputy director for management who acts as vice chairperson; and CHCOs of executive departments and any other members designated by the OPM Director. The council must meet periodically to advise and coordinate the activities of the member agencies on such matters as modernization of human resources systems, improved quality of human resources information, and legislation affecting human resources operations and organizations. The CHCO Council must ensure that representatives of federal employee labor organizations are present at a minimum of one meeting of the council each year. The representatives are not members of the council. Each year the CHCO Council must submit a report to Congress on its activities.

Section 1304 of the law amends 5 U.S.C. § 1103 by adding a subsection (c) which provides that OPM must design a set of systems, including appropriate metrics, for assessing the management of human capital by federal agencies. (See the discussion under 5 U.S.C. Chapter 11 in this compendium.) The CHCO provisions became effective on May 24, 2003, under Section 1305 of the law.

Discussion

The provisions on CHCOs are intended to facilitate communication among executive branch departments and agencies and enhance the coordination of human resources management in the federal government. At two days of hearings in March 2002 on the federal workforce, conducted by the Senate Subcommittee on International Security, Proliferation, and Federal Services, Members took testimony on the positive role that councils play in developing and implementing initiatives to address federal management issues and serving as communities of interest that share best practices. They also received testimony as to the intent of the provisions that CHCOs be senior managers who are charged with deploying human resources management authorities efficiently and strategically.

On May 24, 2003, OPM Director Kay Coles James announced the names of those who will serve on the CHCO Council. The Council conducted its first meeting on June 11, 2003. Council meetings have included, among other issues, discussions on encouraging federal agencies to use the personnel flexibilities that have

already been authorized, career development in the federal government, and emergency procedures for federal agencies.

Selected Source Reading

Armey, Representative Dick. "Homeland Security Act of 2002." Remarks in the House. Congressional Record, daily edition, vol. 148 (November 13, 2002), pp. H8595-H8645.

U.S. Congress. Senate. Committee on Governmental Affairs. Subcommittee on International Security, Proliferation, and Federal Services. The Federal Workforce: Legislative Proposals for Change. Hearing. 107th Congress, 2nd session. Washington: GPO, 2003.

Barbara L. Schwemle

(5) Political Activity of Certain State and Local Employees (Chapter 15; in Part II).

Statutory Intent and History

Chapter 15, commonly referred to as the Hatch Act covering state or local government officers and employees, addresses the extent to which such workers can be politically active. The underlying statutes for the Chapter 15 provisions are the Federal Election Campaign Act Amendments of 1974 (88 Stat. 1290) and the Civil Service Reform Act of 1978 (92 Stat. 1225). The 1974 law removed all but three of the prohibitions on political activities of certain state and local employees. Enforcement provisions that provide penalties for violations were added in 1978.

Major Provisions

Chapter 15 covers state or local government officers or employees who are "employed by a State or local agency [and] whose principal employment is in connection with an activity which is financed in whole or in part by loans or grants made by the United States or a Federal agency." An individual who exercises no functions in connection with such activity is not covered. District of Columbia (DC) government officers or employees, other than the mayor, members of the City Council, or the Recorder of Deeds, are covered by Chapter 73 provisions of the Hatch Act Reform Amendments of 1993 (107 Stat. 1001).

A covered state or local officer or employee may not:

- use official authority or influence for the purpose of interfering with or affecting the result of an election or a nomination for office;
- directly or indirectly coerce, attempt to coerce, command, or advise a state or local officer or employee to pay, lend, or contribute anything of value to a party, committee, organization, agency, or person for political purposes; or
- be a candidate for elective office.

A state or local officer or employee retains the right to vote and express opinions on political subjects and candidates. The prohibition on candidacy for elective office applies to only a limited number of state and local elections. A state or local officer or employee is not prohibited from being a candidate in any election if none of the candidates being nominated or elected represents a party whose candidates for presidential elector received votes in the last preceding election at which presidential electors were selected. Office of Personnel Management (OPM) regulations define this as a nonpartisan election.

Any federal agency making a loan or grant of U.S. funds to a state or local officer or employee for an activity must report to the Special Counsel (who heads the Office of Special Counsel, a federal agency) if it reasonably believes that the individual has violated the prohibitions against influencing elections or taking

part in political campaigns. If warranted, the Special Counsel then investigates and presents its findings and any resulting charges to the Merit Systems Protection Board (MSPB). MSPB fixes the time and place for a hearing and notifies the officer or employee being charged and the employing agency of the alleged violation. The hearing may not be held earlier than 10 days after the notice is mailed.

The state or local officer or employee and the agency may appear with counsel at the hearing. After the hearing, MSPB determines whether a violation has occurred; if so, the board determines whether the violation warrants removal from the office or job and notifies the individual and the agency by mail. MSPB imposes a penalty when it finds that (1) a state or local officer or employee has not been removed from office or employment within 30 days of receiving its notice that the individual has violated the law and must be removed; or (2) a removed state or local officer or employee has been appointed within 18 months to an office or employment in the same state in a state or local agency which does not receive loans or grants from a federal agency. In such cases, MSPB orders the federal agency to withhold from its loans or grants to the state or local agency an amount equal to two years' pay at the rate the individual was receiving when the violation occurred. If the appointment has been made within 18 months to a state or local agency that receives federal loans or grants, MSPB directs that the withholding be made from the agency. The order becomes effective 30 days after it has been mailed to the agency. MSPB may not require an amount to be withheld from a loan or grant pledged by a state or local agency as security for its bonds or notes if such withholding jeopardizes payment of the principal or interest.

MSPB may subpena witnesses to attend and testify and produce documentary evidence relating to any matter concerning political activity of covered state and local employees. When a subpena is disobeyed, a U.S. court may require the attendance and testimony of witnesses and the production of documentary evidence. In case of contumacy or refusal to obey a subpena, the United States District Court within whose jurisdiction the inquiry is proceeding may order the person to appear before MSPB, or to produce documentary evidence if so ordered, or to give evidence concerning the matter in question. Any failure to obey the court order may be punished as contempt. MSPB may order testimony to be taken by deposition at any stage of its proceeding or investigation. A person subpoenaed by MSPB may not be excused from attending, testifying, or producing documentary evidence because to do so could incriminate or subject him to a penalty or forfeiture. A person who falsely testifies may be prosecuted for perjury.

A party aggrieved by an MSPB action may, within 30 days, petition for a review in the United States District Court for the district in which he or she resides. The start of proceedings does not stay the order or determination unless the court so orders, and the officer or employee is suspended from his office or employment while proceedings are pending. The court reviews the entire record, including

questions of fact and law. It may direct that additional evidence be taken. MSPB may modify its findings or determination or order because of additional evidence. The modification is filed with the court if conclusive. The court affirms the determination or order, or the modified action if it is in accord with law. If it is not, the court remands the proceeding to MSPB with directions to comply with the law. The court's actions are final, subject to review by the appropriate United States Court of Appeals, as are those of the court of appeals subject to review by the United States Supreme Court on certiorari or certification.

Discussion

Legislation (H.R. 308) which sought to repeal the prohibition on state or local government officers or employees seeking elected office was introduced in the 105th Congress, but no further action occurred. Similar legislation had been introduced in both the 103rd and 104th Congresses. Also in the 104th Congress, legislation (H.R. 3918) which would have treated DC government employees the same as state and local government employees for purposes of 5 U.S.C. Chapter 15 was introduced, but no further action occurred. Similar legislation also was introduced in the 107th Congress (H.R. 4617).

Discussions to amend the Hatch Act covering state or local government officers and employees might focus on issues including these: whether the availability of federal funds mandates political activity restrictions; whether coercion and patronage would result from a liberalized political activity law; and whether state laws, known as the "little" Hatch Acts, are sufficiently strong to prevent the misuse of government authority.

Selected Source Reading

Boyle, Louis Lawrence. "Reforming Civil Service Reform: Should the Federal Government Continue to Regulate State and Local Government Employees?" Journal of Law and Politics, vol. 7 (winter 1991), pp. 243-288.

CRS Report 97-624 GOV. Federal Restrictions on State or Local Government Officer or Employee Political Activities, by Barbara L. Schwemle (1997). (This CRS report is archived and available from the author of this entry in the compendium.)

Rosenbloom, David H. Federal Service and the Constitution: Development of the Public Employee Relationship. Ithaca: Cornell University Press, 1971.

Snead, John David. "An Inquiry Into the Chilling Effects of Stringent Little Hatch Act Prohibitions," Review of Public Personnel Administration vol. 21 (winter 2001), pp. 259-283.

Commission on Political Activity of Government Personnel. Findings and Recommendations (vol. 1), Research (vol. 2), Hearings (vol. 3). Washington: GPO, 1968.

Office of Special Counsel. Political Activity and the State and Local Employee. Washington: OSC, 2000. (Advisory opinions on application of the law to state and local employees are available at [http://www.osc.gov], visited December 11, 2003.)

Barbara L. Schwemle

(6) Definitions (Chapter 21; in Part III, Subpart A — General Provisions).

Statutory Intent and History

The Pendleton Act of 1883 (22 Stat. 403-407) provides the basis for the definitions of the civil and competitive service terminology still in use today. The act provided that the civil service would be comprised of individuals who had successfully passed competitive examinations. It also provided for specific exceptions and established the President as the officer with the authority to regulate admissions to the civil service. The Homeland Security Act of 2002 (P.L. 107-296; 116 Stat. 2229) and the National Defense Authorization Act for FY2004 (P.L. 108136; 117 Stat. 1621) authorize the creation of new human resources management (HRM) systems for civilian employees of the Departments of Homeland Security and Defense. Both laws stipulate that the Chapter 21 provisions cannot be waived, modified, or otherwise affected by the new HRM systems. (See the discussions of the 5 U.S.C. Chapter 97 and Chapter 99 provisions in this compendium.)

Major Provisions

Sections 2101 through 2109 provide definitions for civil service, armed forces, uniformed services, Senior Executive Service, competitive and excepted services, officer, employee, Member of Congress, congressional employee, veteran, preference eligible, and air traffic controller.

Discussion

Throughout Title 5 there are sections that provide definitions of some of these same categories, particularly of employee and agency. The definitions specifically associated with provisions would govern. However, throughout Title 5, there are cross references to definitions elsewhere in the title. The definition of employee (Section 2105) is probably the most common reference. At other points in Title 5 different definitions are used, and in some instances, it is necessary to follow several references until the specific definition, and its exceptions, become clear. For example, Section 5302 defines employee for the paycomparabilitysystem. Statutory pay system is defined, in part, as a pay system under "Subchapter III, relating to the General Schedule." Section 5331 (definitions under Subchapter III) leads the reader to a cross-reference to the definitions under Section 5102, which is the definitional section for the position classification system. Section 5102 defines employee as "an individual employed in or under an agency," defines agency, and provides a substantial listing of exceptions.

Selected Source Reading

U.S. General Accounting Office. The Excepted Service: A Research Profile. GAO/GGD-97-72. May 1997.

Mitchel A. Sollenberger

---

(7) Merit System Principles (Chapter 23; in Part III, Subpart A — General Provisions).

Statutory Intent and History

The Civil Service Reform Act (CSRA) of 1978 (92 Stat. 1113) is the underlying statute for Chapter 23. The law codifies merit principles and prohibits personnel practices that had previously been expressed in rules, regulations, and executive orders. The legislative history of the CSRA indicates that the statute codified merit system principles for the first time, and required agencies and employees to adhere to them.

Major Provisions

Each agency head is responsible for preventing prohibited personnel practices, for complying with, and enforcing, applicable civil service laws, rules, and regulations, and other aspects of personnel management, and for ensuring that agency employees are informed of the rights and remedies available to them. The law defines personnel actions as: appointments; promotions; adverse actions or other disciplinary or corrective actions; details, transfers, or reassignments; reinstatements; restorations; reemployment; performance evaluations; decisions concerning pay, benefits, or awards, concerning education or training, if such may reasonably be expected to lead to a personnel action; decisions to order psychiatric testing or examination; and any other significant changes in duties, responsibilities, or working conditions. Nine merit system principles and 12 prohibited personnel practices are codified in law and summarized below.

Merit System Principles.

- recruit from qualified individuals to achieve a workforce from all segments of society; selection and advancement solely on the basis of relative ability, knowledge, and skills; assure equal opportunity through fair and open competition;
- fair and equitable treatment of employees and applicants for employment in all aspects of personnel management without regard to political affiliation, race, color, religion, national origin, sex, marital status, age, or handicapping condition, and with proper regard for their privacy and constitutional rights;
- equal pay for work of equal value, with appropriate consideration of both national and local rates paid by employers in the private sector, and appropriate incentives and recognition for excellence in performance;
- employee adherence to high standards of integrity, conduct, and concern for the public interest;
- efficient and effective use of the federal workforce;
- retain employees on the basis of the adequacy of their performance; correct inadequate performance; and separate those who cannot or will not improve performance to meet required standards;

- provide employees effective education and training to improve organizational and individual performance;
- protect employees against arbitrary action, personal favoritism, or coercion for partisan political purposes, and prohibit the use of official authority or influence to interfere with or affect the result of an election or a nomination for election;
- protect employees against reprisal for the lawful disclosure of information reasonably believed to evidence a violation of any law, rule, or regulation, or mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety.

Prohibited Personnel Practices.

- discriminating for or against any employee or applicant for employment on the basis of race, color, religion, sex, national origin, age, handicapping condition, marital status, or political affiliation;
- soliciting or considering any recommendation or statement, oral or written, with respect to any individual who requests, or is under consideration for, any personnel action unless such recommendation or statement is based on the personal knowledge or records of the person furnishing it, and consists of an evaluation of the work performance, ability, aptitude, or general qualifications of such individual, or an evaluation of the character, loyalty, or suitability of such individual;
- coercing the political activity of any person (including the providing of any political contribution or service) or taking any action against any employee or applicant for employment as a reprisal for the refusal of any person to engage in such political activity;
- deceiving or willfully obstructing any person with respect to such person's right to compete for employment;
- influencing any person to withdraw from competition for any position for the purpose of improving or injuring the prospects of any other person for employment;
- granting any preference or advantage not authorized by law, rule, or regulation to any employee or applicant for employment (including defining the scope or manner of competition or the requirements for any position) for the purpose of improving or injuring the prospects of any particular person for employment;
- appointing, employing, promoting, advancing — or advocating such – in or to a civilian position any individual who is a relative of such employee if such position is in the agency in which such employee is serving as a public official or over which such employee exercises jurisdiction or control as an official;
- taking or failing to take, or threatening such, a personnel action with respect to any employee or applicant for employment because of any

disclosure of information, including to the Special Counsel[1041] or an agency Inspector General, by the individual which he or she reasonably believes evidences a violation of any law, rule, or regulation, or gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety; provided the disclosure is not specifically prohibited by law and if such information is not specifically required by executive order to be kept secret in the interest of national defense or the conduct of foreign affairs;

- taking or failing to take, or threatening such, any personnel action against any employee or applicant for employment because of the exercise of any appeal, complaint, or grievance right granted by any law, rule, or regulation; testifying for, or otherwise lawfully assisting, any individual in the exercise of any right referred to above; cooperating with or disclosing information to, the Inspector General of an agency, or the Special Counsel, in accordance with the law; or for refusing to obey an order that would require the individual to violate a law;
- discriminating for or against any employee or applicant for employment on the basis of conduct which does not adversely affect the performance of the individual or the performance of others; except this shall not prohibit an agency from taking into account, in determining suitability or fitness, any conviction of the employee or applicant for any crime under federal, state, or District of Columbia law;
- knowingly taking, recommending, or approving, or failing to do such, any personnel action if the taking of, or failing to take, such action would violate a veterans' preference requirement;
- taking or failing to take any other personnel action if such would violate any law, rule, or regulation implementing, or directly concerning, the merit system principles.

Discussion

No substantive amendments have been made to the merit system principles since their codification in 1978. Concerning the prohibited personnel practices, however, significant amendments have been made. In 1993, the Hatch Act Reform Amendments (107 Stat. 1001) expressly prohibited a Member of Congress from making a recommendation on behalf of an applicant for federal employment, except as to character and the residence of the individual. In 1996, this prohibition was ended by restoring the language first enacted in 1978 (110 Stat. 2395). There is currently no specific prohibition on Members' recommending or referring applicants for federal positions or federal personnel actions. In 1998, the prohibition relating to violation of the veterans' preference

[1041] The Special Counsel heads the Office of Special Counsel (OSC), a federal agency. See the discussion of 5 U.S.C. Chapter 12 for more information on the OSC.

requirement was added in the Veterans Employment Opportunities Act of 1998 (112 Stat. 3187).

H.R. 5512, introduced in the 106th Congress, would have added a 13th prohibited personnel practice related to the implementation or enforcement of any nondisclosure policy, form, or agreement. The bill also would have amended the eighth prohibited personnel practice to clarify the disclosures covered. No further action occurred on the bill. Similar legislation (H.R. 2588 and S. 995) was introduced in the 107th Congress and is pending in the 108th Congress (H.R. 3281, Whistleblower Protection Enforcement Act; and S. 1229 and S. 1358, Federal Employee Protection of Disclosures Act).

At the request of the Administration, legislation (S. 1495) was introduced in the 105th Congress to require the federal appeals court to hear every appeal from a Merit Systems Protection Board (MSPB) decision brought by OPM (currently the court has discretion to decide whether or not to hear OPM petitions). Additionally, the legislation would have granted OPM 60 days to file a petition for review rather than the current 30 days. In a hearing on the bill, OPM justified its request for the amendments by saying that it was in a better position than the court to judge the impact of erroneous MSPB and arbitration decisions and that the 60-day time frame was the same as that for government appeals from the Federal Labor Relations Authority. The Justice Department and the National Academy of Public Administration supported OPM's views. Representatives of the National Treasury Employees Union, the American Federation of Government Employees, and the National Federation of Federal Employees opposed the amendments. Among their comments were these: that the federal circuit should retain its discretion (a system of checks and balances) as appeals were only to be granted in exceptional circumstances; that the other parties to a case have only 30 days to appeal; that arbitration decisions are nonprecedential cases; and that courts make and are qualified to make decisions about whether an appeal should be heard in every case. No further action occurred on the bill.

In the 108th Congress, legislation (H.R. 2867 and S. 1440, Federal Bureau of Investigation (FBI) Reform Act of 2003) is pending to amend 5 U.S.C. § 2303 to increase the protection for FBI whistleblowers. Similar legislation (S. 1974) was introduced in the 107th Congress.

The Homeland Security Act of 2002 (P.L. 107-296; 116 Stat. 2229) and the National Defense Authorization Act for FY2004 (P.L. 108-136; 117 Stat. 1621) authorize the creation of new human resources management (HRM) systems for civilian employees of the Departments of Homeland Security and Defense. Both laws stipulate that the Chapter 23 merit system principles and prohibited personnel practices cannot be waived, modified, or otherwise affected by the new HRM systems. (See the discussions of the 5 U.S.C. Chapter 97 and Chapter 99 provisions in this compendium.)

By law, the Office of Personnel Management is to execute, administer, and enforce the civil service laws and rules and regulations and conduct oversight of any personnel management authorities which it delegates to agency heads. Under its strategic plan, mandated by P.L. 103-62, the Government Performance and Results Act, one of OPM's FY2004 goals is to "monitor and assess agencies' effectiveness in implementing merit-based strategies that support their mission." OPM's FY2004 budget request allocated $16,070,000 (out of a total of $120,246,000) and 136 (out of a total of 796) full-time equivalent employees to carrying out this goal.

MSPB, by law, is required to submit an annual report to the President and Congress which includes an analysis of "whether the actions of OPM are in accord with merit system principles and free from prohibited practices." Its July 1998 report found that OPM's reorganized oversight program had improved; it enjoyed a high degree of top-management support within OPM and was seen as having value to the agencies. Among MSPB's recommendations for further improvement were that evaluation needs to be more consistent in the field divisions, information obtained through oversight needs to be better used and disseminated, and oversight of line managers needs to occur. Recommendations focused on OPM's leadership and coordination in developing human resource management evaluation standards. MSPB's December 2001 report found that OPM's oversight program "seems to have been given the appropriate amount of attention and support," is funded entirely by appropriated funds, and "is sound." The report included recommendations that OPM actively influence "broad-based regulatory or statutory changes where feasible" and "be an active participant in decisionmaking regarding HR [human resources] policies and programs."

Selected Source Reading

Ingraham, Patricia Wallace. The Foundation of Merit: Public Service in American Democracy. Baltimore, MD: Johns Hopkins University Press, 1995.

Pfiffner, James P. and Douglas A. Brook, eds. The Future of Merit: Twenty Years After the Civil Service Reform Act. Washington: Woodrow Wilson Center Press, 2000.

Van Riper, Paul P. History of the United States Civil Service. Evanston, IL: Row, Peterson and Company, 1958.

U.S. Congress. House. Committee on Post Office and Civil Service. Subcommittee on Manpower and Civil Service. History of Civil Service Merit Systems of the United States and Selected Foreign Countries Together with Executive Reorganization Studies and Personnel Recommendations. Committee print 9429. 94th Congress, 2nd session. Washington: GPO, 1976.

Congress. House. Committee on Post Office and Civil Service. Legislative History of the Civil Service Reform Act of 1978. Commitment print. 96th Congress, 1st session. Committee Print 96-2. Washington: GPO, 1979.

Congress. Senate. Committee on Governmental Affairs. Subcommittee on International Security, Proliferation, and Federal Services. Merit System Protection Act of 1997. Hearing. 105th Congress, 2nd session. Washington: GPO, 1998.

CRS Report 96-913A. Recommendations by Members of Congress on Behalf of Applicants for Federal Employment, by Jack H. Maskell (1996). (This CRS report is archived and available from the author of this entry in the compendium.)

U.S. Merit Systems Protection Board. Civil Service Evaluation, The Evolving Role of the U.S. Office of Personnel Management, A Report Concerning Significant Actions of the U.S. Office of Personnel Management. Washington: MSPB, 1998.

——. The U.S. Office of Personnel Management in Retrospect; Achievements and Challenges After Two Decades. Washington: MSPB, 2001.

Barbara L. Schwemle

(8) Authority for Employment (Chapter 31; in Part III, Subpart B — Employment and Retention).

Statutory Intent and History

In addition to the 1966 Title 5 codification statute (P.L. 89-554; 80 Stat. 378), the basic statutes for Chapter 31, "Authority for Employment," include the Postal Revenue and Federal Salary Act of 1967 (P.L. 90-206; 81 Stat. 613), the Civil Service Reform Act of 1978 (P.L. 95-454; 92 Stat. 1111), the Federal Employees Pay Comparability Act (FEPCA) of 1990 (P.L. 101-509; 104 Stat. 1427), and a 1988 amendment to Title 5 authorizing the establishment of the Federal Bureau of Investigation (FBI) and the Drug Enforcement Administration (DEA) Senior Executive Service (P.L. 100-325; 102 Stat. 579). The Homeland Security Act of 2002 (P.L. 107-296; 116 Stat. 2229) and the National Defense Authorization Act for FY2004 (P.L. 108-136; 117 Stat. 1621) authorize the creation of new human resources management (HRM) systems for civilian employees of the Departments of Homeland Security and Defense. Both laws stipulate that the Chapter 31 provisions cannot be waived, modified, or otherwise affected by the new HRM systems. (See the discussions of the 5 U.S.C. Chapter 97 and Chapter 99 provisions elsewhere in this compendium.)

Most recently, Congress amended Chapter 31 to streamline the hiring process for the Securities and Exchange Commission (SEC) with the Accountant, Compliance, and Enforcement Staffing Act of 2003 (P.L. 108-44; 117 Stat. 842) in the wake of unfolding financial market scandals. Following a series of corporate accounting scandals that began with Enron in late 2001, Congress moved to increase the size and budget of the SEC, the federal agency that regulates corporate securities markets. From $438 million in FY2002, the SEC's annual appropriation was increased to $716.3 million for FY2003, and then to $811.5 million for FY2004. The increases were to fund about 900 new professional staff positions, including a substantial number of accountants, examiners, and economists, in addition to the hiring made necessary by staff turnover. The SEC estimated that the FY2003 budget would result in the hiring of 200 lawyers, 250 accountants, 300 examiners, 10 economists, and some other specialists. As FY2003 came to a close, however, the SEC reported that it had been unable to fill many of these jobs and, as a result, $103 million of its appropriation was unspent. Time-consuming hiring procedures and rules that apply to the federal competitive service were considered a major reason for the delay.

Major Provisions

The chapter generally mandates agency hiring of personnel, and also enumerates specific hiring authorizations, restrictions, and prohibitions affecting federal employment. For instance, there are provisions to assist blind and deaf federal employees in the performance of their duties, as well as restrictions on hiring and using attorneys; hiring publicity experts; accepting student volunteers; and using experts and consultants. The employment of private detectives and the appointment of relatives by public officials are prohibited.

The Accountant, Compliance, and Enforcement Staffing Act of 2003 added a new Section 3114 to Subchapter I of Chapter 31. The SEC is authorized to appoint accountants, economists, and securities compliance examiners to competitive service positions by following the procedures that apply to the excepted service. Positions thus filled are not to be considered excepted service positions. The statute directs the SEC to submit two reports to congressional committees describing its exercise of this authority. The initial report is due 90 days after the end of FY2003; the second, 90 days after the end of FY2005.

The purpose and composition of the Senior Executive Service (SES) is specified. Creation of the SES was a key component of the Civil Service Reform Act of 1978. The SES is a corps of top managers and administrators in the federal service encompassing approximately 7,000 positions formerly in General Schedule grades 16-18 and certain positions formerly in Executive Schedule levels IV and V. The SES includes career and political civil servants, with a limit of 10% on noncareer members. It emphasizes mobility, managerial discretion in assignments, accountability and performance of a very high order, and a reward system based on managerial excellence, risk-taking, and initiative.

The chapter also authorizes a separate Senior Executive Service for the FBI and the DEA within the Department of Justice, independent of the government-wide SES, but closely paralleling its pay, performance, and removal provisions. Requirements for an annual report to Congress on the FBI-DEA Senior Executive Service are also set forth.

Discussion

The chapter reflects both evolving trends in the federal workforce and enduring precepts. Provisions concerning work station access for the disabled as well as assistance for handicapped federal employees are recent chapter additions intended to prevent discrimination based on employee disability, and closely parallel similar protections found in the Americans with Disabilities Act (104 Stat. 327, as amended, 105 Stat. 1077, at 1095) applying to the private sector. In both instances, unencumbered entrances, walkways, ramps, and the like are required, along with specially adapted office machinery to assist employees in fulfilling their work potential.

The specified employment prohibitions, on the other hand, are long-standing. The anti-nepotism provision, together with prohibitions on employment of publicity experts and private detectives, reflect rather permanent attitudes about certain public proprieties in federal employment not necessarily paramount in the private sector.

With regard to the SEC provisions, the persistence of corporate and financial scandals in the headlines created a sense of urgency in Congress for reinforcing federal securities regulation. The bill that became P.L. 108-44 (H.R. 658) passed

the House by a vote of 423-0 on June 17, 2003, and was approved without amendment by unanimous consent in the Senate two days later. The legislative history contains no arguments against the concept of streamlined appointment authority for the SEC. However, in the report accompanying H.R. 658 (H.Rept. 108-63), 24 minority members of the House Financial Services Committee expressed the view that the authority should be temporary and supported a sunset date at the end of FY2008. The final version of the legislation makes the expedited hiring authority permanent. The Office of Personnel Management (OPM) did not comment on similar language in hearings on H.R. 1836 in May 2003 before the House Committee on Government Reform. On June 20, 2003, one day after the Senate passed H.R. 658, OPM Director Kay Coles James issued a memorandum stating, among other things, that direct-hire authority[1042] would be available to the SEC for two years to appoint accountants, economists, and securities compliance examiners "to respond to Congressional interest and to help the agency meet its mandate to fill in excess of 800 positions."[1043]

The Senior Executive Service provisions of the Civil Service Reform Act of 1978 were, originally, the most important contribution of this landmark legislation. Since its creation, the SES has continued to be challenged by several major issues. The National Commission on the Public Service took note, in its 2003 report, of problems affecting the SES, such as the inclusion of scientists, other professionals, and technical specialists in the SES, and a compensation and reward system that has failed to function properly. The commission recommended dividing the SES into a Professional and Technical Corps (PTC) and an Executive Management Corps (EMC), and advised that more attention should be paid to developing strong management talent within the federal government. Another issue is the lack of diversity found within the senior executive ranks. A comprehensive report by the General Accounting Office (GAO) documenting the extent of diversity within the SES noted that workforce planning, notably succession planning, could be used by agencies to enhance diversity. In 2003, OPM launched an SES candidate development program, which was presented as an initiative to aid in the development of a high-quality SES that reflects the diversity of America.

The 20th anniversary of the SES in 1998 prompted an examination of the service by OPM and other interested parties. OPM issued, in April 1998, "An Outline of OPM's Proposed Framework for Improving the Senior Executive Service." The Senior Executives Association (SEA) responded to this document in June 1998, and an OPM- and SEA-sponsored survey of SES members was completed in

---

[1042] See the discussion of 5 U.S.C. Chapter 33 in this compendium for more about direct-hire authority, which was enacted by the Homeland Security Act of 2002.

[1043] U.S. Office of Personnel Management, Memorandum for Heads of Executive Departments and Agencies, and Chief Human Capital Officers, "New Human Resources Flexibilities — Direct Hire Authority," June 20, 2003.

1999. These efforts sought to reinforce the concept of a senior executive corps and improve the recruitment and retention of senior executives. Major problems and issues currently facing the Senior Executive Service are pay compression, retirement and succession planning, the proliferation of separate cadres of senior executives at selected agencies, mobility, restructuring, and performance management.

Selected Source Reading

Huddleston, Mark W. Whither the SES? Toward a Higher Civil Service for America: Background Paper for the Twentieth Century Fund New York: Twentieth Century Fund, 1986.

Laurent, Anne. "SES: New/Improved! Concentrated!: Executives in Lather over Plans to Change Senior Executive Service." Government Executive, vol. 30 (June 1998), pp. 18-26.

National Academy of Public Administration, Paths to Leadership: Executive Succession Planning in the Federal Government. A Report by a Panel of the National Academy of Public Administration. Washington: NAPA, 1992.

National Commission on the Public Service, Rebuilding the Public Service Washington: National Commission on the Public Service, 1989.

——. Urgent Business for America. Revitalizing the Federal Government for the 21st Century. Washington: Brookings Institution, 2003.

Congress. House. Committee on Financial Services. Accountant, Compliance, and Enforcement Staffing Act. Report to accompany H.R. 658. 108th Congress, 1st session. H.Rept. 108-63. Washington: GPO, 2003.

Congress. House. Committee on Financial Services. Subcommittee on Capital Markets, Insurance, and Government-Sponsored Enterprises. H.R. 658 — The Accountant, Compliance, and Enforcement Staffing Act of 2003, and H.R. 957

— The Broker Accountability Through Enhanced Transparency Act of 2003. Hearing. 108th Congress, 1st session, March 6, 2003. Washington: GPO, 2003.

U.S. Congress. House. Committee on Government Reform. Instilling Agility, Flexibility and a Culture of Achievement in Critical Federal Agencies: A Review of H.R. 1836, The Civil Service and National Security Personnel Improvement Act of 2003. Hearing. 108th Congress, 1st session, May 6, 2003. Washington: GPO, 2003.

U.S. General Accounting Office. Senior Executive Service: Enhanced Agency Efforts Needed to Improve Diversity as the Senior Corps Turns Over. GAO-0334. January 2003.

U.S. Office of Personnel Management. Office of Executive and Management Policy, Human Resources Development Group. Executive Succession Planning Conference Report. Washington: GPO, 1992.

L. Elaine Halchin
Mark Jickling (SEC-related history)
Clinton T. Brass (SEC personnel provisions)

(9) Examination, Selection, and Placement (Chapter 33; in Part III, Subpart B — Employment and Retention).

Statutory Intent and History

The basic statutory authorities contributing to the provisions of Chapter 33, "Examination, Selection, and Placement," are the 1966 Title 5 codification statute (80 Stat. 378) and the Civil Service Reform Act of 1978 (92 Stat. 1111). Additional provisions derive from a 1967 law providing for the acquisition of career status by certain temporary federal employees (81 Stat. 273); the Intergovernmental Personnel Act of 1970 (84 Stat. 1920); a 1972 amendment to Title 5 providing a career program for and greater flexibility in the management of air traffic controllers (86 Stat. 141 at 142); the Department of Defense Authorization Act, 1986 (99 Stat. 777); the Whistleblower Protection Act of 1989 (103 Stat. 32); the Ethics Reform Act of 1989 (103 Stat. 1756); and the Homeland Security Act of 2002 (P.L. 107-296; 116 Stat. 2229). In recent years, there have been statutes which removed groups of employees from hiring processes managed by the Office of Personnel Management. Policymakers in the Internal Revenue Service, Federal Aviation Administration, and Federal Bureau of Investigation have been granted specific authority to design and implement new systems for selected groups of staff. The Homeland Security Act of 2002 and the National Defense Authorization Act for FY2004 (P.L. 108-136; 117 Stat. 1621) authorize the creation of new human resources management (HRM) systems for civilian employees of the Departments of Homeland Security and Defense. Both laws stipulate that the Chapter 33 provisions cannot be waived, modified, or otherwise affected by the new HRM systems. (See the discussions of the 5 U.S.C. Chapter 97 and Chapter 99 provisions in this compendium.)

The chapter provides certain general conditions for federal employment and also outlines the basic elements of a merit-based civil service system. It includes provisions dealing with competitive and noncompetitive examinations; probationary employment periods; and prohibitions on political influence and offering any recommendation regarding merit system employment, advocacy of the overthrow of the government, and participating in a strike or asserting the right to strike.

Major Provisions

Chapter 33 provides general authority to the President for examination, certification, and appointment in the federal civil service. The President is mandated to prescribe rules for entry into competitive service, for competitive and noncompetitive examinations, and for the probationary period before the appointment becomes final. Political recommendations from Members of Congress and others are prohibited, although competitive appointment based on service in the legislative and judicial branches is allowed under certain conditions.

In addition to general conditions of federal employment, specific conditions of employment governing certain classes of federal employees are given, including those for air traffic controllers, law-enforcement officers, public safety personnel, reemployed annuitants, retired military personnel, and members of the Senior Executive Service (SES). Aspects of employment affecting these classes, such as age limits, veterans' preference, credit for prior military service, promotion policy, and disability credits and preference, are enumerated.

The responsibilities of the Office of Personnel Management (OPM), as the central personnel agency, are detailed, including conducting examinations for the competitive service, maintaining and certifying from a competitive service register of eligibles, prescribing rules governing appointment to positions classified above GS-15, and keeping and making public a government-wide list of vacant positions in the competitive service.

Key provisions of the chapter relate to the inter- and intra-agency detailing of federal employees, as well as detailing to state and local government entities, including limitations on length of details; responsibilities and obligations of detailees accruing special benefits from certain assignments; protection of pay, benefits, and seniority while on detail; and provisions governing injury and death while on detail. On September 9, 2003, OPM published proposed regulations relating to the detail of executive branch employees to the legislative branch (68 FR 53054). The regulations propose to limit such details to 180 days with one additional period of up to 180 days and to limit the activities in which executive branch employees could engage. During consideration of the Transportation and Treasury Appropriation Bill FY2004 (H.R. 2989), the Senate agreed by voice vote to an amendment (No. 1949) offered by Senator Charles Grassley that would prohibit any funds appropriated or made available under the act from being used to implement the regulations. In a March 12, 2003, memorandum to human resources directors, OPM's Associate Director for Human Capital Leadership and Merit Systems Accountability requested that executive branch agencies provide OPM with information about the use of interagency details as part of their workforce strategies.[1044]

Provisions governing the SES are elaborated, including the creation and mission of executive resource, qualification review, and performance review boards within the SES. Specific attention is devoted to aspects of SES employment such as assignment and reassignments and appropriate notice pertaining thereto, career development, and sabbaticals. S. 2651, introduced in the 107th Congress, would have amended 5 U.S.C. § 3132 to establish a new appointment in the SES, simply known as "limited," which would have replaced limited term and limited emergency appointments and to allow limited appointees who meet certain

[1044] U.S. Office of Personnel Management, Memorandum for Human Resources Directors, "Number of Agency Details," Mar. 12, 2003.

conditions to fill career-reserved positions. Sections 3394 and 3395 would have been amended to vary the duration of appointments, extensions, and reassignments and transfers for limited appointees according to the type of SES position a limited appointee filled. Any limited appointee would not have been allowed to serve more than seven consecutive years in any combination of limited appointments. No further action occurred on the bill. In the 108th Congress, the NASA Flexibility Act of 2003, as passed by the Senate (S. 610) and as reported to the House of Representatives (H.R. 1085), includes similar provisions.

Section 1321 of the Homeland Security Act of 2002 repealed the Title 5, United States Code, recertification requirement for senior executives (for agencies that are subject to this chapter of the title; i.e., much of the executive branch) and struck from 5 U.S.C. § 3393 the reference to a senior executive being removed for failure to be recertified.

The Homeland Security Act also amended the Title 5, United States Code, process for hiring in the competitive service (again, for much of the executive branch). Section 1312 of the law amended 5 U.S.C. § 3304(a) by adding a new paragraph (3) providing authority for agencies to appoint, without regard to 5 U.S.C. §§ 3309-3318, candidates directlyto positions for which public notice has been given and OPM has determined that there exists a severe shortage of candidates or there is a critical hiring need. (This authority is often called "direct-hire" authority.) OPM regulations must prescribe criteria for identifying such positions and may delegate authority to make determinations under such criteria.[1045] Section 1312 of the law also added a new Section 3319 — Alternative Ranking and Selection Procedures to Title 5, United States Code. OPM, or an agency which has been delegated examining authority, may establish category rating systems for evaluating applicants for positions in the competitive service. Applicants may be evaluated under two or more quality categories based on merit, consistent with OPM regulations, rather than be assigned individual numerical ratings. Within each quality category, applicants who are eligible for veterans' preference must be listed ahead of applicants who are not eligible for preference. Except for applicants for scientific and professional positions at GS-9 (equivalent or higher), each applicant who is a veteran with a compensable service-connected disability of 10% or more must be listed in the highest quality category.

An appointing official may select any applicant in the highest quality category, or, if fewer than three candidates have been assigned to the highest quality category, in a merged category consisting of the highest and the second highest quality categories. The appointing official may not pass over a preference eligible in the

---

[1045] U.S. Office of Personnel Management, Memorandum for Heads of Executive Departments and Agencies, and Chief Human Capital Officers, "New Human Resources Flexibilities — Direct Hire Authority," June 20, 2003.

same category from which selection is made, unless the requirements of 5 U.S.C. § 3317(b) or § 3318(b), as applicable, are satisfied. Each agency that establishes a category rating system must submit, in each of the three years following this establishment, a report to Congress on the system that must include information on the number of employees hired under the system; the system's impact on the hiring of veterans and minorities, including those who are American Indian or Alaska Native, Asian, Black or African American, and native Hawaiian or other Pacific Islander; and the way in which managers were trained in the administration of the system. OPM published regulations to implement the provisions on June 13, 2003 (68 FR 35265).

Discussion

Examination, selection, and placement provisions in federal civil service law illuminate many key elements and potentially critical stress points in the operation of the personnel system. These include probation, anti-politicization, age limits for certain classes of employment, temporary duty assignments, detailing of employees, veterans preference, loyalty provisions, and prohibitions on the right to strike.

The one-year probationary period for new federal employees has engendered controversy over the years, as have legislative proposals to modify it. Proposals to grant appellate rights to those denied tenure after one year, raise probationary employee benefits, and increase the probationary time from one to three years have all been proposed, but not accepted into law.

Although the statutory limitation on temporary service is three years, abuses of this provision have long been reported, with many instances of individuals complaining of far longer periods of service in temporary status.

The practice of detailing federal employees, notably those from executive branch agencies to the White House, has been a recurring problem for many years. Critics allege that detailed employees have been used to enhance the President's political agenda, and that the number of detailees at work in the White House at any given time is difficult to ascertain because of incomplete or inaccurate reporting.[1046]

Maximum age requirements for federal law enforcement officers and air traffic controllers have raised questions regarding the utility, equity, and possible adverse effects of these limits. The arbitrary loss of highly skilled professionals,

[1046] See, for example, U.S. General Accounting Office, Personnel Practices: Federal Employees Detailed from DOD to the White House, GAO/GGD-88-33, 1988; U.S. General Accounting Office, Personnel Practices: Schedule C and Other Details to the Executive Office of the President, GAO/GGD-93-14, Nov. 1992.

for instance, may be more costly to the agency than any benefits resulting from a reduced workforce.

Appointment, reassignment, transfer, and development in the SES have been repeatedly criticized over the years. Entry into the SES has long been viewed as unduly restricted and haphazard by many career SES candidates. Reassignment, transfer, and mobility programs, regarded as key elements in the reform legislation creating the SES, have been considered a signal failure, since the overwhelming proportion of career SES begin and end their careers in the same agency. Performance appraisal programs have also been found wanting, since only a small number of SES members have ever been faulted for inadequate performance. SES members themselves have long criticized the service for perceived deficiencies in compensation and management, political interference, and low morale.

Selected Source Reading

U.S. General Accounting Office. The Excepted Service: A Research Profile. GAO/GGD-97-72. May 1997.

——. Human Capital: Opportunities to Improve Executive Agencies' Hiring Processes. GAO-03-450. May 2003.

——. IRS Personnel Flexibilities: An Opportunity to Test New Approaches. GAO/T-GGD-98-78. May 12, 1998.

——. Review of Veterans' Preference and the 'Rule of 3.' GAO-03-966R. August 22, 2003.

U.S. Merit Systems Protection Board. Office of Policy and Evaluation. Assessing Federal Job-Seekers in a Delegated Examining Environment. Washington: MSPB, 2001.

——. Competing for Federal Jobs; Job Search Experiences of New Hires. Washington: MSPB [2000].

——. Entering Professional Positions in the Federal Government. Washington: MSPB, 1994.

——. The Federal Selection Interview; Unrealized Potential. Washington: MSPB, 2003.

——. Help Wanted; A Review of Federal Vacancy Announcements. Washington: MSPB, 2003.

——. The 1984 Report on the Senior Executive Service. Washington: MSPB, 1984.

——. The Rule of Three in Federal Hiring: Boon or Bane? Washington: MSPB, 1995.

——. The Senior Executive Service, Views of Former Federal Executives. Washington: GPO, 1989.

Sharon S. Gressle
Barbara L. Schwemle

(10) Part-Time Career Employment Opportunities (Chapter 34; in Part III, Subpart B — Employment and Retention).

Statutory Intent and History

The Federal Employees Part-Time Career Employment Act of 1978 (92 Stat. 1055; 5 U.S.C. §§ 3401-3408) is intended to encourage the use of part-time career employment by requiring all agencies to establish programs for increased part-time career employment opportunities. Proponents of the legislation argued that it would benefit the federal government, and therefore the country at large, as well as a substantial segment of the potential workforce. The federal government would benefit from a system of permanent part-time employment that could tap the talents of many citizens who were not seeking employment because they were either unwilling or unable to work full-time schedules. It was also contended that part-time schedules would benefit several pools of potential employees. These would include women whose family commitments made them unable to work full time; handicapped individuals with the potential for making considerable contributions but who were physically unable to work a 40-hour week; and senior citizens who could bring broad experience to the workplace during a transitional period leading to retirement.

The Homeland Security Act of 2002 (P.L. 107-296; 116 Stat. 2229) and the National Defense Authorization Act for FY2004 (P.L. 108-136; 117 Stat. 1621) authorize the creation of new human resources management (HRM) systems for civilian employees of the Departments of Homeland Security and Defense. Both laws stipulate that the Chapter 34 provisions cannot be waived, modified, or otherwise affected by the new HRM systems. (See the discussions of the 5 U.S.C. Chapter 97 and Chapter 99 provisions in this compendium.)

Major Provisions

Part-time career employment is defined as part-time employment of 16 to 32 hours a week under a schedule consisting of an equal or varied number of hours per day, whether in a position which would be part-time without regard to the statute or one established to allow job-sharing or comparable arrangements. The provisions of the statute do not apply to persons paid at rates equal to the minimum rate of pay for senior-level personnel (5 U.S.C. § 3405(b)). The provisions do not include employment on a temporary or intermittent basis. Federal agencies and the Office of Personnel Management (OPM) are required to establish, maintain, and periodically review the part-time employment program. Representation by employee organizations is allowed.

Discussion

For a period of at least one year prior to enactment of the 1978 statute, federal agencies had been actively exploring the possibilities of increased part-time employment programs. President Carter, in 1977, had instructed the agencies to

establish innovative programs for the purpose of expanding part-time opportunities. During the year before enactment, the number of part-time permanent workers in the federal system increased by about 20%, from 43,000 to 51,000. At the time of enactment, permanent part-time employment constituted over 2.7% of the permanent federal workforce. According to OPM, as of March 2003, permanent part-time employees made up 5.74% of the federal civilian workforce.

Selected Source Reading

Employee Benefits Research Institute. Characteristics of the Part-Time Work Force: Analysis of the March 1993 Current Population Survey. Issue Brief 149. Washington: EBRI, 1994.

U.S. Congress. Senate. Committee on Governmental Affairs. Subcommittee on Governmental Efficiency and the District of Columbia. Status of Implementation of the Part-Time Career Employment Act of 1978. Hearings. 96th Congress, 2nd session. Washington: GPO, 1980.

Kevin R. Kosar

(11) Retention Preference, Voluntary Separation Incentive Payments, Restoration, and Reemployment (Chapter 35; in Part III, Subpart B — Employment and Retention).

Statutory Intent and History

The Veterans' Preference Act of 1944 (58 Stat. 388) and the Civil Service Reform Act of 1978 (92 Stat. 1149) are the underlying statutes for employee retention during reduction in force (RIF). Senior Executive Service (SES) provisions are authorized by the Civil Service Reform Act of 1978 (92 Stat. 1165), except for those on RIFs in the SES, which are authorized by provisions of the Omnibus Budget Reconciliation Act of 1981 (95 Stat. 756); furloughs in the SES, which are authorized by the Civil Service Retirement Spouse Equity Act of 1984 (98 Stat. 3220); and repeal of the SES recertification process, which is provided by the Homeland Security Act of 2002 (P.L. 107-296; 116 Stat. 2229). Voluntary separation incentive payments also are authorized for executive branch agencies by the Homeland Security Act of 2002, and for the Smithsonian Institution by the Smithsonian Facilities Authorization Act (117 Stat. 889). The authority for reemployment after service with an international organization derives from the Foreign Assistance Act of 1969 (83 Stat. 825). Reemployment following limited appointment in the Foreign Service is authorized by the Foreign Service Act of 1980 (94 Stat. 2164). The intent of the laws, with regard to reduction in force, was to codify retention practices. The laws confirmed the regulations and practices in effect at the time.

Major Provisions

Retention during reduction in force is based on tenure, military preference, length of service, and efficiency or performance ratings. Sixty days notice of impending RIF action must be given to the affected employee and his or her labor representative.

Chapter 35 includes several provisions relating to the SES. A career appointee to the SES can be removed during the one-year probationary period or at any time for less than fully successful executive performance. A former career appointee may be reinstated in the SES if the probationary period has been successfully completed, and if the appointee left the SES for reasons other than misconduct, neglect of duty, malfeasance, or less than fullysuccessful executive performance. A career appointee who was appointed from a civil service position to the SES and who is removed from the SES during the probationary period for reasons other than misconduct, neglect of duty, or malfeasance may be placed in a civil service position in any agency. Agencies provide competitive procedures for removing employees from the SES during a RIF of career appointees. Determinations are based primarily on performance. Employees in the SES may be furloughed for reasons of insufficient work, or funds or for other nondisciplinary reasons. Final Office of Personnel Management (OPM)

regulations, which became effective on November 13, 2000, detail the SES performance appraisal process (5 CFR Part 430, Subpart C).

The Homeland Security Act of 2002 delegated to OPM authority to review and approve requests from federal executive branch agencies (as defined at 5 U.S.C. § 105) to offer voluntary separation incentive payments of up to $25,000 to employees in particular occupational groups, organizational units, or geographic locations who retire or resign. OPM is to do this in consultation with the Office of Management and Budget (OMB). The authority to offer separation payments ("buyouts") applies across all executive agencies. Buyouts can be used by agencies seeking to reduce their total employment or to reshape their workforce to meet critical agency needs. Agencies seeking approval from OPM must submit a plan that describes the intended use of the buyouts. Payments are to be made from the agencies' regular appropriations for salaries and are subject to all applicable federal, state, and local income taxes. They are not included in the employee's basic pay for purposes of calculating the amount of his or her retirement annuity.

The Smithsonian Facilities Authorization Act allows the Secretary of the Smithsonian Institution to establish a program "substantially similar" to the program established by the Homeland Security Act. However, the law leaves unclear what approval role, if any, OPM or OMB have under this authority.

Provisions on transfer of functions, waiver of physical qualifications for veterans' preference employees, reinstatement or restoration of individuals suspended or removed for national security, and reemployment after service with an international organization or following limited appointment in the foreign service are also included in Chapter 35.

Discussion

In the 104th Congress, H.R. 3841 would have amended the RIF regulations to increase the weight given to performance appraisal in a RIF. The bill would have codified language on granting additional years of service credit. The additional service credit an employee received for performance would have consisted of the sum of the employee's three most recent annual performance ratings — those received during the four-year period prior to the issuance of RIF notices, or the four-year period prior to the agency-established cutoff date. This would have been an important change. Under the current RIF regulations, the additional years of service credit are totaled, averaged, and then added to seniority to determine retention standing. Under H.R. 3841, employees were to receive five, seven, or 10 additional years of service depending on the number of rating levels in their performance appraisal system. H.R. 3841 passed the House of Representatives after the RIF language was struck, but no further action occurred in the 104th Congress. However, during subcommittee hearings on the measure, federal manager and employee organizations testified that the RIF changes would adversely affect employees who were outstanding performers and politicize the

retention system by allowing managers to give high performance ratings to favored employees.

Draft legislation, prepared but not introduced in the 105th Congress, by the House Civil Service Subcommittee chair, Representative Mica, would have authorized employees in agencies facing workforce reductions to volunteer for RIFs. Additionally, the legislation proposed a separate retention register for federal employees with less than "fully successful" performance ratings. According to the draft, this was to ensure that the poor performers would receive less retention consideration in a RIF than good performers with less seniority.

The Homeland Security Act of 2002 (P.L. 107-296; 116 Stat. 2229) and the National Defense Authorization Act for FY2004 (P.L. 108-136; 117 Stat. 1621) authorize the creation of new human resources management (HRM) systems for civilian employees of the Departments of Homeland Security and Defense. Both laws stipulate that the Chapter 35 provisions cannot be waived, modified, or otherwise affected by the new HRM systems. (See the discussions of the 5 U.S.C. Chapter 97 and Chapter 99 provisions in this compendium.) Section 1321 of the Homeland Security Act repealed the recertification requirement for senior executives. A September 1998 OPM report assessing recertification found that more than 99% of executives were recertified; the average cost of recertifying one executive ranged from $34 to $3,400; and 50 reporting agencies spent about 12,600 work hours on recertification, costing them almost $750,000. The Homeland Security Act delegated to OPM authority to review and approve requests from federal agencies to offer voluntary separation incentive payments of up to $25,000 to employees in particular occupational groups, organizational units, or geographic locations who retire or resign.

In an August 1998 report on downsizing in the federal government during the years 1994 to 1996, OPM found that agencies reduced their workforces without massive reductions in force by using such tools as buyouts (79% of the time) and early retirement (72% of the time). RIFs in all executive branch agencies totaled 2,092 (FY2000), 1,586 (FY2001), 1,360 (FY2002), and 286 (1st quarter of FY2003).

OPM published final revised regulations on the use of performance appraisal ratings to determine retention during a RIF in November 1997 (5 CFR § 351.504). The regulations provide for additional years of service credit ranging from 12 to 20 years and specify that only actual performance ratings can be used to determine retention credit. (Under the previous regulations, an employee received 12, 16, or 20 additional years of service credit for "fully successful," "exceeds fully successful," or "outstanding" performance, and a rating of "fully successful" could have been assumed for missing ratings.) Interim regulations, effective on October 20, 2000 clarified the "longstanding policy that an agency determines the grade or grade-interval range of a released employee's potential retreat rights [to another position] solely on the basis of the official position of

record held by the employee on the effective date of the reduction in force" (5 CFR § 351.701(f)).

Selected Source Reading

Glennon, Thomas A. "RIF Procedures — How They Got Here from There." Management, vol. 3 (spring 1982), pp. 14-16.

White, Shelya. "Reduction in Force — Benefit or Detriment? A Look at Some Tangible and Intangible Results of Federal Sector Reductions in Force (RIF)." International Journal of Public Administration, vol. 26, nos. 10 and 11 (2003), pp. 1145-1165.

Congress. House. Committee on Government Reform and Oversight. Omnibus Civil Service Reform Act of 1996. 104th Congress, 2nd session. H.Rept. 104-831. Washington: GPO, 1996.

Office of Personnel Management. An Assessment of Recertification in the Senior Executive Service. Washington: GPO, 1998.

——. Office of Merit Systems Oversight and Effectiveness. Downsizing in the Federal Government, Report of an Oversight Special Study. Washington: OPM, 1998.

——. Workforce Restructuring Office. Restructuring Information Handbook Module 3: Reduction in Force. Washington: OPM, 1998.

——. Workforce Restructuring Office. The Employee's Guide to Reduction in Force (RIF). Washington: OPM, 1999.

——. Workforce Restructuring Office. The Employee's Guide to Benefits for Those Affected by Reduction in Force. Washington: OPM, 1999.

Barbara L. Schwemle
Patrick J. Purcell (buyout authority)

(12) Information Technology Exchange Program (Chapter 37; in Part III, Subpart B — Employment and Retention).

Statutory Intent and History

Chapter 37, which was established by the E-Government Act of 2002 (P.L. 107347), provides for the exchange of information technology (IT) professionals between the public and private sectors.[1047]

The Intergovernmental Personnel Act, P.L. 91-648 (5 U.S.C. §§ 3371-3375), gives agencies authority to exchange personnel with state and local governments, as well as certain nongovernmental organizations, such as institutions of higher education.[1048] The Homeland Security Act of 2002 (P.L. 107-296; 116 Stat. 2229) and the National Defense Authorization Act for FY2004 (P.L. 108-136; 117 Stat. 1621) authorize the creation of new human resources management (HRM) systems for civilian employees of the Departments of Homeland Security and Defense. Both laws stipulate that the Chapter 37 provisions cannot be waived, modified, or otherwise affected by the new HRM systems. (See the discussions of the 5 U.S.C. Chapter 97 and Chapter 99 provisions in this compendium.)

Major Provisions

This chapter authorizes the exchange of information technology personnel between federal government agencies and private sector organizations. Chapter provisions outline eligibility criteria for federal employees and private sector employees, establish the duration of assignments, require an agency to provide a written agreement between the agency and an employee who participates in an exchange, address the employment and benefits status of federal employees and private sector employees who participate in an exchange assignment, and establish the terms and conditions under which an employee of a private sector organization would be employed by a federal agency. This chapter also authorizes the chief technology officer of the District of Columbia to arrange for public-private exchanges of information technology personnel between his or her office and private sector organizations. Any references in Chapter 37 to federal law or regulations are deemed to be a reference to applicable provisions of the District's laws and regulations.

The Office of Personnel Management (OPM) is responsible for prescribing regulations for administering this chapter, and is required to prepare and submit semiannual reports to the Senate Committee on Governmental Affairs and the

---

[1047] 116 Stat. 2899, at 2925; H.R. 2458.

[1048] U.S. Office of Personnel Management, "Intergovernmental Personnel Act Mobility Program," available at [http://www.opm.gov/programs/ipa/], visited Dec. 3, 2003.

House Committee on Government Reform. OPM also is required to provide a report on all existing public-private exchange programs. Additionally, the General Accounting Office (GAO) is required to prepare and submit a report on information technology training programs.

Discussion

This chapter reflects an interest in recruiting and retaining federal government information technology personnel. In a 2001 report, GAO estimated that the demand for IT workers was high in all sectors, and concluded that the federal government and other employers were having trouble getting enough "highly skilled IT workers" to meet the demand.[1049] Additionally, a comparison of federal compensation with compensation offered by state and local governments, non-profit organizations, private business, and academic institutions showed that the federal government was low on salary levels, rewards and recognition, advancement and training, and the use of recruiting tools.[1050] It is anticipated that the exchange program will help meet the training needs of government employees, while offering private sector employees the opportunity for public service.

It is too early to tell the extent to which federal agencies and their employees, as well as private sector organizations and their personnel, will make use of Chapter 37. OPM issued proposed regulations early in 2004 for implementation of this chapter.[1051]

Selected Source Reading

Mervis, Jeffrey. "A Way Out." Government Executive, vol. 35 (February 2003), pp. 54-57.

National Academy of Public Administration. Comparative Study of Information Technology Pay Systems, Executive Summary. Washington: National Academy of Public Administration, 2001.

[1049] U.S. General Accounting Office, Human Capital: Attracting and Retaining a High-Quality Information Technology Workforce, GAO-02-113T, Oct. 4, 2001, p. 3.

[1050] National Academy of Public Administration, Comparative Study of Information Technology Pay Systems, Executive Summary (Washington: National Academy of Public Administration, 2001), p. 10.

[1051] U.S. Office of Personnel Management, "Information Technology Exchange Program," 69 Federal Register 2308, Jan. 15, 2004.

Congress. House. House Committee on Government Reform. E-Government Act of 2002. Report to accompany H.R. 2458. 107th Congress, 2nd session. H.Rept. 107-787, part 1. Washington: GPO, 2002.

General Accounting Office. Human Capital: Attracting and Retaining a High-Quality Information Technology Workforce. GAO-02-113T. October 4, 2001.

General Accounting Office. National Science Foundation: External Assignments under the Intergovernmental Personnel Act's Mobility Program. GAO-01-1016. September 2001.

L. Elaine Halchin

(13) Training (Chapter 41; in Part III, Subpart C — Employee Performance).

Statutory Intent and History

The 1966 Title 5 codification statute (80 Stat. 378) and the Civil Service Reform Act of 1978 (92 Stat. 1111) are the basic authorities for Chapter 41. Additional authority is provided by a 1982 amendment to Title 5 providing training opportunities for employees under the Office of the Architect of the Capitol and the Botanic Garden (96 Stat. 1647). The Federal Workforce Restructuring Act of 1994 (108 Stat. 1111) added language which served to emphasize the need for training so that it benefits not only the individual, but also the organization and assists in achieving agency mission and goals. The Homeland Security Act of 2002 (P.L. 107296; 116 Stat. 2229) and the National Defense Authorization Act for FY2004 (P.L. 108-136; 117 Stat. 1621) authorize the creation of new human resources management (HRM) systems for civilian employees of the Departments of Homeland Security and Defense. Both laws stipulate that the Chapter 41 provisions cannot be waived, modified, or otherwise affected by the new HRM systems. (See the discussions of the 5 U.S.C. Chapter 97 and Chapter 99 provisions in this compendium.)

Federal employee training programs are designed to insure that federal employees maintain and improve their basic job skills and knowledge in order to render maximum service to their agency's mission and to the public at large. To attain this goal, both government-wide and agency-specific instruction programs are offered to keep federal personnel informed and up to date on professional, scientific, and technical developments related to their fields of expertise. Off-site training programs at colleges and universities are also available, provided that the instruction received relates to and enhances employees' performance in their respective occupations. The ultimate objective of government training is to build and retain a workforce of skilled and efficient employees.

Major Provisions

Chapter 41 consists of provisions governing the availability and use of federal training options for federal employees in both government and nongovernment facilities. The costs of training, employee agreements, and federal assistance to defray costs are also addressed.

Federal training is defined as providing for instruction or education options for federal employees or the placement of employees in instruction or education programs to assist in achieving agency mission and performance goals. Certain agencies are excepted from the provisions of the chapter, and the President is authorized to delete or add exceptions, but may not alter the role of the Office of Personnel Management (OPM) in administering training programs.

Agency heads also are granted authority to establish training programs for their employees. They also may contract-out training programs where considered

appropriate and cost-effective. According to OPM, information on the extent of government-wide training programs is not available because of the widespread dispersal of individual in-house and off-site training programs. Government facilities under agency control are to be used for training when practicable, but other government facilities may be utilized on a cost-reimbursable basis.

Section 1331 of the Homeland Security Act (P.L. 107-296) amended Chapter 41 to permit agencies to select and assign employees to academic training and pay or reimburse the costs thereof. Consistent with the merit system principles at 5 U.S.C. §§ 2301 (b)(2) and (7), an agency that exercises this authority must "provide employees effective education and training to improve organizational performance" while taking into consideration "the need to maintain a balanced and integrated federal workforce." Furthermore, 5 U.S.C. § 4107(b)(2) requires agencies to assure that "the training is not for the sole purpose of providing an employee an opportunity to obtain an academic degree or qualify for appointment to a particular position for which the academic degree is a basic requirement." This training may not be made available to members of or those seeking a position in the Senior Executive Service. Agencies are encouraged, "to the greatest extent practicable, [to] facilitate the use of online degree training."

Federal employees availing themselves of training incur certain obligations, including a requirement to serve an appropriate time with the agency after training, and reimburse the cost of training if there is failure to comply. The government is entitled to pursue costs of training as a debt owed to the United States. Specific costs of training payable by the agency are enumerated, including the cost of the training program, travel and per diem costs, transportation of family and household goods, library and laboratory services, and other services.

Discussion

Allegations of waste and mismanagement have appeared in the media against the government-wide federal employee training system. In past years, the system, costing an estimated $25 billion annually, has been criticized for fragmentation, duplication, confusing eligibility criteria, and inadequate reporting. OPM retains an administrative role in training policy development. However, since 1995, the U.S. Department of Agriculture Graduate School has operated several of the training offices and programs that were formerly the responsibility of OPM.

Selected Source Reading

Congress. House. Committee on Government Operations. Simplifying the Maze of Federal Employment Training Programs. Hearing. 103rd Congress, 2nd session. Washington: GPO, 1994.

General Accounting Office. OPM Sets New Tuition Pricing Policy. GAO/GGD-94-120. 1994.

Office of the Vice President. National Performance Review. From Red Tape to Results: Creating a Government That Works Better & Costs Less. Accompanying Report: Giving Federal Workers the Tools They Need to Do Their Jobs: Federal Training. Washington: GPO, 1993.

Kevin R. Kosar

(14) Performance Appraisal (Chapter 43; in Part III, Subpart C — Employee Performance).

Statutory Intent and History

The underlying statute for Chapter 43, "Performance Appraisal," is the Civil Service Reform Act of 1978 (92 Stat. 1131). The law's intent was to mandate agency establishment of performance appraisal systems so that appraisals of employee performance would be made within a single, interrelated system.

Major Provisions

Agency performance appraisal systems are required to (1) provide for periodic appraisals of job performance; (2) encourage employee participation in establishing performance standards; and (3) use performance appraisal results as the basis for training, rewarding, reassigning, promoting, reducing in grade, retaining, and removing employees. Each agency performance appraisal system must include performance standards permitting the accurate evaluation of job performance on the basis of objective criteria. An employee may be reduced in grade or removed because of unacceptable performance. The law provides 30 days' advance written notice to the employee of the proposed action, a "reasonable" time for the employee to answer orally and in writing, and a written decision of the action recommended. The decision to retain, reduce in grade, or remove an employee must be made within 30 days of the notice period's expiration.

Chapter 43 also authorizes agencies to establish performance appraisal systems for the Senior Executive Service (SES). The systems are designed to permit the accurate evaluation of performance, provide for systematic appraisals, encourage excellence in performance, and provide a basis for making eligibility determinations for retention and performance awards. Appraisals in the SES are based on individual and organizational performance. Performance factors include improvements in efficiency, productivity, and quality of work or service, including any significant reduction in paperwork; cost efficiency; timeliness of performance; other indications of the effectiveness, productivity, and performance quality of the employees for whom the senior executive is responsible; and meeting affirmative action goals, achievement of equal employment opportunity requirements, and compliance with merit system principles. SES performance appraisal systems provide annual summary ratings of performance with one or more fully successful levels, a minimally satisfactory level, and an unsatisfactory level.

Discussion

H.R. 3841, proposed in the 104th Congress, but not enacted, would have required that performance appraisal systems assist employees in improving unacceptable performance and provide for reassignment, reduction in grade, removal, or other appropriate action against employees whose performance was unacceptable.

Upon notification of unacceptable performance, an employee would have been afforded a one-time opportunity to demonstrate acceptable performance before a reduction in grade or removal. H.R. 3841 passed the House of Representatives, but no further action occurred. Another measure, H.R. 3483, would have authorized an agency to remove or take other appropriate action against employees whose performance was unacceptable. It also sought to repeal the procedures on reducing the grade of or removing an employee for unacceptable performance. If this latter provision had been enacted, agencies would have had to use the Chapter 75 adverse action procedures to remove poor performers. H.R. 3483 was referred to committee, but no further action occurred.

Draft legislation, prepared but not introduced in the 105th Congress, by the House Civil Service Subcommittee chair, Representative Mica, would have prohibited the appeal of a denied within grade increase to the Merit Systems Protection Board, delayed the establishment of any new "pass/fail" performance management systems until the Office of Personnel Management (OPM) provided an evaluation of the current ones, and allowed for the removal of a problem employee after one performance improvement plan.

Among the comments expressed about performance appraisal during House hearings conducted in the 104th and 105th Congresses were statements that employees should have an opportunity to improve their performance before being separated; that a fundamental problem is the inability to identify sub-par performance in terms of expected contributions; and that the administrative process surrounding performance appraisal is litigious, complex, time-consuming, and provides excessive due process. Differing opinions were expressed on whether pass/fail performance appraisal systems strengthen or degrade performance, whether the weight of performance ratings should be increased in reduction in force, and whether strong enforcement of the current performance appraisal system is required, rather than amendments to the current system.

OPM's human resource management initiatives for 1998 and 1999 included a recommendation that payand performance systems be aligned with agency missions. Vice President Gore, in an address before a January 1999 international conference on reinventing government, said that the Administration would begin drafting civil service legislation that would establish a set of standards providing for flexible payfor-performance systems which each agency could use to create its own system. He said the legislation would also allow agencies to evaluate their managers, including those in the SES, on a balanced set of results, including the GPRA [Government Performance and Results Act] goals, customer satisfaction rates, and the outcome of employee satisfaction surveys, and that these evaluations would guide in setting salaries and paying bonuses for these

managers.[1052] The president of the National Treasury Employees union, in a news release on the Vice President's announcement, stated that fair performance evaluations mandate federal employee involvement in setting and implementing performance measures, while a news release from the Senior Executives Association president expressed concern about evaluating and paying managers on the basis of surveys "address[ing] issues over which career managers and executives have little impact." A legislative proposal was not submitted to the 106th Congress.

The Homeland Security Act of 2002 (P.L. 107-296; 116 Stat. 2229) and the National Defense Authorization Act for FY2004 (P.L. 108-136, 117 Stat. 1621) authorize the creation of new human resources management (HRM) systems for civilian employees of the Departments of Homeland Security (DHS) and Defense (DOD). Both laws permit changes to the Chapter 43 provisions and specify requirements for performance management systems at DHS and DOD. (See the discussions of the 5 U.S.C. Chapter 97 and Chapter 99 provisions in this compendium.) The National Defense Authorization Act for FY2004 also creates a Human Capital Performance Fund to reward the highest performing and most valuable employees in an agency and offer federal managers a new tool for recognizing employee performance that is critical to an agency's achieving its mission. (See the discussion of the 5 U.S.C. Chapter 54 provision in this compendium.)

A September 1995 MSPB issue paper recommended that Chapter 43 authority on performance-based actions be repealed and that RIF laws be amended to permit RIF procedures to be used to remove poor performers. The same month, OPM published regulations providing agencies with increased flexibility to develop their performance appraisal systems. Eight patterns of summary levels of performance may be used. These patterns range from a pass/fail system with two summary levels (unacceptable and fully successful) to a system with five summary levels (unacceptable, less than fully successful, fully successful, exceeds fully successful, and outstanding).

In a draft framework for the Senior Executive Service (SES) published in April 1998, OPM proposed a three-year performance agreement with annual progress reviews. OPM published a status report on the draft framework in December 1998 and proposed administrative rule changes in July 1999 (64 FR 41334). Final OPM regulations on managing senior executive performance, which became effective on November 13, 2000, "will help agencies hold senior executives accountable by: Reinforcing the link between performance management and strategic planning; requiring agencies to use balanced measures in evaluating

---

[1052] National Partnership for Reinventing Government, Vice President Gore Announces Three Reinvention Initiatives at International REGO Forum, Jan. 14, 1999, available at [http://govinfo.library.unt.edu/npr/library/news/011499.html], visited Dec. 23, 2003.

executive performance; and giving agencies more flexibility to tailor performance management systems to their unique mission requirements and organizational climates"[1053] [5 CFR Part 430, Subpart C]. Some agency performance appraisal systems might change as a result of provisions at Section 1125 of the National Defense Authorization Act for FY2004. This statute shifted the cap on basic pay for the SES from Level IV of the Executive Schedule to Level III. However, the cap will be Level II for any agency that is certified as having a performance appraisal system which makes meaningful distinctions based on relative performance. Agencies might have to modify their performance appraisal systems to achieve certification.

Selected Source Reading

CRS Report RS20303. The Senior Executive Service: Overview and Current Issues, by L. Elaine Halchin.

National Academy of Public Administration. Strengthening Senior Leadership in the Government. Washington: NAPA, 2002.

Congress. House. Committee on Post Office and Civil Service. Legislative History of the Civil Service Reform Act of 1978. Committee print. 96th Congress, 1st session. Committee Print 96-2. Washington: GPO, 1979.

Congress. House. Committee on Government Reform and Oversight.

Omnibus Civil Service Reform Act of 1996. H.Rept. 104-831. 104th Congress, 2nd session. Washington: GPO, 1996.

U.S. Merit Systems Protection Board. Federal Supervisors and Poor Performers. Washington: MSPB, 1999.

——. Removing Poor Performers in the Federal Service. Issue Paper. Washington: MSPB, 1995.

U.S. Office of Personnel Management. An Outline of OPM's Proposed Framework for Improving the Senior Executive Service. Washington: OPM, 1998.

——. Status Report Draft Framework, Status Report as of December 1998. Washington: OPM, 1998.

[1053] U.S. Office of Personnel Management, "Managing Senior Executive Performance," Federal Register, vol. 65, no. 199, Oct. 13, 2000, pp. 60837-60845.

——. Office of Merit Systems Oversight and Effectiveness. Report of a Special Study. Poor Performers in Government: A Quest for the True Story. Washington: OPM, 1999.

U.S. Office of the Vice President. National Performance Review. From Red Tape to Results: Creating a Government That Works Better & Costs Less.

(15) Incentive Awards (Chapter 45; in Part III, Subpart C — Employee Performance).

Statutory Intent and History

The basic statutory authorities contributing to the provisions of Chapter 45, "Incentive Awards," are the 1966 Title 5 codification statute (P.L. 89-554; 80 Stat. 378) and the Civil Service Reform Act of 1978 (P.L. 95-454; 92 Stat. 1111). Additional provisions derive from the Omnibus Budget Reconciliation Act of 1981 (P.L. 97-35, Title XVII, Subchapter II; 95 Stat. 755); Treasury, Postal Service, and General Government Appropriations Act of 1991 (P.L. 101-509, § 529; 104 Stat. 1427); the Treasury, Postal Service, General Government appropriation as found in the Omnibus Consolidated and Emergency Supplemental Appropriations for FY1999 (P.L. 105-277, Division A, § 101(h), § 631); and the Treasury and General Government Appropriations Act of 2002 (P.L. 107-67, Title VI, § 641(d); 115 Stat. 554). The Homeland Security Act of 2002 (P.L. 107-296; 116 Stat. 2229) and the National Defense Authorization Act for FY2004 (P.L. 108-136, 117 Stat. 1621) authorize the creation of new human resources management (HRM) systems for civilian employees of the Departments of Homeland Security and Defense. Both laws stipulate that the Chapter 45 provisions cannot be waived, modified, or otherwise affected by the new HRM systems. (See the discussions of the 5 U.S.C. Chapter 97 and Chapter 99 provisions in this compendium.)

Major Provisions

The chapter sets forth provisions governing the range and scope of contributions and services for which federal employees are eligible to receive monetary and non-monetary awards, including suggestions, inventions, performance, and acts of heroism.

Cash incentive awards are available to federal employees, except for those paid under the Executive Schedule, for suggestions, inventions, superior performance, heroism, or ideas to reduce paperwork. Awards are limited to $10,000, except in cases where accomplishment is unusually outstanding, when awards not to exceed $25,000 are authorized with the approval of the Office of Personnel Management (OPM). Cash awards are in addition to regular pay, and acceptance by the employee absolves the government of any further claims involving use of ideas or devices, etc. The President may grant an incentive award, which may be in addition to an agency award. Subject to limitations, the President may grant rank awards to members of the Senior Executive Service (SES) and individuals serving in certain senior-level positions.[1054] Meritorious Executive awards are to equal 20% of annual basic pay, and Distinguished Executive awards are to equal

[1054] Senior-level positions include positions classified above GS-15 pursuant to 5 U.S.C. § 5108 and scientific or professional positions established under 5 U.S.C. § 3104.

35% of annual basic pay. Cash awards of up to 5% of basic pay are authorized for selected federal law enforcement officers, including those of the U.S. Park Police, the Diplomatic Security Service, and probation officers who possess and make use of one or more foreign languages in the performance of official duties.

Federal employees may receive awards for cost savings disclosures, including those to combat fraud, waste, or mismanagement. The amount of these awards may be $10,000 or an amount that equals 1% of agency cost savings attributable to the award, whichever amount is less. Presidential awards of $20,000 for cost savings disclosures are also allowed, but are limited to 50 in a fiscal year.

Discussion

The federal awards program has recognized many outstanding federal employees by granting monetary and non-monetary awards. Each year, OPM publishes an awards brochure providing statistics on the distribution of the awards, as well as their scope and extent.

Over the years, this program, when compared with awards programs in the private sector, has generally been found to be inadequate. Although legislation has been introduced from time to time to expand the scope of the federal awards program, it actually has changed very little.

Probably the greatest criticisms have been that the amounts of the monetary awards are too small; too few awards are given; and they are too concentrated in certain agencies — notably the defense establishment. Cost-savings awards, for instance, are said to be so small in proportion to cost savings generated for agencies that they are minuscule vis-à-vis those considered appropriate in the private sector. The SES rank awards had remained for 20 years at the same established dollar rates until the 1998 legislation, which keyed the awards to a percentage of basic pay. The minimum award increased from $10,000 to $20,460 in 1999.

Certain agency abuses in the granting of awards have also occurred, with some agencies granting none, others granting too many. In addition, questions have arisen periodically about whether agencies have granted awards in lieu of pay raises, particularly during times of pay freezes or budget austerity, thereby circumventing the rationale of the awards program itself.

Selected Source Reading

Office of Personnel Management. Good Ideas. A Users' Guide to Successful Suggestions Programs. Washington: GPO, 1995.

Office of Personnel Management. Incentive Awards: The Changing Face of Performance Recognition. Washington: OPM, March 2000.

Office of Personnel Management. Review of the Granting of Monetary Awards. Washington: GPO, 1993.

Office of the Vice President. National Performance Review. From Red Tape to Results: Creating a Government That Works Better & Costs Less. Washington: GPO, 1993.

L. Elaine Halchin

(16) Personnel Research Programs and Demonstration Projects (Chapter 47; in Part III, Subpart C — Employee Performance).

Statutory Intent and History

The underlying statute for Chapter 47, "Personnel Research Programs and Demonstration Projects," is the Civil Service Reform Act of 1978 (92 Stat. 1185). The law's intent was to provide agencies with authority to experiment with different personnel management methods through demonstration projects.

Major Provisions

The Office of Personnel Management (OPM) is authorized to:

- establish and maintain (and assist in the establishment and maintenance of) research programs to study improved methods and technologies in federal personnel management;
- evaluate the research programs and establish and maintain a program to collect and disseminate to the public information relating to personnel management research and to facilitate the exchange of information among interested persons and entities; and
- provide for an evaluation of demonstration project results and their impact on improving public management.

Prior to OPM's establishment of a personnel management experiment, a project plan must be developed. Contained within this plan are the project's purpose, the types and numbers of employees to be covered, methodology, duration, training program, anticipated costs, and the evaluation methodology and criteria. Aspects of the project which lack specific authority and current laws, rules, or regulations which must be waived in order for the project to be conducted must be specifically described in the plan as well. Once the demonstration project plan is finalized by OPM, it is published in the Federal Register and is the subject of a public hearing. Employees likely to be affected by the experiment, and both the Senate and the House of Representatives, are notified about the proposed project 180 days in advance of its implementation date. Each agency involved must approve the final version of the plan which must also be submitted by OPM to both houses of Congress at least 90 days in advance of the project's effective date.

By statute, the number of active demonstration projects that can be operating simultaneously is limited to 10, and the total number of employees covered is capped at 50,000. An individual demonstration project cannot cover more than 5,000 workers. Each demonstration project runs for five years and terminates before the end of this period. A project may, however, continue beyond this date to the extent necessary to validate the project results.

If OPM or the agency determine that a project imposes substantial hardship on, or is not in the best interests of, the public, federal government, employees, or eligibles, either or both may terminate it.

OPM's annual report to Congress includes a summary of research programs and demonstration projects conducted during the year, the effect of the programs and projects on improving public management and increasing government efficiency, and recommendations of policies and procedures which will improve management and efficiency.

Discussion

In the 104th Congress, H.R. 3841 sought to amend Chapter 47 to make several changes: coverage of a government corporation under a demonstration project; OPM development or approval of a demonstration project plan; solicitation of comments on the project plan, 30-days' notice to affected employees; projects lasting five years; project extensions for up to two years, up to 15 projects; up to five projects covering 5,000 or more individuals, including collective bargaining unit employees in a project, evaluation of the projects, terminating a project, and obtaining congressional approval for making a project permanent. Another bill, H.R. 3483, was similar to H.R. 3841, but would have deleted the requirement for a public hearing, provided 150 days' notice, and included expedited congressional procedures for making a project permanent. H.R. 3841 passed the House of Representatives and H.R. 3483 was referred to committee, but no further action occurred on either bill.

Among the comments on the demonstration project proposals expressed during House hearings were the following views:

- demonstrations projects should help determine whether one system should apply to all employees or each agency should have a system tailored to its needs;
- the number of individuals covered by a demonstration project and the number of demonstration projects should be limited, because they place some federal employees in the precarious position of being test subjects for untried personnel practices;
- consultations should include both managers and supervisors; and
- public hearings on proposed demonstration projects, independent evaluations of demonstration projects and their impact on public management, and OPM annual reports on research and demonstration projects and their effect on improving public management and increasing government effectiveness should be continued.

Discussions about the issue continued in the 105th Congress. Draft legislation, prepared but not introduced by the House Civil Service Subcommittee chair, Representative Mica, would have amended the demonstration project authority to increase the number of demonstration projects authorized at any time from 10

to 15, and to eliminate the restriction of 5,000 employees per demonstration. Additionally, bargaining over wages and benefits would have been prohibited, and "impact and implementation" bargaining would have been limited. During a June 1998 hearing on the draft bill, OPM testified in favor of making demonstration projects permanent after testing and evaluation. (OPM's 1998 and 1999 human resources management initiatives proposed that it be granted this authority.) Two federal employee unions opposed limiting the subjects that could be negotiated between labor and management. The Senior Executives Association supported such bargaining limits and favored limiting to 25,000 the number of employees in an agency who could participate in a demonstration project. The General Accounting Office noted that use of the demonstration project authority has been limited.

Vice President Gore, in an address before a January 1999 international conference on reinventing government, said that the Administration would begin drafting civil service legislation that would establish a set of standards for flexibility in pay, hiring, and retention which each agency could use to create agency-specific systems. Labor and management would mutually agree upon any plan before its implementation. A legislative proposal was not submitted to the 106th Congress.

In the 108th Congress, S. 129, the Federal Workforce Flexibility Act of 2003, as introduced, included amendments to several major features of current law on demonstration projects. The requirements that a public hearing be conducted, that a demonstration project be limited to 5,000 employees, that the number of projects in effect at any one time be limited to 10, and that Congress receive a report on a project's final plan 90 days before a project's effective date would have been removed. The time period required for advance notification of affected employees would have been shortened, and the requirement for advance notification of Congress would have been removed. The provisions were removed from S. 129 during markup by the Senate Committee on Governmental Affairs. (Similar provisions were included in S. 2651 introduced in the 107th Congress.)

In the 108th Congress as well, H.R. 1085, the NASA Flexibility Act of 2003, would amend current law to allow a demonstration project at NASA to cover 8,000 employees rather than 5,000 employees.

The Homeland Security Act of 2002 (P.L. 107-296; 116 Stat. 2229) and the National Defense Authorization Act for FY2004 (P.L. 108-136, 117 Stat. 1621) authorize the creation of new human resources management (HRM) systems for civilian employees of the Departments of Homeland Security and Defense. Both laws stipulate that the Chapter 47 provisions cannot be waived, modified, or otherwise affected by the new HRM systems. (See the discussions of the 5 U.S.C. Chapter 97 and Chapter 99 provisions in this compendium.)

Three demonstration projects have been made permanent, and four have been completed. One at the Department of Commerce, testing pay-for-performance

using broad pay bands, was implemented in March 1998 and modified in September 1999. Another one, covering the civilian acquisition workforce at the Department of Defense and testing streamlined hiring processes and broad pay bands, among other features, had a phased implementation which was completed in October 1999. Demonstration projects are in progress at eight DOD laboratories. Congress authorized a demonstration project for the Internal Revenue Service in the Internal Revenue Service Restructuring and Reform Act of 1998 (112 Stat. 715).

In a 2001 report on lessons learned from the demonstration projects, OPM determined, among other findings, that successfully tested alternative systems and flexibilities should be able to be converted to permanent programs without separate legislation; that agencies need to have an executive champion who will promote, defend, and support an alternative system; that if alternative systems are extended government-wide, there should be flexibility to customize programs; and that the effectiveness of alternative systems needs to be continuously evaluated.

Selected Source Reading

U.S. Congress. House. Committee on Government Reform and Oversight. Omnibus Civil Service Reform Act of 1996. H.Rept. 104-831. 104th Congress, 2nd session. Washington: GPO, 1996.

Congress. House. Committee on Post Office and Civil Service. Legislative History of the Civil Service Reform Act of 1978. Commitment print. 96th Congress, 1st session. Committee Print 96-2. Washington: GPO, 1979.

Merit Systems Protection Board. Federal Personnel Research Programs and Demonstration Projects: Catalysts for Change. Washington: GPO, 1992.

Office of Personnel Management. Demonstration Projects and Alternative Personnel Systems; HR Flexibilities and Lessons Learned. Available at [http://www.opm.gov/demos/index.htm], visited December 11, 2003.

——. Demonstration Projects; Beyond Current Flexibilities. Available at [http://www.opm.gov/demos/index.htm], visited December 11, 2003.

——. Demonstration Projects Evaluation Handbook. Available at [http://www.opm.gov/demos/index.htm], visited December 11, 2003.

——. Demonstration Project Fact Sheets. Available at [http://www.opm.gov/demos/index.htm], visited December 11, 2003.

U.S. Office of the Vice President. National Performance Review. From Red Tape to Results: Creating a Government That Works Better & Costs Less.

Accompanying Reports: Reinventing Human Resource Management. Washington: GPO, 1993.

Barbara L. Schwemle

(17) Agency Personnel Demonstration Project (Chapter 48; in Part III, Subpart C — Employee Performance).

Statutory Intent and History

The Investor and Capital Markets Fee Relief Act (P.L. 107-123; January 16, 2002; 115 Stat. 2390) included "pay parity" provisions that allowed the Securities and Exchange Commission (SEC) to raise the salaries of certain employees to levels comparable to those of federal bank examiners, whose pay ranges from $180,000 to $250,000, depending on the agency. These provisions appear in Section 8 of the legislation, which created a new Chapter 48 in Subpart C of Part III of Title 5, United States Code.

Congress's intent was to address the SEC's difficulty in attracting qualified employees and unusually high staff turnover. The basic problem was that the skills required by the SEC — mastery of securities law and regulation, or detailed knowledge of financial markets — are in high demand on Wall Street, where some of the highest salaries in the world are offered.

The Office of Personnel Management (OPM) opposed the pay parity provisions because of concerns about the fragmentation of personnel systems and adverse effects on the ability of federal employees to move from one agency to another. In a May 15, 2001 letter to Chairman Dan Burton of the House Government Reform Committee, OPM noted that it had approved special pay rates for SEC lawyers, accountants, and examiners in March 2001. The letter recommended that the pay parity provisions not be enacted until the effectiveness of these special pay rates could be assessed, and also called for more study of the SEC pay situation. Chairman Burton also stated that the SEC pay raises should not be enacted without a broad review of the effects on the civil service system.

Estimates of the cost of granting pay parity raises to SEC employees were in the range of $60-$80 million. The Senate version of the FY2002 Commerce-State-Justice appropriations legislation provided $60 million for this purpose, but this provision was not adopted in conference. (The SEC's FY2002 budget was set at $437.9 million.)

The Administration's FY2003 budget requested $466.9 million for the SEC, still not enough to fund pay parity fully. In the wake of the Enron scandal, Congress passed the Sarbanes-Oxley accounting reform legislation (P.L. 107-204; 116 Stat. 745), which included a provision authorizing appropriations of $775 million for the SEC in FY2003. The FY2003 appropriation was finally set at $716.3 million. For FY2004, the conference report provides $811.5 million for the SEC.

Major Provisions

Chapter 48 authorizes the SEC to appoint and fix the compensation of officers, attorneys, economists, examiners, and other employees "as may be necessary" for carrying out its functions. The SEC may set and adjust basic rates of pay for all

employees without regard to the provisions of Chapter 51 or Subchapter III of Chapter 53 of Title 5, United States Code. The SEC may provide additional compensation or benefits to employees if the same types of compensation or benefits are provided by federal bank regulators (agencies referred to under Section 1206 of the Financial Institutions Reform, Recovery, and Enforcement Act of 1989 (12 U.S.C. § 1833 b)). In setting the total amount of compensation for these employees, the SEC is required to consult with the banking agencies and to maintain comparability of pay and benefits.

The SEC is also directed to implement the pay parity provisions in consultation with OPM and in a manner consistent with merit system principles.

Discussion

After Enron and the succeeding wave of corporate accounting scandals, and the revelations of abuses by stock analysts and others in the securities industry, there was little controversy about the need to increase the size and resources of the SEC. In budget terms, the cost of pay parity was rather small compared to the overall increases in SEC appropriations that were enacted post-Enron. On the other side of the issue, arguments in favor of a uniform civil service pay system remained, as did uneasiness about rank-and-file SEC staffers earning more than the President or Vice President. However, with the scandals still fixed in recent memory (and with new investigations, such as those involving mutual funds, continuing to develop), there has been no move to reverse the SEC's pay parity authority. There has been some interest in extending the pay parity provisions to the Commodity Futures Trading Commission (CFTC), which regulates the futures exchanges, but no authorizing legislation has yet advanced in Congress.

Selected Source Reading

Congress. House. Committee on Financial Services. Investor and Capital Markets Fee Relief Act. Report to accompany H. 1088. 107th Congress, 1st session. H.Rept. 107-52, part 1. Washington: GPO, 2001.

Congress. Senate. Committee on Banking, Housing, and Urban Affairs. Saving Investors Money and Strengthening the SEC. Hearing on S. 143. 107th Congress, 1st session, February 14, 2001. S.Hrg. 107-266. Washington: GPO, 2002.

General Accounting Office. Securities and Exchange Commission: Human Capital Challenges Require Management Attention. GAO-01-947. September 2001.

Mark Jickling (SEC-related history)
Clinton T. Brass (personnel provisions)

(18) Classification (Chapter 51; in Part III, Subpart D — Pay and Allowances).

Statutory Intent and History

The current system for classifying and grading most positions in the federal civil service was established under the Classification Act of 1923 (42 Stat. 1488). This statute was the initial systematic attempt to achieve a uniform alignment of jobs and salaries among various federal departments and agencies. The act established the following principles:

- positions covered by the act were to be classified and graded according to their duties and responsibilities;
- the same pay scale was to apply to all positions falling into the same class and grade, regardless of agency;
- the different pay scales and the various classes and grades were to be logically associated so that pay was properly related to work; and
- one agency would be responsible for equalizing and coordinating the classification and grading of positions for all agencies.

The Classification Act of 1949 (63 Stat. 954) maintained the principles set out in 1923, adding that there should be equal pay for equal work, and that the positions be grouped, or classified, in such a way that the position classification system could be used in all phases of personnel administration.

The Internal Revenue Service Restructuring and Reform Act of 1998 (112 Stat. 711), the Homeland Security Act of 2002 (P.L. 107-296; 116 Stat. 2229), and the National Defense Authorization Act for FY2004 (P.L. 108-136, 117 Stat. 1621) allow the Internal Revenue Service (IRS), Department of Homeland Security (DHS), and Department of Defense (DOD) to establish classification systems independent of Chapter 51. (See the discussions of the 5 U.S.C. Chapter 95, Chapter 97, and Chapter 99 provisions, respectively, in this compendium.)

Major Provisions

Four services had been established in 1923: Professional and Scientific; Clerical, Administrative, and Fiscal; Subprofessional; and Crafts, Protective, and Custodial. Under the 1949 act, the newly established General Schedule comprised positions classified under the first three of these services. No similar schedule was established for the fourth service. The 1949 act also added the GS-16, -17, and -18 grades, which became known as the "supergrades" and were later the foundation for the Senior Executive Service under provisions of the Civil Service Reform Act of 1978 (P.L. 95-454; 92 Stat. 1111). These grades were abolished by the Federal Employees Pay Comparability Act of 1990 (FEPCA; P.L. 101-509; 104 Stat. 1427, at 1443).

Discussion

Government-wide classification of positions is an issue that has generated substantial controversy over the course of the last several years. Critics point out the problems of managing an enormous system which is both rigid and cumbersome. On the other hand, if the system is administered consistently, the uniformity of position classification, occupational definition, and grading provide a framework within which staff and positions can transfer from one agency to another. The controversy led to the enactment of statutes allowing the Department of Homeland Security, Department of Defense, and Internal Revenue Service to design classification systems outside of Chapter 51, potentially affecting approximately 30% of the federal civilian workforce.

Even before the Office of Personnel Management (OPM) was dramatically downsized in 1994, there was an effort to vest the responsibility for position classification in the agencies. Among the favorable arguments was that each agency has its own culture, and that human resources managers should be allowed to classify and grade positions according to these cultures. The National Academy of Public Administration was a proponent of this philosophy. Soon after the Academy issued a report to this effect, the Director of OPM held extensive discussions with several leading personnel administrators in federal agencies. It was determined that while the classification system has substantial problems, they are not so dire that a complete overhaul should be undertaken.

Selected Source Reading

Congressional Budget Office. Changing the Classification of Federal White-Collar Jobs: Potential Management and Budgetary Impacts. CBO Papers, July 1991. Washington: CBO, 1991.

General Accounting Office. High-Risk Series: Strategic Human Capital Management. GAO-03-120. January 2003.

Mitchel A. Sollenberger

(19) Pay Rates and Systems (Chapter 53; in Part III, Subpart D — Pay and Allowances).

Chapter 53, "Pay Rates and Systems," provides the statutory basis for several major pay systems within the federal service. This profile of Chapter 53 departs from the compendium's usual format for profiling Title 5 chapters. Rather than present each system's statutory intent, summary of major provisions, and discussion under separate headings, this profile combines these topics under one heading for each pay system. Among the pay systems discussed are the pay comparability system, the General Schedule, the Senior Executive Service, the Executive Schedule, and the prevailing rate (blue collar) system. Systems covered in other titles of the United States Code, but related to the General Schedule, such as those in the foreign service and veterans hospitals, are not discussed.

In addition, the Internal Revenue Service Restructuring and Reform Act of 1998 (112 Stat. 711), the Homeland Security Act of 2002 (P.L. 107-296; 116 Stat. 2229), and the National Defense Authorization Act for FY2004 (P.L. 108-136, 117 Stat. 1621) allow the Internal Revenue Service (IRS), Department of Homeland Security (DHS), and Department of Defense (DOD), respectively, to establish classification and pay systems independent of Chapter 53. (See the discussions of the 5 U.S.C. Chapter 95, Chapter 97, and Chapter 99 provisions, respectively, in this compendium.) The DHS and DOD systems are currently being designed, and it remains to be seen how the pay comparability system and the prevailing rate system will be changed for these agencies.

Pay Comparability System (5 U.S.C. §§ 5301-5307). Prior to 1962, the system of classification of jobs followed the principle of equal pay for equal work within a pay system, but there was no method of equating pay for equal work among the various systems. P.L. 87-793 (76 Stat. 832, at 841), provided that federal salary schedules be based on equal pay for substantially equal work, and on comparability of federal salary rates with those in private industry for the same levels of work. While the comparability principle was in place, Congress continued to legislate the rates of adjustment, perpetuating a salary lag between federal and private sector pay. The Pay Comparability Act of 1970 (84 Stat. 1946) was considered to be the most important pay legislation subsequent to the 1962 statute. The act established a mechanism under which the Bureau of Labor Statistics conducted a survey of private sector salaries, and the President, his agent, and two advisory groups determined the appropriate rate of adjustment for the General Schedule. This rate of adjustment went into effect automatically unless Congress acted to disapprove it, or the President determined that another rate or schedule of implementation was appropriate. The system established under this statute was utilized for almost 20 years. By the time it was amended, the gap between private and federal white collar salaries had widened to over 30%. During the conference on the Treasury, Postal Service, and General Government Appropriations Act for FY1991, a new pay setting mechanism was

crafted. The Federal Employees Pay Comparability Act (FEPCA; 104 Stat. 1429) currently governs the pay policy for most of the federal civilian workforce.

FEPCA continued, with some changes, the mechanism under which rates are to be adjusted for the General Schedule and related systems. The key difference is that the rate of adjustment is to be equal to one-half percent less than the rate of change in the private sector wages and salaries element of the Employment Cost Index for a given period of time. The second principal innovation under FEPCA was the establishment of a system of locality-based payments. Recognizing that the incomparabilities in salaries ranged from a large gap between private and federal salaries in some localities to no gap at all in other localities, Congress determined that there would be an identification of localities and that the rate of adjustment (in addition to the annual national General Schedule adjustment) would be based on salary surveys conducted within these localities. The plan was to bring federal salaries across the country to within 5% of the private sector salaries for comparable occupations in each locality at the end of 10 years.

Because of a wide range of circumstances, the pay setting provisions of FEPCA have never been fully implemented. The mechanisms have been utilized, but policymakers in the executive and legislative branches have determined that the rates of adjustment should be reduced. The result is that there has not been a systematic reduction in the gap between federal and private sector salaries. In a tight job market, and while the government is downsizing, this gap may not have a negative effect on the potential for the government to recruit and retain the personnel needed to reach mission goals. On the other hand, selectively within certain occupations, a hiring crisis could result. The locality pay provisions in FEPCA are written in a manner which requires that if, in any given year, no locality-based payments were allowed, the salary of the individual would fall back to the base rate of the General Schedule. If Congress or the President determined that a locality-based payment were not appropriate, it is assumed that a saved-pay provision would be enacted to protect the current payable rates.

General Schedule (5 U.S.C. §§ 5331-5338). These sections provide the housekeeping elements for the General Schedule. The language relates to defining the scope of positions and agencies to which the pay schedule applies, establishes Office of Personnel Management (OPM) authority for setting minimum pay rates for new appointees and rates of basic pay, and sets out the rules for periodic and special within-grade (or "step") increases. Although these provisions are not controversial in and of themselves, the within-grade provisions could be affected by various proposals to change the pay-for-performance policies within the human resources management arena.

Senior Executive Service (5 U.S.C.§§ 5381-5385). The structure and appointment policies for the Senior Executive Service (SES), established by the Civil Service Reform Act of 1978, are codified in Chapter 33, Subchapter VIII, of Title 5. The National Defense Authorization Act for FY2004 significantly changed the compensation system for the SES. The SES remains essentially a rank-in-person

compensation system, with the general guidelines set forth in the law. SES base compensation ranges from 120% of the minimum pay of a GS-15 to Level II of the Executive Schedule. There is also a system of monetary performance awards which may be accorded to members of the SES. OPM will promulgate regulations under which the range of rates of pay and a rigorous performance management system will be established. Under the new statute, locality pay is no longer available to the SES.

Executive Schedule (5 U.S.C. §§ 5312-5318). The Executive Schedule is a series of five pay levels for officers of the executive branch, most of whom are political appointees subject to the confirmation process. Level Isalaries are primarily for the heads of departments, and Level V salaries apply, generally, to positions such as general counsels and assistant administrators in independent agencies. Generally, when Congress establishes an agency or realigns agency responsibilities, these sections of Title 5 will be amended to reflect the change in salary level for specific positions.

The salary levels are applied to several positions that do not appear on the Executive Schedule. For example, several legislative branch agency officials, such as the Comptroller General and the Librarian of Congress, are paid at rates equal to specified levels of the Executive Schedule.

The Executive Schedule was established under the provisions of the Government Employees Salary Reform Act of 1964 (P.L. 88-426; 78 Stat. 400). Previously, Congress had been setting salaries for positions as they were created. The statute brought salaries into alignment for the various officers of the executive branch. Congress continued to legislate salary increases for these positions. From 1975 until 1990, salaries were adjusted under the Executive Cost of Living Adjustment Act of 1975 (89 Stat. 419). Salaries for Members of Congress and judges were also adjusted under the same provisions. Although the salaries were to be adjusted at the same rate and time as the General Schedule, Congress usually voted to deny the increases. Under the Ethics Reform Act of 1989 (103 Stat. 1716), as amended, there is to be an annual adjustment based on the increase in private sector wages and salaries, minus one-half percent. The adjustment cannot be more than 5%, and it cannot exceed the rate of adjustment for the base pay of General Schedule salaries. Since 1993, there have been five adjustments, with 2.2% scheduled as an adjustment in January 2004.

Under statute (81 Stat. 613, at 642, as amended by 78 Stat. 400), there is to be a quadrennial review of federal officials' salaries, with subsequent recommendations by the President to Congress. However, the Citizens' Commission on Public Service and Compensation has not been activated since the most recent review in FY1988.

Prevailing Rate System (5 U.S.C. §§ 5341-5349). Since the late 19th century, skilled (blue-collar) federal employees have been paid on the basis of the prevailing wage rates for similar occupations in specific geographic areas. While

there existed a general statutory authority for the Civil Service Commission (now Office of Personnel Management) to set blue-collar salaries, there was no specific statutory language covering wage administration. The Federal Wage System was established in 1972 (86 Stat. 564).

A wage survey is conducted in each of the 135 wage areas in the United States by the agency in the area which is the lead federal blue-collar employer, usually the Department of Defense. Adjustments in wage rates are staggered throughout the year, depending on the timing of the surveys. Historically, it was administratively possible to maintain consistent and equitable salary relationships between the federal and private sector skilled labor forces.

However, since 1978, Congress has limited federal blue-collar salaries to a maximum adjustment rate equal to the General Schedule rate of adjustment. The result is that, while federal wages in some areas have kept pace with those in the private sector, federal wages in high cost areas have not done so. One of the reasons Congress found it necessary to place caps on these wages is that many of the supervisors are General Schedule employees. Allowing blue-collar wages to advance while white-collar salaries were limited would result in line employees being paid more than supervisory staff. Most interested parties have long acknowledged that there are significant flaws in the Federal Wage System, but remedial proposals have not been forthcoming.

Miscellaneous. The other sections of this chapter of Title 5 apply to grade retention policy (generally under a reduction in force), pay policy related to student employees, and special occupational pay systems established by OPM. The 1990 FEPCA statute also established pay systems for administrative law judges, contract appeals board members, and senior-level positions (those graded above GS-15, but not in the Senior Executive Service). The act also provided a means of identifying critical positions and of setting salary levels for these positions. Under the Homeland Security Act of 2002 (P.L. 107-296; 116 Stat. 2229), the limitation of total aggregate annual compensation was increased from Level I of the Executive Schedule to the salary of the Vice President. Agencies may apply these provisions only after OPM has certified that the agency has an appropriate appraisal system in place.

<u>Selected Source Reading</u>

Advisory Committee on Federal Pay. The Bottom Line on Federal Pay — The Gap Became a Canyon. Washington: 1989.

Congressional Budget Office. Comparing the Pay of Federal and Nonfederal Executives: An Update. Washington: CBO, 2003.

——. Measuring Differences Between Federal and Private Pay. Washington: CBO, 2002.

General Accounting Office. Federal Pay: Private Sector Salary Differences by Locality. GGD-91-63FS, B-236949. May 1991.

President's Panel on Federal Compensation. Staff Report of the President's Panel on Federal Compensation. Washington: GPO, 1976.

Mitchel A. Sollenberger

(20) Human Capital Performance Fund (Chapter 54; in Part III, Subpart D — Pay and Allowances).

Statutory Intent and History

Title XI, Subtitle C of the National Defense Authorization Act for Fiscal Year 2004 (117 Stat. 1641; P.L. 108-136, Section 1129) amends Part III, Subpart D of Title 5, United States Code by adding a new Chapter 54 entitled "Human Capital Performance Fund." (The provisions were also included in H.R. 1836, 108th Congress, as reported.) The legislation states that the purpose of the provisions is to promote better performance in the federal government. The fund is to reward the highest performing and most valuable employees in an agency and offer federal managers a new tool for recognizing employee performance that is critical to an agency's achieving its mission. A $500 million Human Capital Performance Fund was proposed by President George W. Bush in his FY2004 budget to create and reinforce the value of pay systems based on performance. The Consolidated Appropriations Act, 2004 (P.L. 108-199; 118 Stat. 3, at 339), provided a $1 million appropriation for the fund, with several provisos.

Major Provisions

Organizations eligible for consideration to participate in the fund are executive departments, government corporations, and independent agencies. The General Accounting Office is not covered by the chapter. The fund may be used to reward General Schedule, Foreign Service, and Veterans Health Administration employees; prevailing rate employees; and employees included by OPM following review of plans submitted by agencies seeking to participate in the fund. However, Executive Schedule (or comparable rate) employees; SES members; administrative law judges; contract appeals board members; administrative appeals judges; and individuals in positions which are excepted from the competitive service because of their confidential, policy-determining, policy-making, or policy-advocating character are not eligible to receive payments from the fund.

OPM will administer the fund, which is authorized a $500,000,000 appropriation for FY2004. Such sums as may be necessary to carry out the provision shall be authorized for each subsequent fiscal year. In the first year of implementation, $50,000,000 (up to 10% of the appropriation) is authorized to be available to participating agencies to train supervisors, managers, and other individuals involved in the appraisal process on using performance management systems to make meaningful distinctions in employee performance and on using the fund.

Agencies seeking to participate in the fund must submit plans to OPM for approval. The plans must incorporate the following elements:

- adherence to merit principles under 5 U.S.C. § 2301;
- a fair, credible, and transparent performance appraisal system;

- a link between the pay-for-performance system, the employee performance appraisal system, and the agency's strategic plan;
- a means for ensuring employee involvement in the design and implementation of the pay-for-performance system;
- adequate training and retraining for supervisors, managers, and employees in the implementation and operation of the pay-for-performance system;
- a process for ensuring ongoing performance feedback and dialogue among supervisors, managers, and employees throughout the appraisal period, and setting timetables for review;
- effective safeguards to ensure that the management of the pay-for-performance system is fair and equitable and based on employee performance; and
- a means for ensuring that adequate agency resources are allocated for the design, implementation, and administration of the pay-for performance system.

An agency will receive an allocation of monies from the fund once OPM, in consultation with the Chief Human Capital Officers (CHCO) Council, reviews and approves its plan. (The CHCO Council will include an evaluation of the formulation and implementation of agency performance management systems in its annual report to Congress.) Ninety percent of the remaining amount appropriated to the fund ($405,000,000, monies not yet appropriated) may be allocated to the agencies. An agency's prorated distribution may not exceed its prorated share of executive branch payroll. (Agencies must provide OPM with necessary payroll information.) If OPM were not to allocate an agency's full prorated share, the remaining amount would be available for distribution to other agencies.

Ten percent of the remaining amount appropriated to the fund ($45,000,000, monies not yet appropriated), as well as the amount of an agency's prorated share not distributed because of the agency's failure to submit a satisfactory plan, will be allocated among agencies with exceptionally high-quality plans. Such agencies will be eligible to receive a distribution in addition to their full prorated distribution.

Agencies, in accordance with their approved plans, may make human capital performance payments to employees based on exceptional performance contributing to the achievement of the agency mission. In any year, the number of employees in an agency receiving payments may not be more than the number equal to 15% of the agency's average total civilian full-time and part-time permanent employment for the previous fiscal year. A payment may not exceed 10% of the employee's basic pay rate. The employee's aggregate pay (basic, locality pay, human capital performance pay) may not exceed Executive Level IV ($134,000 in 2003).

A human capital performance payment is in addition to annual pay adjustments and locality-based comparability payments. Such payments are considered basic pay for purposes of Civil Service Retirement System, Federal Employees' Retirement System, life insurance, and for such other purposes (other than adverse actions) which OPM determines by regulation. Information on payments made and the use of monies from the fund must be provided by the agencies to OPM as specified.

Initially, agencies shall use monies from the fund to make the human capital performance payments. In subsequent years, continued financing of previously awarded payments shall be derived from other agency funds available for salaries and expenses. Under current law at 5 U.S.C. § 5335, agencies pay periodic within-grade increases to employees performing at an acceptable level of competence. Presumably, funds currently used to pay within-grade increases could be used to make human capital performance payments instead. Monies from the fund may not be used for new positions, for other performance-related payments, or for recruitment or retention incentives.

OPM shall issue regulations to implement the new Chapter 54 provisions. Those regulations must include criteria governing:

- an agency's plan;
- allocation of monies from the fund to the agencies;
- the nature, extent, duration, and adjustment of, and approval processes for, payments to employees;
- the relationship of agency performance management systems to the Human Capital Performance Fund;
- training of supervisors, managers, and other individuals involved in the process of making performance distinctions; and
- the circumstances under which funds could be allocated by OPM to an agency in amounts below or in excess of the agency's pro rata share.

Discussion

The effectiveness of agency performance management systems and whether the performance ratings would be determined according to preconceived ideas of how the ratings would be arrayed across the particular rating categories are among the concerns expressed by federal employees and their unions and representatives about the fund. Other concerns are that the fund could take monies away from the already reduced locality-based comparability payments and that the performance award amounts would be so small as not to serve as an incentive (this may be of particular concern given the FY2004 appropriation of $1 million).

Selected Source Reading

Congress. Conference Committees, 2003. Making Appropriations for Agriculture, Rural Development, Food and Drug Administration, and Related Agencies for the Fiscal Year Ending September 30, 2004, and for Other Purposes. Conference Report to Accompany H.R. 2673. H.Rept. 108-401. 108th Congress, 1st session. Washington: GPO, 2003, pp. 253, 763.

Congress. Conference Committees, 2003. National Defense Authorization Act for Fiscal Year 2004. Conference Report to Accompany H.R. 1588. H.Rept. 108-354. 108th Congress, 1st session. Washington: GPO, 2003, pp. 339, 1026.

Barbara L. Schwemle

(21) Pay Administration (Chapter 55; in Part III, Subpart D — Pay and Allowances).

Statutory Intent and History

For the most part, the pay administration provisions in Title 5 reflect practices put in place in the early to mid-20th century through various statutes. The practices authorized in these sections, such as the bi-weekly pay period, enable the federal government to administer the various pay systems. The Homeland Security Act of 2002 (P.L. 107-296; 116 Stat. 2229) and the National Defense Authorization Act for FY2004 (P.L. 108-136, 117 Stat. 1621) authorize the creation of new human resources management (HRM) systems for civilian employees of the Departments of Homeland Security and Defense. Both laws stipulate that the Chapter 55 provisions cannot be waived, modified, or otherwise affected by the new HRM systems, except that, for the Department of Defense, Subchapter V of the chapter, "Premium Pay," may be waived, modified, or otherwise affected by the new HRM system, apart from Section 5545b ("Pay for firefighters").

Major Provisions

Many of the sections in this chapter focus on the managerial details of pay administration. These include the identification of bi-weekly and monthly pay periods, the various bases for withholding pay, payment for accumulated and accrued leave, payments to missing employees, and settlement of accounts. Also included in this chapter are premium pay provisions and the policy for dual pay and dual employment. Statutes enacted to provide civilian agencies with buyout authority are found as notes to 5 U.S.C. § 5597, "Separation Pay."

Discussion

Chapter 55 comprises provisions that define the "bread and butter" administrative processes through which federal employees are compensated. Recently the overtime cap was raised and flexible spending accounts were established. Dual pay and dual employment provisions set out the rules under which a retired member of the armed forces working as a federal civilian employee receives reduced retirement pay.

Overtime Cap. The National Defense Authorization Act of FY2004 amended 5 U.S.C. § 5542 to provide that an employee whose basic pay rate exceeds GS-10, Step 1, will receive overtime at a rate which is the greater of one-and-one-half times the hourly rate for GS-10, Step 1, or his or her hourly rate of basic pay. Overtime compensation has been limited to GS-10, Step 1, to the disadvantage of personnel whose hourly rate of basic pay exceeded this limit.

Pre-tax Employee Benefits. The federal government, like many other public and private employers, offers its employees a choice of pre-tax benefits through a cafeteria plan (defined in 26 U.S.C. § 125). To provide pre-tax benefits, a

cafeteria plan must offer employees the choice of cash or one or more qualified benefits, and cannot discriminate among employees on the basis of compensation. The benefits are pre-tax in that they reduce income for calculation of income and employment taxes.

Although there is no specific authority for federal agencies to offer a flexible benefits plan to employees, under 5 U.S.C. § 5525, agency heads may make allotments from employee pay as they think appropriate. The Office of Personnel Management operates the federal program, known as FedFlex, and currently offers employees[1055] a choice of one (or more) of three pre-tax benefits: payment of health insurance premiums (premium conversion); a health care flexible spending arrangement; and a dependent care flexible spending arrangement.

Federal retirees are not eligible to participate in the flexible benefit program or to have their health insurance premiums paid on a pre-tax basis. Legislation has been introduced in each session of Congress, since premium conversion began, to permit federal retirees to pay health insurance premiums on a pre-tax basis.

Premium Conversion. Beginning in October 2000, federal employees automatically have health insurance premiums (paid by the employees) taken from their income on a pre-tax basis. That is, for calculation of income and employment taxes, an employee's income is reduced by the value of the insurance premiums. This has been called "premium conversion" because the health insurance premiums were converted from a post-tax to a pre-tax basis, saving the employee the income and employment taxes that previously would have been imposed on the value of the health insurance premium. Employees do have the option of electing out of the premium conversion.

Flexible Spending Arrangements. Beginning in 2003, federal employees are able to set aside funds for health and dependent care expenses on a pre-tax basis through a program of flexible spending arrangements known as FSAFEDS. A flexible spending arrangement for health (or dependent) care reimburses an employee for eligible expenses not covered by health insurance (or for dependent care expenses). Dependent care expenses reimbursed through a flexible spending arrangement are not eligible expenses for the dependent care tax credit, and for tax purposes there is a maximum of $5,000 in dependent care expenses that can be paid through an employer-provided reimbursement arrangement. The limitations on the amount of income an employee can set aside in a health care reimbursement account are determined by the employer. For federal employees, in 2004, the maximum that can be set aside in a health reimbursement account is $4,000. P.L. 108-126 provided that any

[1055] Agencies that are not part of the executive branch may choose to offer the FedFlex program. Therefore, not all federal employees are eligible for participation in FedFlex, and some employees are not eligible for all the FedFlex benefits.

administrative fees associated with the flexible spending arrangements are paid by the federal agency and not the employee. In addition, any unused FSA funds revert to the plan administrator and not to the employee.

Selected Source Reading

General Accounting Office. Sunday Premium Pay: Millions of Dollars in Sunday Premium Pay Are Paid to Employees on Leave. GAO/GGD-95-144. May 1995.

President's Panel on Federal Compensation. Staff Report of the President's Panel on Federal Compensation, "Chapter VII Premium Pay." Washington: GPO, 1976.

Office of Personnel Management, The Federal Flexible Benefits Plan ("FedFlex"), available at the OPM website, [http://www.opm.gov/insure/health/pretaxfehb/fedflex.pdf], visited January 6, 2004.

Office of Personnel Management, The Flexible Spending Account Program Overview 2004, OPM-FSA-OVTF-10-03, available at the FSAFEDS administrators website: [https://www.fsafeds.com/forms/OPM-FSA-OVTF-10-031.pdf], visited January 6, 2004.

Mitchel A. Sollenberger (general pay administration)
Christine Scott (pre-tax benefits)

(22) Travel, Transportation, and Subsistence (Chapter 57; in Part III, Subpart D — Pay and Allowances).

Statutory Intent and History

Chapter 57, "Travel, Transportation, and Subsistence," provides for the payment of various travel, transportation, and subsistence expenses, including those for new and transferring employees; overseas travel; and transportation of family, household goods, personal effects, and privately owned vehicles. Reiterating policy set by the Travel Expense Act of 1949 (P.L. 81- 92, 81st Congress; 63 Stat. 166) and codified in 1966 (P.L. 89-554; 80 Stat. 378), only actual and necessary travel expenses are allowed. The Homeland Security Act of 2002 (P.L. 107-296; 116 Stat. 2229) and the National Defense Authorization Act for FY2004 (P.L. 108-136, 117 Stat. 1621) authorize the creation of new human resources management (HRM) systems for civilian employees of the Departments of Homeland Security and Defense. Both laws stipulate that the Chapter 57 provisions cannot be waived, modified, or otherwise affected by the new HRM systems. (See the discussions of the 5 U.S.C. Chapter 97 and Chapter 99 provisions in this compendium.)

Major Provisions

Provisions of Chapter 57 provide details regarding allowances permitted for travel, transportation, and subsistence expenses. Typical of the provisions are those governing the transportation of an employee's immediate family and household goods and personal effects when the employee is transferred to a post to which the family is not permitted to accompany him or her for military or other reasons. Per diem allowances, travel expenses, and storage allotments are authorized in this chapter as well.

Other policies established by Chapter 57 include provision for the traveling expenses of the President and mileage allowances for Members of Congress. Relocation allowances for employees, including the conditions to be met by agencies entering into contracts with private firms in support of these allowances, and payment of expenses to obtain professional credentials are included.

Discussion

Most of Chapter 57 has not been amended for more than a decade. The Joint Financial Management Improvement Project (JFMIP), in a 1995 report, made a number of recommendations on travel management. One such recommendation was that a government-issued charge card should be used for all travel-related expenses. Cost savings of $62 million were anticipated. P.L. 105-264, enacted on October 19, 1998, address this recommendation by requiring the use of the federal travel charge card for payment of all official government travel expenses to the maximum extent practicable. Other provisions of the law include authorizing the government to collect financial information needed to verify that charges on the card are business related, and providing that employees whose

charge payments are overdue will have the delinquent amounts deducted from their paychecks. Concerns about fraud, waste, and abuse in the use of travel cards by federal employees prompted Congress to act. Two statutes that apply only to Department of Defense (DOD) personnel include provisions dealing with travel card management. Section 1008 of P.L. 107-314[1056] amends 10 U.S.C. § 2784 by inserting a section on the disbursement of travel allowances and offsets for delinquent travel card charges. Provisions in Section 1009 of P.L. 108-136 also address the disbursement of travel allowances, determinations of creditworthiness, and penalties for misusing travel cards.

The JFMIP also recommended improvements in automating and auditing travel data. P.L. 105-264 establishes requirements for prepayment audits of federal agency transportation expenses to verify that charges are correct. The General Services Administration (GSA) estimates that this will save $50 million per year. Efforts to further automate and audit travel will likely continue.

With the passage of P.L. 107-107, [1057] the National Defense Authorization Act for FY2002, federal employees who receive promotional items, such as frequent flier miles, as a result of official government travel may keep and use the promotional items. Section 1116 of P.L. 107-107 applies to any items received before, on, or after the date of enactment (December 28, 2001).

Through the use of contractors, GSA is establishing an online travel system, the eTravel Service (eTS). The Web-based system will include all aspects of travel, including authorizing travel, making reservations, filing travel claims, and reconciling vouchers. A proposed rule requires federal agencies to begin implementing eTS no later than December 31, 2004. GSA's system is separate from DOD's online travel management system, the Defense Travel System (DTS), which began operating in 2003.

GSA annually adjusts per diem rates for payment of lodging and meals during official government travel within the continental United States. Effective October 1, 2000, changes in the per diem rates occur at the start of the fiscal year. Effective January 1, 1999, federal employees are reimbursed for all local taxes on hotel room charges (in the past, taxes were not always reimbursed). Incidental expenses for laundry and dry cleaning will not be reimbursed for short-term travel of less than four days.

Following the Internal Revenue Service's increase in its standard mileage reimbursement rate, from 36 cents to 37.5 cents per mile for 2004, the

---

[1056] 116 Stat. 2458, at 2634.

[1057] 5 U.S.C. § 5702 note; 115 Stat. 1012, at 1241.

Administrator of General Services, who sets the reimbursement rate for all federal employees, also increased the GSA rate to 37.5 cents per mile.[1058]

Selected Source Reading

U.S. Congress. House. Committee on Government Reform and Oversight. Subcommittee on Government Management, Information and, Technology.

H.R. 3637, Travel Reform and Savings Act of 1996. Hearing on H.R. 3637. 104th Congress, 2nd session, July 9, 1996. Washington: GPO, 1997.

U.S. Congress. Senate. Committee on Governmental Affairs. Travel and Transportation Reform Act of 1997. 105th Congress, 2nd session. S.Rept. 105-295. Washington: GPO, 1998.

U.S. General Services Administration. "Federal Travel Regulation: eTravel Service (eTS)." Federal Register, vol. 68, no. 125 (June 30, 2003), pp. 38661-38665.

U.S. Joint Financial Management Improvement Program, Improving Travel Management Governmentwide. Washington: GPO, 1995.

L. Elaine Halchin

[1058] The mileage reimbursement rate established by the General Services Administration cannot exceed the rate established by the Internal Revenue Service (5 U.S.C. § 5704).

(23) Allowances (Chapter 59; in Part III, Subpart D — Pay and Allowances).

Statutory Intent and History

This chapter, with a few subsequent modifications, derives from the statute codifying Title 5 in 1966 (80 Stat. 378). It provides for payment of various allowances to cover the costs of specific expenses outside of those normally expected or to enhance recruitment and retention.

Major Provisions

General allowance provisions include those for living quarters for personnel stationed in foreign countries; differential cost-of-living allowances (COLAs) for personnel living in high-cost areas such as Alaska; "danger pay" to be given to personnel assigned to areas where war conditions or other threatening elements are present; incentive allowances for physicians; and other cost-of-living and uniform allowances.

Discussion

Non-foreign area cost-of-living allowances and physicians' comparability allowances are frequently examined by executive branch administrators, Members of Congress, and federal employees to ensure that the intent of the authorizing statutes is carried out.

The Office of Personnel Management's (OPM) Special COLA Research Announcement (see "Selected Source Reading," below) in July 2000 provided the following information:

The Government pays nonforeign area COLAs to approximately 44,000 Federal white-collar and U.S. Postal Service employees in Alaska, Hawaii, Guam, the Commonwealth of the Northern Mariana Islands, Puerto Rico, and the U.S. Virgin Islands. COLA rates reflect differences in living costs between the allowance areas and the Washington, DC, area. OPM conducts surveys in the COLA areas and in the Washington, DC, area to determine COLA rates. The law limits COLAs to no more than 25 percent of basic pay .... Since 1991, OPM's surveys conducted using the existing methodology have indicated that, using this methodology, COLA rates would have been reduced in several allowance areas. This has raised concerns relating to the COLA methodology. Since 1991, Congress has barred COLA rate reductions. The bar is in effect through December 31, 2000. Congress also required OPM to study and submit a report on the COLA program and the compensation of Federal employees in the COLA areas. Since 1996, the Government and the plaintiffs have engaged in a cooperative effort under [a memorandum of understanding]. This cooperative effort led to a proposed settlement of Caraballo, et al. v. United States, No. 1997-0027 (D.V.I.), a case brought in the District Court of the Virgin Islands.

The settlement, which the court approved on August 17, 2000, formed the basis for new regulations for the COLA program. OPM published proposed regulations to significantly modify the COLA methodology consistent with the court agreement on November 9, 2001 (66 FR 56741). The final regulations were published on May 3, 2002 (67 FR 22339). Current COLA rates are: in Alaska, 25% (Anchorage, Fairbanks, Juneau, and rest of the state); in Hawaii, 25% (Honolulu), 16.5% (Hawaii County), 23.25% (Kauai County), and 23.75% (Kalawao and Maui Counties); in Guam and the Commonwealth of the Northern Mariana Islands, 25%; in Puerto Rico, 11.5%; and in the U.S. Virgin Islands, 22.5%.

Federal physicians may receive up to $30,000 per year as a physicians' comparability allowance (PCA). The allowance had been reauthorized every three years. In the 106th Congress, the Federal Physicians Comparability Allowance Amendments of 2000 (114 Stat. 3054) permanently authorized the comparability allowance and treated it as part of basic pay for retirement purposes. In FY2000 (actual data), 47% of all eligible physicians, or 1,521 physicians, received a PCA and the average PCA paid was $17,889. For FY2001, approximately 1630 physicians (48% of all those eligible) received a PCA.

In the 107th Congress, the National Defense Authorization Act FY2002 (115 Stat. 1238) amended current law to provide hostile fire pay of $150 per month in certain circumstances. During the same Congress, the Foreign Relations Authorization Act FY2003 (116 Stat. 1380) amended current law with regard to the baggage allowance and to provide an allowance to Foreign Service employees who are outside their countries of employment and require medical treatment in specific circumstances.

The Homeland Security Act of 2002 (P.L. 107-296; 116 Stat. 2229) and the National Defense Authorization Act for FY2004 (P.L. 108-136, 117 Stat. 1621) authorize the creation of new human resources management (HRM) systems for civilian employees of the Departments of Homeland Security and Defense. Both laws stipulate that the Chapter 59 provisions cannot be waived, modified, or otherwise affected by the new HRM systems. (See the discussions of the 5 U.S.C. Chapter 97 and Chapter 99 provisions in this compendium.)

Selected Source Reading

Federal Physicians Association. 2001 Presidential Report on the Physicians' Comparability Allowance Program , available at [http://www.fedphy.org/pay_reports.htm], visited December 11, 2003.

U.S. Office of Personnel Management, "Nonforeign Area Cost-of-Living Allowances," Special COLA Research Announcement, available at [http://www.opm.gov/oca/cola/html/cola-n.htm], visited December 11, 2003. See also the COLA Settlement Litigation website at [http://www.colasettlement.com/], visited December 11, 2003.

Barbara L. Schwemle

(24) Hours of Work (Chapter 61; in Part III, Subpart E — Attendance and Leave).

Statutory Intent and History

The 1966 Title 5 codification statute (80 Stat. 378), the Civil Service Reform Act of 1978 (92 Stat. 1111), and the Federal Employees Flexible and Compressed Work Schedules Act of 1982 (96 Stat. 227) are the basic authorities contributing to the hours of work provisions of Chapter 61. The Homeland Security Act of 2002 (P.L. 107-296; 116 Stat. 2229) and the National Defense Authorization Act FY2004 (P.L. 108-136, 117 Stat. 1621) authorize the creation of new human resources management (HRM) systems for civilian employees of the Departments of Homeland Security and Defense. Both laws stipulate that the Chapter 61 provisions cannot be waived, modified, or otherwise affected by the new HRM systems. (See the discussions of the 5 U.S.C. Chapter 97 and Chapter 99 provisions in this compendium.)

The impetus for revamping federal employee hours of work into flexible and compressed schedules stems from the reality that variations on the standard eight-hour work day can oftentimes lead to greater efficiency, productivity, and employee morale. Studies in both the federal and private sector appear to support the conclusion that alternative work-hour options benefit both employees and management.

Major Provisions

In general, the hours of work provisions of Chapter 61 establish the basic work week for federal employees, list official federal holidays, and define the availability of flexible and compressed work schedule options. Pursuant to this chapter, agency heads are responsible for establishing the basic 40-hour workweek, hours and days of duty, telecommuting policy, approval of scheduling academic programs for improving job-centered skills, and approval of premium pay provisions.

Provisions governing compensation for 11 federal holidays are set forth. Federal compensable holidays identified in the chapter include New Year's Day, the birthday of Martin Luther King Jr., Washington's Birthday, Memorial Day, Independence Day, Labor Day, Columbus Day, Veterans Day, Thanksgiving Day, Christmas Day, and Inauguration Day (the last reserved for employees in Washington, DC and the immediate vicinity, and observed only quadrennially).

Flexible and compressed work schedules are defined. Consistent with certain mandatory hours of attendance, and provided that agency operations are not disrupted as a result, agencies may authorize employees to vary the length of a workweek or workday and schedule the 80 hours biweekly work requirement in less than 10 workdays, including a four-day workweek and variation in reporting and departure times. Provisions affecting compensatory time, premium pay

provisions, night differential pay, and leave and retirement provisions interactive with flexible and compressed work schedules are described. Collective bargaining is authorized for determining flexible and compressed work schedules.

Federal employees may not coerce fellow employees with respect to participation or non-participation in flexible and compressed work schedules; the Office of Personnel Management (OPM) has responsibility for administering the program.

Discussion

The transformation of the federal workplace in terms of wide-ranging work schedule variation, including flexible sign-in-sign-out and compressed schedules, is a revolutionary change from the generations-old "nine to five/Monday through Friday" workweek pattern. The responsibility of the agency head for determining the efficiency of the system and managing workload accomplishment remains in place, subject to the challenges posed by flexible work schedules. Aside from a few complaints that certain core hours are sometimes inadequately covered, the system appears to work well.

Selected Source Reading

Congress. House. Committee on Post Office and Civil Service. Federal Employees Leave Sharing Amendments Act of 1993. Committee Rept. 103-246. 103rd Congress, 1st session. Washington: GPO, 1993.

General Accounting Office. Alternative Work Schedules: Many Agencies Do Not Allow Employees the Full Flexibility Permitted by Law. Washington: GPO, 1994.

Kevin R. Kosar

(25) Leave (Chapter 63; in Part III, Subpart E — Attendance and Leave).

Statutory Intent and History

The 1966 Title 5 codification statute (80 Stat. 378) and the Civil Service Reform Act of 1978 (92 Stat. 1111) are the basic authorities underlying Chapter 63. Additional authorities contributing to its provisions include a 1968 statute authorizing federal employee leaves of absence to attend funerals of immediate relatives who died while serving as members of the armed forces in combat zones or for those employees called to duty as members of the National Guard or armed forces reserves (82 Stat. 1151, as amended by P.L. 108-136, Sections 1113 and 1114); the Treasury, Postal Service, and General Government Appropriations Act of 1995 (108 Stat. 2423); the Federal Employees Leave Sharing Act of 1988 (102 Stat. 2834); the Family and Medical Leave Act of 1993 (107 Stat 19); and provisions for leave transfers in major disasters and emergencies (111 Stat. 196). The Homeland Security Act of 2002 (116 Stat. 2229) and the National Defense Authorization Act for FY2004 (P.L. 108-136, 117 Stat. 1621) authorize the creation of new human resources management (HRM) systems for civilian employees of the Departments of Homeland Security and Defense. Both laws stipulate that the Chapter 63 provisions cannot be waived, modified, or otherwise affected by the new HRM systems. (See the discussions of the 5 U.S.C. Chapter 97 and Chapter 99 provisions in this compendium.)

Federal employee annual, sick, holiday, and other leave options are among the most important and expensive elements of the basic federal benefits package. Insofar as total federal compensation comparability is concerned, leave benefits, along with health and retirement, are considered to be key components in comparing federal and private sector employment.

Major Provisions

Federal employee leave benefits are defined as regular workdays, for which employees are compensated, exclusive of holidays. Provisions detail categories of leave, the leave accrual process, and federal leave bank programs.

Federal leave benefits accrue to full-time and part-time employees, and are authorized during any part of the work year, subject to approval of agency heads. Annual leave is accrued on the basis of length of service and ranges from four hours to eight hours per biweekly pay period. Applicable federal service in another agency is creditable for annual leave purposes. Accumulation of annual leave, with certain exceptions, is limited to 30 days in a calendar year. Payment for unused annual leave, upon separation from the federal service, is authorized for up to 30 days, except for members of the Senior Executive Service and Senior Foreign Service, who may accumulate and be compensated for annual leave up to 90 days.

Federal employee sick leave accrues at the rate of four hours per biweekly pay period. There is no limit on sick leave accrual and, under the Civil Service Retirement System (CSRS), but not the Federal Employees Retirement System (FERS), unused sick leave may be credited for retirement purposes upon separation of the employee. Sick leave may be used in connection with child adoption, and up to 30 days of sick leave may be advanced in the case of serious illness. Sick leave is not charged to certain federal law enforcement officers for injury or illness resulting from performance of duty.

The Office of Personnel Management (OPM) is authorized to establish a program by which federal employees may transfer accumulated annual leave, subject to certain limitations, to other employees in cases of medical emergencies. Provisions for restoring unused transferred leave are provided. Federal employees are prohibited from exercising any coercion, intimidation, or promises in connection with receipt or donation of annual leave.

Agencies are authorized to establish their own voluntary leave banks for use by federal employees. Agencies in the excepted service may establish separate leave bank programs. An employee's accrued annual leave, up to 50% of his or her annual entitlement, may be contributed to the leave bank and made available to another employee needing leave for a medical emergency. No coerciveness may be involved in the granting or utilization of annual leave for this purpose. Leave Bank Boards review and administer the leave banks.

Discussion

Federal leave benefits — annual, sick, holiday, and other — at an estimated cost of 15% of the federal payroll, are a prime and costly part of the benefits package to federal employees. One indication of cost is that a prime inducement for entry and retention in the Senior Executive Service was the entitlement to unlimited accrual of annual leave benefits and the subsequent curtailment thereof to a maximum of 90 days. Other federal employees may accrue a maximum annual carryover of 30 days of annual leave. All unused annual leave from the current year is computed, considered compensable income, and granted to the federal employee upon separation from the federal service, either through normal retirement or other means.

Federal sick leave, accrued at the rate of 13 days per calendar year for all full-time employees, and proportionally less, according to work schedules, for part-time employees, may be accumulated without limit. Payouts for unused sick leave are not permitted.

The federal leave bank program has been a dramatic new departure in allocating additional annual leave to federal employees requiring it for medical emergencies. Pursuant to the program, federal employees may donate or borrow annual leave. An individual's donation of annual leave may not exceed 50% of his

or her annual entitlement. Intra-agency, a federal employee may designate a co-worker as beneficiary of donated annual leave because of medical emergency.

Selected Source Reading

Office of the Vice President. National Performance Review. Creating a Government That Works Better & Costs Less. Accompanying report: Enhancing the Quality of Worklife. Washington: GPO, 1993.

Congress. House. Committee on Post Office and Civil Service. Study of Total Compensation in the Federal, State and Private Sectors. Committee print 98-16. 98th Congress, 2nd session. Washington: GPO, 1984.

Kevin R. Kosar

(26) Labor-Management Relations (Chapter 71; in Part III, Subpart F — Labor-Management and Employee Relations).

Statutory Intent and History

Title VII of the Civil Service Reform Act of 1978 (92 Stat. 1191; P.L. 95-454) gives federal employees the statutory right to form labor unions and bargain collectively over the terms and conditions of employment.[1059] The statute excludes specific agencies and gives the President the authority to exclude other agencies for reasons of national security.

The Civil Service Reform Act of 1883 (commonly called the Pendleton Act, after its sponsor, Senator George Pendleton) established the Civil Service Commission (CSC). The act was an attempt to reform the political patronage system. It provided for merit hiring and promotion of federal employees, but did not give federal workers the right to unionize.

After President John Kennedy issued Executive Order 10988 in January 1962, union membership among federal employees increased significantly. The order gave employees of the executive branch the right to form unions and bargain collectively. Federal employees were allowed to bargain over the conditions of employment but not over work assignments. The authority to set wages and fringe benefits remained with Congress. Agencies could require union representatives to bargain during nonwork hours. Federal workers were not allowed to strike. Collective bargaining agreements could include negotiated procedures for resolving grievances. The CSC and the Department of Labor were required to develop a code of fair labor practices. The executive order did not apply to the Federal Bureau of Investigation (FBI), the Central Intelligence Agency (CIA), or other agencies or subagencies primarily performing investigative, intelligence, or security functions, if the head of the agency determined that union representation was not in the interests of national security.

Executive Order 11491, issued by President Richard Nixon in October 1969, replaced Executive Order 10988. President Nixon's order created a more independent administrative structure for federal labor-management relations. The Federal Labor Relations Council (FLRC) was created to administer and interpret the executive order, and the Federal Services Impasses Panel was created to resolve bargaining impasses. Members of the FLRC included the Chairman of the CSC, the Secretary of Labor, and an appointee from the Executive Office of the President. The Assistant Secretary of Labor for Labor-Management Relations was given responsibility for determining the appropriateness of bargaining units, supervising union elections, and settling

[1059] 5 U.S.C. §§ 7101-7135.

complaints of unfair labor practices. The executive order listed specific actions for both labor and management that would be considered unfair labor practices. Union representatives were required to bargain during nonwork hours. The executive order did not require bargaining unit members to pay dues. The order required unions to make regular financial reports available to members. The order did not cover the FBI, CIA, or the General Accounting Office (GAO). The language giving agency heads the authority to exclude unions was similar to the language in Executive Order 10988.

Executive Order 11491 was amended by other executive orders. Executive Order 11616, issued by President Nixon in August 1971, required collective bargaining agreements to include negotiated procedures for resolving grievances and designated the Director of the Office of Management and Budget as the presidential appointee to the FLRC.

Major Provisions

Executive orders may be amended or withdrawn. Title VII of the Civil Service Reform Act of 1978 (CSRA) established in statute the right of federal employees to organize and bargain collectively. The law applies to executive branch agencies, the Library of Congress, and the Government Printing Office. The CSRA excludes from coverage members of the armed forces, Foreign Service employees, the FBI, CIA, GAO, National Security Agency, Tennessee Valley Authority, the Federal Services Impasses Panel, and the newly created Federal Labor Relations Authority (FLRA). The CSRA also gives the President the authority to exclude, in the interests of national security, any agency or subagency whose primary function involves investigative, intelligence, counterintelligence, or security work.

Under the CSRA, federal employees can bargain over the conditions of employment, but not over wages, benefits, or other matters set in law. Federal employees cannot strike. The CSRA lists both labor and management unfair labor practices. The CSRA requires unions to make regular financial reports available to members. Bargaining agreements must include negotiated procedures for resolving grievances. Grievance procedures must provide for binding arbitration. Union representatives are allowed official time for contract negotiations. Official time for other matters can be negotiated. The CSRA does not require bargaining unit members to pay dues.

The CSRA changed the administrative structure of federal labor-management relations. The CSRA replaced the CSC with the Office of Personnel Management (OPM) to administer and enforce civil service law and the Merit Systems Protection Board to hear and decide employee appeals of adverse personnel actions and other matters. The CSRA created the FLRA and retained the Federal Services Impasses Panel. The FLRA determines appropriate bargaining units, supervises union elections, and resolves complaints of unfair labor practices. To make the agency independent of other federal agencies, the three members of the

FLRA are appointed by the President and confirmed by the Senate. No more than two members of the FLRA may belong to the same political party. The Office of General Counsel of the FLRA investigates and prosecutes charges of unfair labor practices.

Discussion

Recent legislation has given federal agencies greater flexibility in personnel matters. Legislation creating the Transportation Security Administration (TSA) gave the agency head the authority to exclude airport screeners from collective bargaining. Legislation creating the Department of Homeland Security (DHS) gave the President different authority to exclude DHS agencies from collective bargaining. The Secretaries of DHS and the Department of Defense (DOD) have been given the authority to establish personnel systems for all or parts of their departments.

The Aviation and Transportation Security Act of 2001 (P.L. 107-71) created the TSA and shifted the responsibility for airport screening to the federal government. The act gave the head of the TSA, which was later transferred to DHS, the authority to determine the terms and conditions of employment for federally employed airport screeners. In January 2003, the head of the TSA announced that the agency would not bargain with airport screeners.

The Homeland Security Act of 2002 (P.L. 107-296; 116 Stat. 2229) gave the Secretary of DHS, in regulations issued jointly with the Director of OPM, the authority to establish a human resources management system for all or parts of the department. Any such system must allow employees to organize and bargain collectively. An agency or subagency transferred to the department can be excluded from collective bargaining if the agency was previously excluded by executive order or, if employees were not previously organized, the agency's primary function involves investigative, intelligence, counterintelligence, or security work, and the President determines that union representation is not in the national interest. An agency or subagency whose employees were previously represented by a union (or unions) can be excluded from collective bargaining if (a) the responsibilities of the agency change and a majority of the employees have as their primary duty intelligence, counterintelligence, or investigative work directly related to terrorism; or (b) the President determines that union representation would have a substantial adverse impact on the ability of the department to protect homeland security and Congress is given a written explanation 10 days before the President takes action. An employee may be excluded from a bargaining unit if the employee's responsibilities change (or the individual is a new employee) and the employee's primary duty consists of intelligence, counterintelligence, or investigative work directly related to terrorism. The act also gave the Secretary of DHS the authority to create an internal process for hearing employee appeals of adverse personnel actions.

The Department of Defense Authorization Act of 2004 (P.L. 108-136, 117 Stat. 1621) gave the Secretary of Defense the authority, in collaboration with the Director of OPM, to create a human resources management system for all or parts of the department. The system must ensure that civilian employees have the right to organize and bargain collectively. The President retains the authority to exclude from collective bargaining any agency whose primary function involves investigative, intelligence, counterintelligence, or security work, if the President determines that union representation is not in the national interest. The act gives DOD the authority to establish, together with OPM, a labor-management relations system. The act allows DOD to bargain at a national level with employee unions (i.e., rather than bargaining with each local). The act gave the Secretary of Defense the authority to create an internal process for hearing employee appeals of adverse personnel actions.

Selected Source Reading

CRS Report RL31500. Homeland Security: Human Resources Management, by Barbara L. Schwemle.

CRS Report RL31954. Civil Service Reform: Analysis of the National Defense Authorization Act of 2004, coordinated by Barbara L. Schwemle.

U.S. Federal Labor Relations Authority. A Guide to the Federal Service Labor-Management Relations Program. Washington: GPO, 2001.

Gerald Mayer

(27) Antidiscrimination in Employment and Employees' Right to Petition Congress (Chapter 72; in Part III, Subpart F — Labor Management and Employee Relations).

Statutory Intent and History

The Civil Service Reform Act of 1978 (CRSA; 92 Stat. 1111), President Carter's plan for revamping the civil service system, included provisions to shift authorities between federal agencies with respect to enforcement of laws to eliminate employment discrimination. The intent of the act was to separate the conflicting roles of the Civil Service Commission (CSC) as both federal personnel manager and protector of employee rights and assign these tasks to two new agencies, the Office for Personnel Management (OPM) and Merit Systems Protection Board (MSPB), respectively. But principal responsibility for implementing equal employment opportunity (EEO) policy in the federal government was placed with the Equal Employment Opportunity Commission (EEOC). The act also created a minority recruitment program to insure that groups previously underrepresented in federal agencies would be actively encouraged to apply.

Historically, the concept of merit selection of employees began with a 19th century statute, the Civil Service Act of 1883 (the Pendleton Act), that required open, competitive examinations for public service jobs in which both men and women were eligible to compete, although categories of work were usually designated by sex. Civil service employment, like employment generally, remained largely sex (and race) segregated for many years. Federal concern with equal employment opportunity for government workers began incrementally in 1941, when President Franklin Roosevelt barred discrimination in federal programs concerned with defense production and set up a Committee on Fair Employment Practice. From this narrow base, in the decades following World War II, additional steps were taken by Congress, the courts, and the executive branch to extend equal employment opportunity more widely in both the public and private sectors.

When Congress enacted Title VII of the Civil Rights Act of 1964, prohibiting employment discrimination on the basis of race, color, religion, sex, or national origin, the federal government was specifically excluded from the definition of employer covered by the act (42 U.S.C. § 2000e et seq.). Section 701 of the act did provide, however, that federal sector employment decisions were to be free from discrimination, and authorized the President to enforce this policy. The CSC was thereafter directed by Executive Orders 11246 and 11478 to protect federal employee rights by establishing comprehensive procedures for investigation and resolution of EEO charges. Doubts as to the efficacy of the CSC regulatory program, however, compounded by lack of a viable judicial remedy, eventually led Congress to adopt the Equal Employment Opportunity Act of 1972, adding section 717 to Title VII (42 U.S.C. § 2000e-16). Section 717 created a private right

of action for executive branch employees to challenge discriminatory practices in federal court. It also strengthened CSC authority to devise "necessary and appropriate" remedies to enforce Title VII, "including reinstatement or hiring of employees with or without back pay." Authority for enforcing Title VII in federal employment was transferred to the EEOC by Reorganization Plan No. 1 of 1978 and the CSRA.

In later years, Congress expanded federal employee rights with passage of the Rehabilitation Act of 1973 (29 U.S.C. § 791), and amendments to the Equal Pay Act (1974; 20 U.S.C. § 206(d)) and the Age Discrimination in Employment Act (1978; 29 U.S.C. §§ 631, 633a), prohibiting, respectively, discrimination based on age, physical or mental impairment, and sex-based wage inequality. These statutes, in turn, define the kinds of discrimination forbidden by the CSRA (5 U.S.C. §§ 72017204). And to assure that equal employment opportunity was extended in fact, as well as in word, to certain groups whose options for federal employment had previously been limited, the CSRA mandated a recruitment program to eliminate underrepresentation of minorities within the various departments and agencies.

The Homeland Security Act of 2002 (P.L. 107-296; 116 Stat. 2229) and the National Defense Authorization Act for FY2004 (P.L. 108-136, 117 Stat. 1621) authorize the creation of new human resources management (HRM) systems for civilian employees of the Departments of Homeland Security and Defense. Both laws stipulate that the Chapter 72 provisions cannot be waived, modified, or otherwise affected by the new HRM systems. (See the discussions of the 5 U.S.C. Chapter 97 and Chapter 99 provisions in this compendium.)

Major Provisions

Section 7201 states that it is the policy of the United States to ensure equal employment opportunities for employees without discrimination because of race, color, religion, sex, or national origin. This section also requires OPM to develop a continuing program for the recruitment of minorities for employment in federal agencies. Under this program, each executive agency is required to administer the antidiscrimination policy in a manner designed to eliminate underrepresentation of minorities in the various categories of civil service employment within the federal service, with special efforts directed at recruiting in minority communities, in educational institutions, and from other sources. OPM is further required to conduct a continuing program of assistance to agencies in carrying out the program, as well as evaluation and oversight to determine the program's effectiveness in eliminating minority underrepresentation. The EEOC is charged with establishing guidelines for carrying out the program. OPM reports to Congress annually with data regarding the minority recruitment program in order to evaluate its effectiveness.

Section 7202 requires that the same benefits be provided in an executive agency or in the competitive service for a married female employee and her spouse and

children as are provided for a married male employee and his spouse and children, and vice versa.

Section 7203 prohibits discrimination because of a handicapping condition in an executive agency or in the competitive service if OPM believes the job can be performed by an individual with such a condition. An exception is made for any employment situation that might endanger the health or safety of the employee or others.

Section 7204 bans discrimination because of race, color, creed, sex, or marital status with respect to general schedule pay rates, prevailing rate systems, or appointments to positions classified above GS-15.

Subchapter II, Section 7211, "Employees' Right to Petition Congress," protects the right of employees, individually or collectively, to petition Congress, or a Member of Congress, or to furnish information to either house of Congress, to a committee or Member.

Discussion

Although the Civil Service Act of 1883 inaugurated the idea of a merit system for appointing federal employees, the principle of equal employment opportunity was expanded considerably by the great social and political changes of the second half of the 20th century. Current protections for federal workers are an amalgam of merit system principles and nondiscrimination requirements administered jointly by employing federal agencies, MSPB, and the EEOC. The first line of defense against federal workplace discrimination is an internal administrative process established by each federal agency to receive, investigate, and adjudicate employee complaints of unlawful discrimination. These internal agency rules have been much criticized both for perpetuating an inherent conflict of interest — by making the agency the judge of its own actions — and for encouraging large numbers of baseless complaints due to lack of substantive standards. The CSRA gave the EEOC exclusive jurisdiction to review agency decisions involving federal employees where only discrimination issues are alleged or no appeal rights to MSPB exist. Complicating the relationship between the MPSB and the EEOC is an election of remedies requirement in the CSRA, designed to avoid duplicative processing of complaints, though the agencies are required to work together. In "mixed cases," involving a discrimination claim stemming from an adverse personnel action appealable to the MSPB, the board has concurrent jurisdiction, subject to EEOC review of the equal employment opportunity portion of the employee's case. Thus, an MSPB decision adverse to the employee may be reviewed by the EEOC. Any difference of opinion between the agencies must be submitted to a statutory special panel for resolution.

A significant incentive for the federal employee EEO claims was provided by the Civil Rights Act of 1991 (42 U.S.C. §1981a(b)). Formerly, remedies for discrimination were limited to back pay, reinstatement, and injunctive relief.

Under the 1991 act, the EEOC (and the federal courts) may award up to $300,000 in compensatorydamages to federal employees who prove "intentional" discrimination by their agencies violative of Title VII or the Rehabilitation Act of 1973. The damage award is meant to compensate for "future pecuniary losses, emotional pain, suffering, inconvenience, mental anguish, loss of enjoyment of life, and other nonpecuniary losses." Jury trials may be had by federal employees seeking judicial relief in damages under the 1991 act.

A new law approved by Congress, effective October 1, 2003, may encourage earlier settlement of employment discrimination claims against federal agencies. Under prior law, agencies were responsible for paying out of their own funds settlements reached during the administrative stage of a discrimination or whistleblowing retaliation complaint. Once the complaint went to court, however, the judgment or settlement was paid from the government-wide judgment fund. Section 201 of the Notification and Federal Employee Anti-Discrimination and Retaliation Act (No FEAR Act; P.L. 107-174) holds the particular agency — rather than the government as a whole — fiscally accountable by requiring that discrimination awards, judgments, and settlements be paid from the budget of the agency wrongdoer. The law also requires that applicants, employees, and former employees be given written notice and training about their rights, and that the information and statistics be posted on the agencies' Internet sites.

Selected Source Reading

Congress. Senate. Committee on Governmental Affairs. Reorganization Plan No. 1 of 1978: To Make the Equal Employment Opportunity Commission the Principal Federal Agency in Fair Employment Enforcement. Hearing. 95th Congress, 2nd session. Washington: GPO, 1978.

Congress. House. Committee on Post Office and Civil Service. Subcommittee on Investigations. Discrimination in the Federal Government. Hearing. 95th Congress, 2nd session. Washington: GPO, 1978.

General Accounting Office. Equal Employment Opportunity: Rising Trends in EEO Complaint Caseloads in the Federal Sector. GAO/GGD-98-157BR. July 1998.

Charles Dale

(28) Suitability, Security, and Conduct (Chapter 73; in Part III, Subpart F — Labor-Management and Employee Relations).

Statutory Intent and History

The 1966 Title 5 codification statute (80 Stat. 378) is the basic authority for Chapter 73, Suitability, Security, and Conduct. Additional authorities include provisions of a 1967 statute amending Title 5 and codifying recent law (81 Stat. 195 at 208) and the Omnibus Crime Control and Safe Streets Act of 1968 (82 Stat. 197 at 235). The Homeland Security Act of 2002 (P.L. 107-296; 116 Stat. 2229) and the National Defense Authorization Act for FY2004 (P.L. 108-136, 117 Stat. 1621) authorize the creation of new human resources management (HRM) systems for civilian employees of the Departments of Homeland Security and Defense. Both laws stipulate that the Chapter 73 provisions cannot be waived, modified, or otherwise affected by the new HRM systems. (See the discussions of the 5 U.S.C. Chapter 97 and Chapter 99 provisions in this compendium.)

The chapter enumerates basic standards for conduct and behavior of federal employees. As such, its content relates essentially to law enforcement. Prohibitions against disloyalty, strikes against the government, advocating overthrow of the government, and improper gift-giving or acceptance, are admonitions to avoid activities that could lead not only to dismissal, but to prosecution as well.

Major Provisions

The President is authorized to promulgate standards governing federal employee conduct. Included are provisions related to loyalty and striking, security clearance, political activities (for a discussion of the provision relating to employee political activities, see this compendium's discussion of 5 U.S.C. Chapter 73, Subchapter III), and receipt of foreign gifts and decorations. Employee misconduct is also covered, including prohibition on gifts to superiors, drug abuse, and alcohol abuse and alcoholism.

The chapter sets forth employment limitations in the federal service, including prohibitions against those advocating overthrow of the government, participation in or advocacy of striking against the government, or inciting a riot or civil disorder. Regulations concerning those removed for national security reasons, including appointments elsewhere in the government for such individuals, are authorized.

The President, Vice President, Members of Congress, and federal employees are prohibited from accepting foreign gifts and decorations, except those of minimal value, certain travel expenses, an educational scholarship, or medical treatment. Gifts of more than minimal value become the property of the United States, and

violation of these provisions subjects the individual to civil action by the government.

Federal employee misconduct provisions include solicitation of gifts for superiors or acceptance by superiors of gifts from subordinates. Excessive use of intoxicants is a bar to federal employment. The Office of Personnel Management (OPM) is responsible for developing treatment programs for federal employees suffering from drug abuse and alcoholism.

Discussion

Chapter 73 is the major civil enforcement authority insofar as federal employee conduct and behavior are concerned. Its prohibitions on the right to strike or advocate a strike, gift acceptance restrictions, and misconduct proscriptions, ranging from engaging in riots and disorder to alcohol and drug abuse, are accompanied by prescribed penalties — the maximum being removal from the service — and rehabilitation options, such as treatment programs for drug and alcohol abuse. With the exception of national security breaches, little attempt has been made of late to modify this enforcement authority.

Selected Source Reading

Rosenbloom, David H. Federal Service and the Constitution: Development of the Public Employee Relationship. Ithaca: Cornell University Press, 1971.

General Accounting Office. The Public Service: Issues Affecting Its Quality, Effectiveness, Integrity, and Stewardship. Washington: GPO, 1990.

President's Council on Integrity and Efficiency. A Progress Report to the President. Fiscal Year 1993. Washington: GPO, 1993.

Mitchel A. Sollenberger

(29) Political Activities (Chapter 73, Subchapter III; in Part III, Subpart F — Labor-Management and Employee Relations).

Statutory Intent and History

Chapter 73 political activities provisions derive from the Hatch Act, initially adopted in 1939 (53 Stat. 1147) and subsequently amended several times, the most recent major modifications being the Hatch Act Reform Amendments of 1993 (107 Stat. 1001). The intent of these laws is to regulate the political activities of certain federal employees and to provide penalties for violations.

Major Provisions

The Hatch Act and its amendments cover employees or officeholders in executive agencies or in positions within the competitive service that are not in executive agencies, as well as the U.S. Postal Service and Postal Rate Commission employees. District of Columbia government employees or office holders, other than the mayor, city council members, and the recorder of deeds, are also covered. The President, Vice President, General Accounting Office employees, and members of the uniformed services are not covered by this law.

Subchapter III of Chapter 73 provides that employees may take an active part in political management or in political campaigns, except as prohibited, and retain the right to vote as they choose and express their opinions on political subjects and candidates. Exceptions are noted, such as employees of the Criminal Division of the Department of Justice, Federal Bureau of Investigation, and administrative law judges.

The Office of Personnel Management (OPM) may prescribe regulations permitting employees, with certain exceptions, to take an active part in political management and political campaigns involving the municipality or other political jurisdictions in which they reside. However, employees are prohibited from being candidates for partisan political office. Restrictions are present regarding the solicitation and acceptance of political contributions.

The law provides that, if the Special Counsel (who heads a separate federal agency, the Office of Special Counsel) receives an allegation concerning any matter relating to prohibited political activities, withholding of information, political intrusion into personnel decisionmaking, and discrimination, the Special Counsel can investigate and seek corrective action under 5 U.S.C. § 1214 and disciplinary action under 5 U.S.C. § 1215 in the same way as if a prohibited personnel practice were involved. An employee or individual who violates Section 7323 or 7324, relating to prohibitions on the use of official influence or official information and solicitation, shall be removed from his or her position, and funds appropriated for the position from which the individual was removed thereafter may not be used to pay him or her. However, if the Merit System

Protection Board finds by unanimous vote that the violation does not warrant removal, a penalty of not less than 30 days' suspension without pay shall be imposed by direction of the Board.

Discussion

The modifications effected by the Hatch Act Reform Amendments of 1993 were adjusted slightly by the Legislative Branch Appropriations Act, 1997 (110 Stat. 2416), which modified 5 U.S.C. § 3303 with a provision stating: "An individual concerned in examining an applicant for or appointing him in the competitive service may not receive or consider a recommendation of the applicant by a Senator or Representative, except as to the character or residence of the applicant."

In January 1998, OPM published final regulations on political activities of federal employees residing in designated localities. Spotsylvania County, Virginia, and St. Mary's County, Maryland, were added as designated localities, thereby qualifying federal employees who reside in these counties to a partial exemption from the prohibition at 5 U.S.C. § 7323(a)(2)(3) on political contributions and running for election to a partisan political office.

In the 105th Congress, draft legislation prepared but not introduced by the House Civil Service Subcommittee chair, Representative Mica, would have authorized civil monetary penalties and debarment from employment for former federal employees convicted of Hatch Act violations during their federal employment.

In the 108th Congress, a provision at Section 1109 of H.R. 1588, the National Defense Authorization Act for FY2004, as passed by the House of Representatives, on clarification of the Hatch Act was dropped in conference. (A similar provision also was included in H.R. 1836, which was marked up by the House Committee on Government Reform, but has not seen further action.) It would have exempted a federal employee or individual who was employed by the Department of Defense Inspector General's office before the act's enactment date and transferred to a Special Court sponsored by the United Nations from the provisions of 5 U.S.C. § 7326. Section 7326 authorizes an employee's removal from his or her position or 30 days' suspension without pay for violating the prohibitions on federal employee political activities. The exemption would have no longer applied if the employee or individual subsequently became reemployed in the civil service. The provision would have provided that once employees in this specific category leave government service, they would no longer by covered by the Hatch Act restrictions on political activities by federal employees. H.R. 1509, which would have applied this provision to a broader category of employees, was referred to the House Committee on Government Reform, but has not seen further action as of this writing.

The Homeland Security Act of 2002 (P.L. 107-296; 116 Stat. 2229) and the National Defense Authorization Act for FY2004 (P.L. 108-136, 117 Stat. 1621)

authorize the creation of new human resources management (HRM) systems for civilian employees of the Departments of Homeland Security and Defense. Both laws stipulate that the Chapter 73 provisions cannot be waived, modified, or otherwise affected by the new HRM systems. (See the discussions of the 5 U.S.C. Chapter 97 and Chapter 99 provisions in this compendium.)

Questions about application of the Hatch Act to campaign activity by executive branch personnel and to soliciting campaign contributions in federal buildings are especially raised during presidential election years. The Office of Special Counsel reiterates the law's provisions in providing guidance to federal employees.[1060]

Selected Source Reading

Aberbach, Joel D. and Bert A. Rockman. In the Web of Politics; Three Decades of the U.S. Federal Executive. Washington: Brookings Institution Press, 2000.

Rosenbloom, David H. Federal Service and the Constitution: Development of the Public Employee Relationship. Ithaca, New York: Cornell University Press, 1971.

Commission on Political Activity of Government Personnel. Findings and Recommendations (vol. 1), Research (vol. 2), Hearings (vol.3). Washington: GPO, 1968.

Congress. House. Committee on Post Office and Civil Service. Federal Employees Political Activities Act of 1993. H.Rept. 103-16. 103rd Congress, 1st session. Washington: GPO, 1993.

Congress. Senate. Committee on Governmental Affairs. Hatch Act Reform Amendments of 1993. S.Rept. 103-57. 103rd Congress, 1st session. Washington: GPO, 1993.

General Accounting Office. U.S. Attorneys; Laws, Rules, and Policies Governing Political Activities. GAO/GGD-00-171. July 2000.

CRS Report 98-885 A. "Hatch Act" and Other Restrictions in Federal Law on Political Activities of Government Employees, by Jack Maskell. (1998).

CRS Report 96-913 A. Recommendations by Members of Congress on Behalf of Applicants for Federal Employment, by Jack H. Maskell (1996). (This CRS report is archived and available from the author of this entry in the compendium.)

[1060] See OSC's Hatch Act website at [http://www.osc.gov/hatchact.html], visited Dec. 22, 2003.

U.S. Office of Special Counsel. Political Activity and the Federal Employee. Washington: OSC, 2000.

Barbara L. Schwemle

(30) Adverse Actions (Chapter 75; in Part III, Subpart F — Labor-Management and Employee Relations).

Statutory Intent and History

The current system for adverse actions in the federal civil service generally was established under the Civil Service Reform Act of 1978 (P.L. 95-45; 92 Stat. 1134). The intent was to streamline and codify disciplinary procedures. The subchapter relating to national security was established under P.L. 81-733 (64 Stat. 476).

Major Provisions

This chapter prescribes the cause and procedure for suspension for 14 days or less; removal, suspension for more than 14 days, reduction in grade or pay, or furlough for 30 days or less; actions against administrative law judges; actions involving national security; and actions involving the Senior Executive Service. It authorizes an agency, under regulations promulgated by the Office of Personnel Management (OPM), to take these actions for such cause as will promote the efficiency of the service. An employee against whom an action has been proposed is entitled to certain procedures such as advance written notice, a reasonable time to answer orally or in writing and to furnish affidavits and other documentary evidence, representation by an attorney or other representative, and a written decision and specific reasons therefor.

An agency may remove, suspend, reduce in grade, reduce in pay, or furlough an administrative law judge only for good cause established and determined by the Merit Systems Protection Board on the record after an opportunity for a hearing before the board.

Notwithstanding other statutes, the head of certain defined agencies may suspend without pay an employee when the agency head considers suspension necessary in the interest of national security. Subject to certain procedural requirements, an agency head may remove such a suspended employee when, after such investigation and review as the head considers necessary, the head determines that removal is necessary in the interests of national security. After suspension and before removal, an employee who has a permanent and indefinite appointment, has completed a probationary period, and is a citizen of the United States, is entitled to a written statement of the charges against him; an opportunity to answer the charges and submit affidavits; a hearing, at the request of the employee, by an agency authority duly constituted for this purpose; a review of his case by the agency head or designee, before a decision adverse to the employee is made final; and a written statement of the decision by the agency head.

Under regulations prescribed by OPM, an agency is authorized to remove from the civil service or suspend for more than 14 days certain career appointees of the Senior Executive Service only for misconduct, neglect of duty, malfeasance, or failure to accept a directed reassignment or to accompany a position in a transfer

of function. An employee against whom such an action is proposed is entitled to certain procedures, including advance written notice, a reasonable time to answer orally and in writing and to furnish affidavits and other documentary evidence, representation by an attorney or other representative, and a written decision and specific reasons therefor. An employee against whom an action is taken also is entitled to appeal to the Merit System Protection Board.

Discussion

This chapter establishes the cause and procedural protections for various disciplinary actions in the civil service and specifies the individuals who are entitled to protection. It attempts to strike a balance between management rights and employee protection.

The Homeland Security Act of 2002 (P.L. 107-296; 116 Stat. 2229) and the National Defense Authorization Act for FY2004 (P.L. 108-136, 117 Stat. 1621) authorize the creation of new human resources management (HRM) systems for civilian employees of the Departments of Homeland Security (DHS) and Defense (DOD). Both laws permit changes from the Chapter 75 provisions for DHS and DOD. (See the discussions of the 5 U.S.C. Chapter 97 and Chapter 99 provisions in this compendium.)

Selected Source Reading

Bussey, Ellen M., ed. Civil Service Law and Procedure: A Basic Guide, 2nd ed. Washington: Bureau of National Affairs, Inc., 1990.

Congress. House of Representatives. Committee on Reform and Oversight. Subcommittee on Civil Service. Civil Service Reform Issues. Hearing. 105th Congress, 2nd session. Washington: GPO, 1998.

Merit Systems Protection Board. Removing Poor Performers in the Federal Service. Issue Paper. Washington: MSPB, 1995.

Thomas Nicola

(31) Appeals (Chapter 77; in Part III, Subpart F — Labor-Management and Employee Relations).

Statutory Intent and History

The current system for appeals in the federal civil service was established under the Veterans Preference Act of 1944 (P.L. 78-359; 58 Stat. 390) and the Civil Service Reform Act of 1978 (P.L. 95-454; 92 Stat. 1138). The intent was to uphold the merit system by ensuring protection of federal employees from arbitrary agency actions.

Major Provisions

An employee or applicant for employment may submit an appeal to the Merit Systems Protection Board (MSPB) from any action appealable to the board under any law, rule, or regulation. An appellant has a right to a hearing for which a transcript will be kept, and to be represented by an attorney or another representative.

MSPB may hear any case appealed to it, or may refer the case to an administrative law judge or other employee of MSPB designated by the board to hear cases. A decision must be made after receipt of written representations of the parties to an appeal and after an opportunity for a hearing. If an employee or applicant prevails in an appeal, the employee or applicant is granted the relief provided in the decision when it is made. The decision remains in effect pending the outcome of any petition for review unless certain circumstances are met.

An agency's decision is sustained only if it is supported by substantial evidence in the case of an action based on unacceptable performance or by a preponderance of evidence in any other case. Nonetheless, an agency's decision may not be sustained if the employee or applicant for employment shows harmful error in applying the agency's procedures, or shows that the decision was based on any prohibited personnel practice, or that the decision was not in accordance with law.

The law provides for procedures to be followed by the Office of Personnel Management (OPM), if it decides to intervene, as well as those conditions whereby the Equal Employment Opportunity Commission (EEOC) becomes involved when discrimination (so-called mixed cases) has been alleged. Procedures to be followed for judicial review of MSPB decisions when they are appealed are prescribed.

Discussion

Jurisdiction by both MSPB and EEOC over mixed cases has been controversial. Critics assert that dual jurisdiction is inefficient, expensive, and time-consuming; supporters argue that it is necessary to ensure adequate review. Proposals to

streamline appeals by authorizing only the board or the commission (but not both), to hear them have been considered.

The Homeland Security Act of 2002 (P.L. 107-296; 116 Stat. 2229) and the National Defense Authorization Act for FY2004 (P.L. 108-136, 117 Stat. 1621) authorize the creation of new human resources management (HRM) systems for civilian employees of the Departments of Homeland Security (DHS) and Defense (DOD). Both laws permit changes from the Chapter 77 provisions DHS and DOD. (See the discussions of the 5 U.S.C. Chapter 97 and Chapter 99 provisions in this compendium.)

Selected Source Reading

Broida, Peter. A Guide to Merit Systems Protection Board Law and Practice, 15th ed. Arlington, VA: Dewey Publications, Inc., 2003.

Council on Excellence in Government, U.S. Chamber of Commerce, Reason Public Policy Institute, ASPA, The George Washington University, and Government Executive. Transitioning to Performance-based Government: A Report to the 43rd President and the 107th Congress on the Transition. Dialogue Series 16. Washington: 2000.

"Symposium on the Civil Service Reform Act of 1978: An Evaluation." Policy Studies Journal, vol. 17 (winter 1988-1989), pp. 311-447.

Vaughn, Robert G. Merit Systems Protection Board: Rights and Remedies (rev. ed.). New York: Law Journal Seminars-Press, 1995.

Congress. House of Representatives. Committee on Government Reform and Oversight. Subcommittee on General Oversight and Investigations. Omnibus Civil Service Reform Act of 1996, Report to Accompany H.R. 3841. H.Rept. 104-831. 104th Congress, 2nd session. Washington: GPO, 1996.

Congress. House of Representatives. Committee on Post Office and Civil Service. Legislative History of the Civil Service Reform Act of 1978. Committee print. 96th Congress, 1st session. Committee Print 96-2. Washington: GPO, 1978.

Congress. Senate. Committee on Governmental Affairs. Subcommittee on Oversight of Government Management, Restructuring and District of Columbia.

Report of George V. Voinovich, Chairman, Report to the President: The Crisis in Human Capital. 106th Congress, 2nd session. Washington: GPO, 2000, pp. 54-55.

General Accounting Office. Merit Systems Protection Board: Mission Performance, Employee Protections, and Working Environment. GAO/GGD95-213. 1995.

Merit Systems Protection Board. Removing Poor Performers in the Federal Service. Issue Paper. Washington: MSPB, 1995.

S. Office of the Vice President. National Performance Review. From Red Tape to Results: Creating a Government That Works Better & Costs Less: Accompanying Report: Reinventing Human Resource Management. Washington: GPO, 1993.

Thomas Nicola

(32) Services to Employees (Chapter 79; in Part III, Subpart F — Labor-Management and Employee Relations).

Statutory Intent and History

The 1966 Title 5 codification statute (80 Stat. 378) is the basic statutory authority for Chapter 79, "Services to Employees." Additional authorities include the Anti-Drug Abuse Act of 1986 (100 Stat. 3207) and the Federal Employees Clean Air Incentives Act (107 Stat. 1995). The Homeland Security Act of 2002 (P.L. 107296; 116 Stat. 2229) and the National Defense Authorization Act for FY2004 (P.L. 108-136, 117 Stat. 1621) authorize the creation of new human resources management (HRM) systems for civilian employees of the Departments of Homeland Security and Defense. Both laws stipulate that Chapter 79 provisions cannot be waived, modified, or otherwise affected by the new HRM systems. (See the discussions of the 5 U.S.C. Chapter 97 and Chapter 99 provisions in this compendium.)

The chapter addresses federal employee health, safety, and commuting concerns. In addition to prescribing treatment programs for federal employees with alcohol and drug-related illness, provisions are set forth encouraging and mandating creation of proactive health and safety measures to prevent employee illness and disability.

Major Provisions

The provisions of Chapter 79 govern the establishment of agency health, safety, drug abuse, and alcohol abuse programs. They regulate the issuance of protective clothing and equipment for federal employees, and the creation of programs intended to encourage alternative means of commuting to the workplace, other than "singleoccupancy motor vehicles."

Agency heads are authorized to establish health service programs to promote and maintain the physical and mental fitness of their employees. Programs are limited to treatment of on-the-job illness and dental conditions requiring emergency treatment, pre-employment and other examinations, referral to private physicians and dentists, and preventive health programs.

The Secretary of Labor is responsible for creating safety programs covering federal employees within the agencies. The President may establish a safety council to advise the Secretary in administering the safety programs and to prevent injuries and accidents. Agency heads are responsible for the promotion of organized programs to reduce accidents, illness, and injuries, and to encourage safe practices and eliminate workplace hazards. Available appropriations may be used for purchase and maintenance of special equipment for protection of employees in performing assigned tasks.

Agency heads, in cooperation and consultation with the Office of Personnel Management (OPM) and the Secretary of Health and Human Services, are required to establish prevention, treatment, and rehabilitation programs for drug and alcohol abuse affecting employees within their agencies.

Agency heads are authorized to create programs to encourage employees and student volunteers to commute to and from work by means other than motor vehicles. In furtherance of such programs, options may include public transit passes or reimbursement therefor; furnishing space, facilities, and services to bicyclists; and offering other non-monetary incentives for alternative commuting options by employees. The President is required to designate one or more agencies to prescribe guidelines for alternative commuting programs, and such designees submit to the President and to Congress biannual reports on the number and type of agency programs, the extent of employee participation, and the costs to the government, and an assessment of environmental or other benefits resulting from such programs.

Discussion

Public health and safety programs have assumed increasing importance within the federal service in recognition of rapidly escalating costs of health care and the burdens placed on federal employee health insurance programs. A more proactive approach has long been advocated by federal agencies responsible for health and safety, notably the Department of Labor's Occupational Safety and Health Administration (OSHA), including strong emphasis on workplace safety, prevention of illness, influenza inoculation programs, and the like. Although the chapter cites the need for limited health care facilities within the agencies, emphasis still remains on referral to private sector practitioners, except in cases of medical emergency.

Encouragement of mass transit and other options, other than privately owned motor vehicles, for commuting to and from the workplace has long been advocated, but with modest results. In recent years, Congress has authorized agencies to use appropriated funds to provide monetary subsidies to employees in order to offset, at least partially, the cost of using mass transit for commuting.

Selected Source Reading

Congress. House. Committee on Post Office and Civil Service. Federal and Postal Service Employees Occupational Safety and Health Act of 1994. H.Rept. 103-858. 103rd Congress, 2nd session. Washington: GPO, 1994.

General Accounting Office. Federal Personnel: Employment Policy Challenges Created by an Aging Workforce. GAO/GGD-93-138. September 1993.

Mitchel A. Sollenberger

(33) Retirement (Chapter 83; in Part III, Subpart G — Insurance and Annuities).

Statutory Intent and History

The Civil Service Retirement System (CSRS) was established in 1920 (42 Stat. 1047). The law had a dual purpose; to provide for an adequate retirement income for individuals who had devoted much of their work lives to government service, and to provide an efficient and humane method to remove from duty older employees whose productivity was diminishing due to age. The original CSRS law included a provision for mandatory retirement at age 70, a requirement eliminated in 1978, except for certain public safety occupations. The CSRS retirement system is a defined benefit system in that employees contribute a defined percentage of their income to the system, and receive in turn a defined percentage of their top three years of compensation annually upon retirement.

From 1920 to 1984, CSRS was the retirement plan covering most civilian federal employees. Coverage was extended to Members of Congress and congressional employees in 1946. In 1935, Congress enacted the Social Security system for private sector workers, and the Social Security Amendments of 1983 (97 Stat. 65) mandated that all workers hired into permanent federal positions on or after January 1, 1984, be covered by Social Security. Since Social Security duplicated some existing CSRS benefits, and because the combined employee contribution rates for Social Security and CSRS would have reached more than 13% of pay, it was necessary to design an entirely new retirement system for federal employment, using Social Security as the base. Congress enacted the Federal Employees' Retirement System Act of 1986 (FERS) (100 Stat. 514). CSRS was closed to new entrants at the end of 1983, and all new federal employees hired since then are covered by FERS. As turnover in the workforce occurs, the number of workers in CSRS will decline, and eventually it will cease to exist. Less than one-third of the federal workforce is currently covered by CSRS.

The Homeland Security Act of 2002 (P.L. 107-296; 116 Stat. 2229) and the National Defense Authorization Act for FY2004 (P.L. 108-136, 117 Stat. 1621) authorize the creation of new human resources management (HRM) systems for civilian employees of the Departments of Homeland Security and Defense. Both laws stipulate that the Chapter 83 provisions cannot be waived, modified, or otherwise affected by the new HRM systems. (See the discussions of the 5 U.S.C. Chapter 97 and Chapter 99 provisions in this compendium.)

Major Provisions

Subchapter II of Chapter 83 requires forfeiture of a civil service or military annuity by individuals convicted of crimes against the national security.

Subchapter III of Chapter 83 provides a CSRS annuity to "vested" employees. Vesting requires five years of federal civilian service. Most CSRS participants must pay 7% of their salary into the retirement system throughout their federal

employment (certain occupational groups pay slightly more and receive higher benefits). An immediate annuity is provided for federal employees retiring at age 55 with 30 years of service, age 60 with 20 years of service, or age 62 with 5 years of service. Vested employees separating before retirement eligibility may draw a deferred annuity at age 62. In certain situations, including job abolishment or reductions-in-force, a reduced early retirement benefit is payable to workers retiring at any age with 25 years of service or at age 50 with 20 years. Different age and service criteria for retirement pertain to certain occupational groups. If the individual retires before age 55, his or her annuity is permanently reduced by 2% for each year of difference between the worker's actual age at retirement and 55.

Chapter 83 sets out the formulas for computing CSRS annuities. Special higher benefit formulas apply to Members of Congress and congressional employees, federal law enforcement officers, firefighters, and air traffic controllers. Regular federal employees retiring with 30 years of service receive an annuity of 56.25% of their average annual pay of their highest-paid 3 consecutive years ("high-3"). Members of Congress receive 75% of high-3 pay after 30 years; federal law enforcement officers, firefighters and air traffic controllers receive 50% of high-3 pay with 20 years of service.

Disabled workers who are unable to perform their federal jobs due to physical or mental impairment are provided disability retirement. Disability retirement benefits are calculated according to the same rules applicable to regular retirement, but there is a minimum benefit of 40% of high-3 pay.

Chapter 83 provides survivor benefits to spouses and dependent children of deceased CSRS workers and retirees. Retirees electing survivor coverage contribute up to 10% of their annuities in order to provide a spouse survivor benefit of up to 55% of the retiree's annuity.

CSRS annuities are adjusted annually by the rate of increase in the Consumer Price Index (CPI) over a one-year period.

Discussion

CSRS came under criticism in the 1970s for a number of reasons. Some argued that the system locked employees in the federal workforce, because the retirement benefits built up by employees were not portable. (The FERS program, by contrast, was designed to be portable.) Another criticism was that the automatic postretirement cost-of-living adjustments (COLAs) were too generous and skewed federal pay benefits towards the retired workforce. Congress first enacted COLAs for CSRS in 1962. The purpose of COLAs is to protect the purchasing power of retirement income from erosion due to inflation. Critics indicated that few private pension plans offered COLAs. Additionally, COLAs are subject to congressional intervention, whereby Congress may eliminate, reduce, or delay COLAs for federal retirees.

Selected Source Reading

CRS Report 98-810 EPW. Federal Employees' Retirement System: Benefits and Financing, by Patrick J. Purcell.

CRS-346 CRS Report RL30631. Retirement Benefits for Members of Congress, by Patrick J. Purcell. Patrick J. Purcell

(34) Federal Employees' Retirement System (Chapter 84; in Part III, Subpart G — Insurance and Annuities).

Statutory Intent and History

From 1920 to 1984, the Civil Service Retirement System (CSRS) was the retirement plan covering most civilian federal employees. Coverage of CSRS was extended to Members of Congress and congressional employees in 1946. In 1935, Congress enacted the Social Security system for private sector workers, and the 1983 amendments to the Social Security Amendments Act (97 Stat. 65) mandated that all workers hired into permanent federal positions on or after January 1, 1984, be covered by Social Security. Because Social Security duplicated some existing CSRS benefits, and because the combined employee contribution rates for Social Security and CSRS would have reached more than 13% of pay, it was necessary to design an entirely new retirement system for federal employment, using Social Security as the base. Congress enacted the Federal Employees Retirement System (FERS) in 1986 (100 Stat. 514). CSRS was closed to new entrants at the end of 1983, and all new federal employees hired since then are covered by FERS. FERS now covers more than two-thirds of civilian federal employees.

The Homeland Security Act of 2002 (P.L. 107-296; 116 Stat. 2229) and the National Defense Authorization Act for FY2004 (P.L. 108-136, 117 Stat. 1621) authorize the creation of new human resources management (HRM) systems for civilian employees of the Departments of Homeland Security and Defense. Both laws stipulate that the Chapter 84 provisions cannot be waived, modified, or otherwise affected by the new HRM systems. (See the discussions of the 5 U.S.C. Chapter 97 and Chapter 99 provisions in this compendium.)

Major Provisions

Subchapter II of Chapter 84 provides a basic annuity for Federal Employees' Retirement System (FERS) participants. Employees are vested after five years of service. Most FERS participants contribute 0.8% of pay into the pension plan. Federal law-enforcement officers, firefighters, air traffic controllers, and congressional employees contribute 1.3% of pay. FERS participants may retire at age 55 with 30 years of service. The minimum retirement age is increasing to age 57 as the Social Security normal retirement age rises to 67. FERS participants may retire with a reduced annuity at age 55 (rising to 57) with 10 through 29 years of service. The annuity is permanently reduced 5% for each year between the individual's age at retirement and 62. FERS also provides disability retirement and survivor benefits. Post-retirement cost-of-living adjustments are paid to retirees age 62 or over (and to disability and survivor annuitants of any age). If the increase in the Consumer Price Index (CPI) is 3% or more, increases are limited to one percentage point less than the rate of increase in the CPI.

Subchapter III of Chapter 84 provides a Thrift Savings Plan (TSP). The government contributes to the TSP 1% of the pay of all FERS participants and

matches up to 5% of pay voluntarily contributed by FERS workers. The maximum FERS employee contribution in 2004 is 14% of pay up to a maximum of $13,000. The maximum employee salary deferral will increase by $1,000 per year until it reaches $15,000 in 2006, after which it will be indexed to the CPI. At retirement, TSP accounts may be withdrawn as a lifetime annuity, as a lump sum, or in equal payments over a specific time period. Separating employees may withdraw their TSP account balance (subject to possible tax penalties) or roll it over to an individual retirement arrangement or another employer's qualified retirement plan.

Discussion

FERS was designed by Congress in the mid-1980s to be comparable to retirement plans offered by large employers in the private sector. As recently as 1988, 70% of employees in medium and large establishments in the private sector were covered under a defined benefit retirement plan, according to the Department of Labor. By 1997, however, only 50% of employees in medium and large establishments in the private sector were covered by a defined benefit plan. Moreover, in recent years, many large employers have converted their traditional defined benefit plans to "cash balance" plans that mimic the benefit accumulation patterns of a defined contribution plan, and typically pay a smaller benefit to career employees than they would have accumulated under a traditional defined benefit pension. As traditional defined benefit plans become less common in the private sector, Congress may decide to examine the structure of the Federal Employees' Retirement System to determine whether or not the retirement benefits offered to federal employees are still comparable to those offered in the private sector.

The Thrift Savings Plan (TSP) has proven to be a popular plan for savings by FERS participants. About four-fifths of eligible employees make voluntary contributions to the TSP. The FERS plan permits portability of retirement monies from the government to qualifying private plans.

Selected Source Reading

CRS Report 98-810 EPW. Federal Employees' Retirement System: Benefits and Financing, by Patrick J. Purcell.

CRS Report RL30387. Federal Employees' Retirement System: The Role of the Thrift Savings Plan, by Patrick J. Purcell.

Patrick J. Purcell

(35) Health Insurance (Chapter 89; in Part III, Subpart G — Insurance and Annuities).

Statutory Intent and History

Before 1959, the federal government did not provide health benefits to its civilian employees or retirees. The need for a government-wide health benefits program was recognized when Congress passed the Federal Employees Health Benefits Act of 1959 (P.L. 86-382; 73 Stat. 708) authorizing the Federal Employees Health Benefit Program (FEHBP). The program went into operation on July 1, 1960. The act and its subsequent amendments established eligibility for benefits and election of coverage by participants; the types of health benefit plans that may be offered; the types of benefits that may be provided; the role of the U.S. Office of Personnel Management (OPM); the level of government contributions; the establishment of an Employees Health Benefits Fund to pay for program expenses; the creation of an advisory committee; and provisions for studies, reports, and audits.

While the law was periodically amended to extend eligibility for coverage to additional employee groups, the basic structure of FEHBP has undergone relatively few changes since the program began operation. However, the Health Benefits Insurance — Federal Contribution Act (P.L. 91-418; 84 Stat. 869) completely altered the way the government contribution toward employees health plan premiums was determined in an effort to "provide automatic indexing of the Government contribution to reflect increases in medical price inflation." Beginning in 1971, the act established the formula for computing the government's premium share as the average premium of the six largest plans. Subsequently, the government's contribution increased from 40% to 50% of the average of the "Big Six" plan premiums in 1974, and to 60% in 1975 and thereafter. In 1997, the Balanced Budget Act (P.L. 105-33; 111 Stat. 251) replaced the Big Six formula with a formula setting the government's share of premiums at 72% of the weighted average premium of all plans in the program, not to exceed 75% of any given plan's premium. The new formula was effective in 1999.

The Homeland Security Act of 2002 (P.L. 107-296; 116 Stat. 2229) and the National Defense Authorization Act for FY2004 (P.L. 108-136, 117 Stat. 1621) authorize the creation of new human resources management (HRM) systems for civilian employees of the Departments of Homeland Security and Defense. Both laws stipulate that the Chapter 89 provisions cannot be waived, modified, or otherwise affected by the new HRM systems. (See the discussions of the 5 U.S.C. Chapter 97 and Chapter 99 provisions in this compendium.)

Major Provisions

Participation in FEHBP is voluntary, and enrollees may change from one plan to another during designated "open season" periods. Active and retired Members of Congress may participate under the same rules as other federal employees. At the time of retirement, enrollees have a one-time election to continue to

participate in FEHBP as retirees, provided they have been enrolled for at least five years immediately before retirement and are eligible for an immediate annuity.

FEHBP offers enrollees a choice of 6 fee-for-service (FFS) plans available government-wide, one consumer-driven option plan[1061] also offered government-wide, another 6 available to employees of certain small federal agencies, and about 240 health maintenance organizations (HMOs) serving limited geographic areas. Some plans are offering a "high" benefit and cost option and a "standard" option.

Although there is no core or standard benefit package required for FEHBP plans, all plans cover basic hospital, surgical, physician, and emergency care. Plans are required to cover certain special benefits including prescription drugs (which may have separate deductibles and coinsurance); mental health care with parity of coverage for mental health and general medical care coverage; child immunizations; and protection of enrollee out-of-pocket costs for "catastrophic" health care costs. Plans must include certain cost containment provisions, such as offering preferred provider organization (PPOs) networks as a component of the FFS plans, and hospital preadmission certification. There are variations in the amounts plans pay for benefits (as reflected in coinsurance provisions and deductibles), the availability of ancillary benefits (such as dental care or coverage of chiropractors), and the catastrophic cost protections.

OPM interprets the health insurance laws, writes regulations, and administers FEHBP. It approves qualified plans for participation in the program, negotiates yearly with plans to determine benefits and premiums for the following year, manages premium payments, and publishes information concerning plan options.

Discussion

FEHBP is the largest employer-sponsored health insurance program in the United States. Total annual cost of the program in FY2002 was about $22.7 billion, including $11.2 billion in enrollee and U.S. Postal Service payments. An issue sometimes raised regarding the design of the program is that the plans are not selected through competitive bidding, and, except for HMOs, most of the FFS plans in the program today have participated in the program for many years. Some plans have participated continuously since the start of the program. One

[1061] Beginning in 2003, a consumer-driven option plan was added to the FEHB program. This option provides beneficiaries with greater flexibility in health care spending through a personal care account (PCA) of $1,000 for a self-only plan and $2,000 for a family plan. Once the PCA has been exhausted, beneficiaries are responsible for paying for their own benefits, up to a prescribed amount. Traditional health care coverage begins after covered eligible expenses (paid out by the PCA and the member) total $1,600 for self-only plans and $3,200 for family plans.

concern about design of the programs is that enrollees must choose among several plans, which may be confusing. Others say choice helps ensure competition among plans, thus keeping premiums down. Still others say choice has no effect on costs, either to increase or decrease them. In recent years, fewer that 3% of enrollees changed plans during the annual open season. Another concern is that FEHBP plans compete for enrollees who are good risks (i.e., those who are less likely to experience health care costs in excess of the plan's premium), potentially causing some plans to enroll a larger proportion of high-cost enrollees. However, OPM monitors enrollment trends and seeks to minimize adverse risk selection.

Selected Source Reading

CRS Report RL31231. Health Insurance for Federal Employees and Retirees, by Carolyn L. Merck.

CRS Report RS20818. Federal Employees Health Benefits Program: Brief Facts, by Carolyn L. Merck.

Hinda Ripps Chaikind

(36) Long-Term Care Insurance (Chapter 90; in Part III, Subpart G — Insurance and Annuities).

Statutory Intent and History

The Long-Term Care Security Act (114 Stat. 762; P.L. 106-265) authorizes a long-term care insurance program for federal workers and their families. The resulting program, sponsored by the Office of Personnel Management (OPM), is administered by Long Term Care Partners, a joint venture created for this purpose by the John Hancock Life Insurance Company and the Metropolitan Life Insurance Company. Long Term Care Partners offers insurance policies that can be individually modified with respect to amount of coverage (e.g., $100 or $150 a day), years of coverage, length of the elimination period (the period of time before benefits begin to be paid), inflation protection, and other features. Participation is voluntary, with premium costs paid by those who are enrolled, not the government. During an initial open season from July 1 through December 31, 2002, current employees and their spouse could enroll in the program with minimal underwriting (medical screening); retirees and other eligible people had to go through more extensive underwriting.[1062] Since that time, all applicants aside from newly hired employees must complete the more extensive underwriting.

The federal employee long-term care insurance program has several objectives. The first is to encourage federal workers to consider purchasing long-term care insurance by making them aware of the cost of nursing home and community-based services and the limited assistance that most families can expect from Medicare, Medicaid, and private health insurance. Second, the program is designed to help participants choose coverage that is suitable for their needs and interests. Long-term care insurance is a complicated product for which it is useful to have an intermediary select an insurance carrier, choose a reasonable range of policy options, and prepare and distribute educational material. Finally, the federal program is intended to serve as a model for other employers to offer similar coverage. Compared to individual market policies, employment-based plans can have lower premiums due to administrative cost savings. The federal program was one of several proposals President Clinton made in January 1999 to help families with their long-term care needs.

The Long-Term Care Security Act has been amended four times through the end of 2003 to clarify and expand the list of eligible participants. P.L. 107-104 prohibits states from imposing taxes (other than general business taxes) on policy premiums.

[1062] The earliest effective date for people enrolling during the open season was October 1, 2002. A short early-enrollment period was held in the spring of 2002; it was intended for people able to choose coverage without the educational material being prepared for the open season.

Major Provisions

The Long-Term Care Security Act requires OPM to establish a program under which eligible individuals may obtain long-term care insurance. As amended, the act defines eligible individuals to include most federal and U.S. Postal Service employees,[1063] active members of the uniformed services, employees of the Tennessee Valley Authority, District of Columbia government employees who were first employed before October 1, 1987, and employees of the District of Columbia courts. Also eligible are annuitants of those groups and surviving spouses who are receiving a federal survivor annuity. Eligible relatives include current spouses of employees and annuitants, adult children, parents, parents-in-law, and some step-parents.

The long-term care insurance contracts must be tax-qualified (i.e., comply with the conditions specified in Section 7702B of the Internal Revenue Code), fully insured (perhaps through reinsurance), and issued by a carrier that is licensed to issue long-term care insurance in all states. There is no guaranteed issue (i.e., policies do not have to be issued to all who apply), and it is explicitly provided that coverage need not be made available to individuals who would immediately qualify for benefits. As nearly as practicable, underwriting standards for a spouse must be like those for the eligible individual. More stringent underwriting may apply to individuals who declined coverage when they first had an opportunity to enroll. Contracts must be guaranteed renewable so long as premiums are paid. Coverage must be fully portable.

The act authorizes OPM to contract with qualified carriers without competitive bidding. It sets out terms and conditions for this master contract, which normally shall be for seven years. One requirement is that premiums should reasonably and equitably reflect the benefits provided, as determined by OPM, and not be adjusted during the term of the contract unless adjustment is mutually agreed to by OPM and the carrier.

Individuals obtaining coverage are responsible for 100% of the premiums. Withholding from pay or annuities is authorized. Administrative start-up costs may be paid out of the Employees' Life Insurance Fund, with reimbursement from the carriers within the first year. Subsequently, carriers are to make periodic contributions to a Long-Term Care Administrative Account within this fund to defray OPM expenses in administering the program.

[1063] Federal and Postal Service employees generally may participate in the long-term care insurance program if they are eligible to participate in the Federal Employees Health Benefit (FEHB) program, whether or not they actually do.

Contract terms relating to the nature, provision, and extent of coverage or benefits supersede and preempt state or local laws or regulations. Cost accounting standards issued pursuant to Section 26(f) of the Office of Federal Procurement Policy Act do not apply.

The act provides for various reports and record keeping, including evaluations by the General Accounting Office (GAO) before the end of the third and fifth years of the program. Within 180 days after receiving the second GAO report, the President shall submit to Congress written recommendations as to whether the program should be continued without modification, terminated, or restructured.

OPM has authority to prescribe necessary regulations for the program. In consultation with the carriers, it is to provide periodic coordinated enrollment, promotion, and education efforts. In addition, OPM is to ensure that applicants are furnished information needed to evaluate the advantages and disadvantages of obtaining long-term care insurance, including information about costs and benefits, the effects of inflation, circumstances when premiums may be raised, and other matters.

Discussion

Long-term insurance can help protect the income and assets of people who need daily assistance due to frailty or chronic medical conditions. Coverage can also help people gain access to better-quality or additional services, either in nursing homes or in the community or at home. While there has been a steady increase in the number of long-term care policies sold over the last decade, only a small proportion of the generation nearing retirement has obtained coverage. One reason is cost: typically, long-term care insurance is purchased by people in their 50s or 60s, when the annual cost is higher than if bought earlier. Another reason is complexity: long-term care insurance is difficult even for financially astute people to understand. In addition, some people are concerned that premiums will increase at some point in the future and that they will be forced to drop their policies.[1064]

The federal long-term care insurance program is designed to avoid some of these problems. By offering coverage to all federal employees and their families, not just those approaching retirement, the program attempts to enroll participants when annual costs are lower. There are also cost savings from reduced administrative costs, though these might be partially offset by cost increases from different underwriting standards. The program's educational material and clear information about costs are aimed at helping people make prudent choices about

[1064] Long-term care insurance usually is sold for premiums that stay the same in subsequent years (unless the policy-holder later elects to purchase inflation protection); however, this is not guaranteed.

benefits. While there is no guarantee that premiums will not be raised in the future, OPM oversight (and the possibility of congressional review) may make this less likely than for insurance sold in the private market.

As of the end of 2003, a little over 200,000 policies had been obtained through the program.

Selected Source Reading

American Academy of Actuaries. Long-Term Care: Actuarial Issues in Designing Voluntary Federal-Private LTC Insurance Programs. Washington: 1999.

Coronel, Susan A. Long-Term Care Insurance in 2000-2003. Health Insurance Association of America. Washington: 2003.

Long Term Care Partners. Information about the long-term care insurance program for federal workers is available through the company's website, at [http://www.ltcfeds.com], visited January 26, 2004.

National Association of Insurance Commissioners. A Shopper's Guide to Long-term Care Insurance. Kansas City, MO: 2003.

U.S. Congress. House. Committee on Government Reform. Long-Term Care Security Act. Part 1, to accompany H.R. 4040. H.Rept. 106-610. Washington: GPO, 2000.

——. Senate. Committee on Governmental Affairs. Long-Term Care Security Act. Report to accompany S. 2420. S.Rept. 106-344. Washington: GPO, 2000.

U.S. Office of Personnel Management. Information about the long-term care insurance program for federal workers is available through the OPM website, at [http://www.opm.gov/insure/ltc], visited January 26, 2004.

Bob Lyke

(37) Personnel Flexibilities Relating to the Internal Revenue Service (Chapter 95; in Part III, Subpart I — Miscellaneous).

Statutory Intent and History

Subtitle C of the Internal Revenue Service (IRS) Restructuring and Reform Act of 1998 (112 Stat. 711) at Section 1201 amended Part III of Title 5, United States Code, by adding a new Subpart I — "Miscellaneous," and Chapter 95 — "Personnel Flexibilities Relating to the IRS." The legislation was based on the report of the National Commission on Restructuring the IRS, which recommended that the IRS and the Department of the Treasury be given more flexibility to hire qualified personnel needed to implement modernization. The intent of the law was to make various personnel rules and procedures on hiring, evaluating, promoting, and firing employees more flexible; to foster creativity, innovation, and quick problem resolution among employees; and to increase the accountability of IRS managers and employees and their focus on the mission, goals, and objectives of the agency. The law also was designed to revitalize the IRS workforce and change the culture of the agency so that it would be an efficient, modern, and responsive organization designed to meet the needs of taxpayers.

Major Provisions

A summary of some of the major provisions follows.

Under Section 9501, the personnel flexibilities are to be exercised in a manner consistent with Title 5, United States Code, provisions on merit system principles; prohibited personnel practices; veterans' preference; and, except as otherwise specifically provided, labor-management relations. Employees within a unit to which a labor organization is accorded exclusive recognition shall not be subject to various flexibilities unless the IRS and the labor organization enter into a written agreement which specifically provides for the exercise of the flexibility. The written agreement may be imposed by the Federal Services Impasses Panel.

When the Secretary of the Treasury seeks a grant of critical pay authority for one or more positions at the IRS, the Office of Management and Budget, under Section 9502, may fix the basic pay rate at any rate up to the Vice President's salary ($198,600 as of January 2003). The Secretary of the Treasury is authorized, under Section 9503, to establish, fix the compensation of, and appoint individuals to, designated critical administrative, technical, and professional positions in the IRS until July 22, 2008 (10 years after enactment of the law). The positions are those that require expertise of an extremely high level in an administrative, technical, or professional field and are critical to the IRS's successful accomplishment of its mission. Exercise of the authority is necessary to recruit or retain an individual exceptionally well qualified for the position. The number of critical positions may not exceed 40 at any one time. The terms of

such appointments may not exceed four years. Total annual compensation for critical positions may not exceed the highest total annual compensation payable to the Vice President.

The Secretary of the Treasury is authorized, under Section 9504, subject to approval by the Office of Personnel Management (OPM), to provide for variations from current law on recruitment, relocation, and retention incentives until July 22, 2008 (10 years after enactment of the law). IRS senior executives with program management responsibility over significant IRS functions may be paid a performance bonus if the Secretary of the Treasury, under Section 9505, finds the award warranted by the executive's performance. This authority continues until July 22, 2008 (10 years after enactment of the law). The bonus is not subject to 5 U.S.C. § 5384(b)(2), which limits Senior Executive Service performance awards to no less than 5% or more than 20% of basic pay. The executive's performance will be evaluated by the Secretary's taking into account contributions toward the successful accomplishment of goals and objectives specified in certain laws and by performance metrics or plans. Any award that exceeds 20% of an executive's basic pay rate must be approved by the Secretary. A performance bonus award may not be paid to an executive in a calendar year if, or to the extent that, the executive's total annual compensation will exceed the maximum amount of total annual compensation payable to the Vice President.

In applying 5 U.S.C. § 3132, career reserved position in the IRS means a position which may be filled only by a career appointee; or a limited emergency appointee or a limited term appointee who, immediately upon entering the career-reserved position, was serving under a career or career-conditional appointment outside the Senior Executive Service (SES); or whose limited emergency or limited term appointment is approved in advance by OPM (Section 9506). The number of positions filled by limited emergency or limited term appointees may not exceed 10% of the total number of SES positions in the IRS. The term of a limited emergency or limited term appointee may not exceed three years.

The exercise of any of the flexibilities under Sections 9502 through 9510 shall not affect the Secretary of the Treasury's authority, under Section 9507, to implement a demonstration project for the IRS, subject to 5 U.S.C. Chapter 47. The law specifies various requirements for a demonstration project.

Under Section 9508, the Secretary of the Treasury established a performance management system for the IRS in lieu of a system established under 5 U.S.C. § 4302. The system will maintain individual accountability by establishing one or more retention standards for each employee related to his or her work and expressed in terms of individual performance. The standards will be communicated to employees. Periodic determinations of whether each employee does or does not meet his or her established retention standards will be made. With respect to any employee whose performance does not meet established retention standards, actions could be taken including denying basic pay increases, promotions, and credit for performance during a reduction in force.

The performance system will establish goals or objectives for individual, group, or organizational performance (or any combination thereof) that are consistent with IRS performance planning procedures and also will provide for communicating goals or objectives to employees and will use such goals and objectives to make performance distinctions among employees or groups of employees. An employee's performance will be considered "unacceptable" if it fails to meet a retention standard.

The Secretary of the Treasury may establish an awards program designed to provide incentives for and recognition of organizational, group, and individual achievements. It will provide for awards to employees who, as individuals or members of a group, contribute to meeting performance goals and objectives by such means as superior individual or group accomplishment, a documented productivity gain, or sustained superior performance.

The notice period for actions based on unacceptable performance or adverse actions is 15 days. An IRS employee may not appeal the denial of a periodic step increase to the Merit Systems Protection Board.

The Secretary of the Treasury, under Section 9509, may, subject to OPM criteria, establish one or more broad-banded systems covering all or any portion of the IRS workforce. Such a system has been established for IRS managers and supervisors. Broad-banded system means a system for grouping positions for pay, job evaluation, and other purposes that differs from the General Schedule classification system as a result of combining grades and related ranges of rates of pay in one or more occupational series. The law specifies requirements for the OPM criteria.

An IRS employee may be selected for a permanent appointment in the competitive service in the IRS through internal competitive promotion procedures, under Section 9510, subject to meeting certain conditions stated in the law. The Secretary of the Treasury may establish category rating systems for evaluating applicants for IRS positions in the competitive service. Qualified candidates will be divided into two or more quality categories on the basis of relative degrees of merit, rather than assigned individual numerical ratings. Each applicant who meets the minimum qualification requirements for the position to be filled shall be assigned to an appropriate category based on an evaluation of his or her knowledge, skills, and abilities relative to those needed for successful performance in the job to be filled. Within each quality category, preference eligibles shall be listed ahead of other individuals. For other than scientific and professional positions at or higher than GS9 (or equivalent), preference eligibles with a compensable service-connected disability of 10% or more, and who meet the minimum qualification standards, will be listed in the highest quality category. An appointing authority may select any applicant from the highest quality category. If fewer than three candidates have been assigned to the highest quality category, the individual may be selected from a merged category consisting of the highest and second highest quality categories. The appointing

authority may not pass over a preference eligible in the same or a higher category from which the selection is made, unless the requirements of 5 U.S.C. § 3317(b) or § 3318(b) are satisfied.

The Secretary of the Treasury may detail employees among IRS offices without regard to current law, which limits details and renewals of details to 120 days. A probationary period of up to three years may be established by the Secretary of the Treasury for IRS positions that require a longer period for the incumbent to demonstrate complete proficiency. The IRS Commissioner was authorized to pay voluntary separation incentive payments (VSIP) up to $25,000 to any employee who voluntarily separated (whether by retirement or resignation) before January 1, 2003 (Section 1202).

Section 1203 of the act authorizes the IRS Commissioner to terminate any IRS employee if there is a final administrative or judicial determination that the employee committed any act or omission in performing his or her official duties. The termination shall be a removal for cause on charges of misconduct. The acts or omissions which could result in termination are the following.

- willful failure to obtain the required approval signatures on documents authorizing the seizure of a taxpayer's home, personal belongings, or business assets;
- providing a false statement under oath with respect to a material matter involving a taxpayer or taxpayer representative;
- with respect to a taxpayer, taxpayer representative, or other employee of the Internal Revenue Service, the violation of — (A) any right under the Constitution of the United States; or (B) any civil right established under — (i) Title VI or VII of the Civil Rights Act of 1964; (ii) Title IX of the Education Amendments of 1972; (iii) the Age Discrimination in Employment Act of 1967; (iv) the Age Discrimination Act of 1975; (v) Section 501 or 504 of the Rehabilitation Act of 1973; or (vi) Title I of the Americans with Disabilities Act of 1990;
- falsifying or destroying documents to conceal mistakes made by any employee with respect to a matter involving a taxpayer or taxpayer representative;
- assault or battery on a taxpayer, taxpayer representative, or other IRS employee, but only if there is a criminal conviction, or a final judgment by a court in a civil case, with respect to the assault or battery;
- violations of the Internal Revenue Code of 1986, Department of the Treasury regulations, or IRS policies (including the Internal Revenue Manual) for the purpose of retaliating against, or harassing, a taxpayer, taxpayer representative, or other IRS employee;
- willful misuse of the provisions of Section 6103 of the Internal Revenue Code of 1986 for the purpose of concealing information from a congressional inquiry;
- willful failure to file any return of tax required under the Internal Revenue Code of 1986 on or before the date prescribed therefor (including any

extensions), unless such failure is due to reasonable cause and not to willful neglect;
- willful understatement of federal tax liability, unless such understatement is due to reasonable cause and not to willful neglect; and
- threatening to audit a taxpayer for the purpose of extracting personal gain or benefit.

The IRS Commissioner, at his or her sole discretion, may take a personnel action other than termination for an act or omission and may establish a procedure which will be used to determine whether an individual should be referred to the Commissioner for a determination on a personnel action. Any determination of the Commissioner may not be appealed in any administrative or judicial proceeding.

Under Section 1204 of the act, the IRS shall not use records of tax enforcement results to evaluate employees or to impose or suggest production quotas or goals with respect to such employees. The IRS shall use the fair and equitable treatment of taxpayers by employees as one of the standards for evaluating employee performance. Each appropriate supervisor shall certify quarterly by letter to the IRS Commissioner whether or not tax enforcement results are being used in a manner prohibited by this section. The IRS Commissioner implemented an employee training program under Section 1205 of the act. The law specified requirements for the training plan.

Discussion

Among issues related to implementation of the law, those on employee misconduct, training, and critical pay authority have been closely followed. Recent audits conducted by the Treasury Inspector General for Tax Administration (TIGTA) found that allegations of employee misconduct were accurately reported; training data are not adequate or reliable enough for the IRS Oversight Board to perform an assessment (costs of training courses and allocation of training resources cannot be determined); and the Secretary of the Treasury and the board need to exercise additional scrutiny to ensure that the critical pay authority is used appropriately. In its 2003 review of the IRS, the Joint Committee on Taxation determined that serious employee misconduct remains at low levels (more than 90% of the Section 1203 violations involve employee tax compliance), and anxiety about Section 1203 contributes to a decline in enforcement activity. The IRS reported to the Joint Committee that the streamlined critical pay authority has resulted in the recruitment of talented executives with wide-ranging skills.

Various bills were introduced in the 106th and 107th Congresses to amend the Section 1203 provisions on termination of employment for misconduct. In the 108th Congress, the following bills are pending: H.R. 1528, Taxpayer Protection and IRS Accountability Act of 2003, as passed by the House, and H.R. 1661, Taxpayer and Fairness Protection Act of 2003, both to amend Section 1203 with

regard to disciplinary actions and to add a reporting requirement that misconduct allegations be summarized by category; S. 1637, Jumpstart Our Business Strength (JOBS) Act, as reported to the Senate, to prohibit an individual who violates Section 1203 from receiving a tax collection contract; S. 882, Tax Administration Good Government Act, to amend Section 1203 and to provide that the use of critical pay authority be approved by the IRS Oversight Board; and H.R. 3625, Department of the Treasury Inspector General Consolidation Act of 2003, to add a requirement that the Inspector General's report include misconduct cases.

Selected Source Reading

Congress. Conference Committee. Internal Revenue Service Restructuring and Reform Act of 1998, Conference Report to Accompany H.R. 2676. 105th Congress, 2nd session. H.Rept. 105-599. Washington: GPO, 1998.

Congress. House. Committee on Ways and Means. Internal Revenue Service Restructuring and Reform Act of 1997, Report to Accompany H.R. 2676. 105th Congress, 1st session. H.Rept. 105-364, part 1. Washington: GPO, 1997.

Congress. Joint Committee on Taxation. Report of the Joint Committee on Taxation Relating to the Internal Revenue Service As Required by the IRS Reform and Restructuring Act of 1998. JCX-53-03. Washington: GPO, 2003, pp. 42-50.

Congress. National Commission on Restructuring the Internal Revenue Service. A Vision for a New IRS. Washington: GPO, 1997.

Congress. Senate. Committee on Finance. Internal Revenue Service Restructuring and Reform Act of 1998, Report to Accompany H.R. 2676. S.Rept. 105-174. 105th Congress, 1st session. Washington: GPO, 1998.

Department of the Treasury. Treasury Inspector General for Tax Administration. Employee Misconduct Allegations Were Accurately Reported. 2003-10-184. Washington: TIGTA, 2003.

——. Information on Employee Training Is Not Adequate to Determine Training Cost or Effectiveness. 2003-10-212. Washington: TIGTA, 2003.

——. Oversight of Streamlined Critical Pay Authority Could Be Improved. 200310-116. Washington: TIGTA, 2003.

U.S. General Accounting Office. IRS and TIGTA Should Evaluate Their Processing of Employee Misconduct Under Section 1203. GAO-03-394. February 2003.

——. Tax Administration; IRS' Implementation of the Restructuring Act's Personnel Flexibility Provisions. GAO/GGD-00-81. April 2000.

Barbara L. Schwemle

(38) Department of Homeland Security (Chapter 97; in Part III, Subpart I — Miscellaneous).

Statutory Intent and History

The Homeland Security Act of 2002 (P.L. 107-296; 116 Stat. 2229) authorized the creation of a new human resources management (HRM) system for employees of the Department of Homeland Security (DHS). In the aftermath of the September 11, 2001 terrorist attacks on the World Trade Center and the Pentagon, and the discovery of anthrax in Washington, DC, and other cities, Congress and the Administration determined that a new Cabinet-level department was needed to coordinate efforts to protect the nation from terrorist attacks. As part of creating that new department, the Administration believed strongly that, to meet the exigencies of national security and emergency situations, a flexible and modern HRM system for DHS was mandated. The President frequently referred to the requirements of that system as putting the right people in the right place at the right time. (See the discussion at 5 U.S.C. Chapter 99 for information on the new HRM system at the Department of Defense.)

Major Provisions

Title VIII, Subtitle E, Section 841 of the Homeland Security Act amends Title 5 United States Code by adding a new Chapter 97 — "Department of Homeland Security" to Part III, Subpart I. The new Section 9701(a) of Title 5 United States Code provides that, notwithstanding any other provision of Part III, the Secretary of Homeland Security may, in regulations prescribed jointly with the Director of the Office of Personnel Management, establish, and from time to time adjust, an HRM system for some or all of the organizational units of DHS.

The HRM system must be flexible and contemporary. It cannot waive, modify, or otherwise affect:

- the public employment principles of merit and fitness at 5 U.S.C. § 2301, including the principles of hiring based on merit, fair treatment without regard to political affiliation or other non-merit considerations, equal pay for equal work, and protection of employees against reprisal for whistleblowing;
- any provision of 5 § 2302 relating to prohibited personnel practices;
- any provision of law referred to in 5 U.S.C. § 2302(b)(1), (8), and (9); or any provision of law implementing any provision of law referred to in 5 U.S.C. § 2302(b)(1), (8), and (9) by providing for equal employment opportunity through affirmative action; or providing any right or remedy available to any employee or applicant for employment in the civil service;
- Subparts A (General Provisions), B (Employment and Retention), E (Attendance and Leave), G (Insurance and Annuities), and H (Access to Criminal History Record Information) of Part III of Title 5, United States Code; and Chapters 41 (Training), 45 (Incentive Awards), 47 (Personnel Research Programs and Demonstration Projects), 55 (Pay

Administration), 57 (Travel, Transportation, and Subsistence), 59 (Allowances), 72 (Antidiscrimination, Right to Petition Congress), 73 (Suitability, Security, and Conduct), and 79 (Services to Employees) of Title 5; or
- any rule or regulation prescribed under any provision of law referred to in any of the statements in bullets immediately above.

The use of a category rating system for evaluating applicants for positions in the competitive service is permitted under the new system.

Nothing in the new Section 9701 constitutes authority to:

- modify the pay of any employee who serves in an Executive Schedule position or a position for which the rate of basic pay is fixed in statute by reference to the Executive Schedule;
- fix pay for any employee or position at an annual rate greater than the maximum amount of cash compensation allowable under 5 U.S.C. § 5307 in a year; or
- exempt any employee from the application of 5 U.S.C. § 5307.

It is the sense of the Congress that employees of DHS are entitled to fair treatment in any appeals that they bring in decisions relating to their employment. In prescribing regulations for any such appeals procedures, the Secretary of Homeland Security and the Director of OPM should ensure that employees of the department are afforded the protections of due process and, toward this end, should be required to consult with the Merit Systems Protection Board (MSPB) before issuing any such regulations. Any regulations which relate to any matters within the purview of Chapter 77 (on appeals) must be issued only after consultation with the MSPB and must ensure the availability of procedures which must be consistent with requirements of due process and provide, to the maximum extent practicable, for the expeditious handling of any matters involving DHS. Any regulations must modify procedures under Chapter 77 only insofar as such modifications are designed to further the fair, efficient, and expeditious resolution of matters involving the employees of DHS.

The law also includes provisions related to labor management relations and collective bargaining. (See 5 U.S.C. Chapter 71 in this compendium.)

Effective five years after the conclusion of the transition period defined under Section 1501 of the act (a 12-month period beginning 60 days after the act's enactment date of November 25, 2002), all authority to issue regulations under the section (including regulations which would modify, supersede, or terminate any regulations previously issued under the section) must cease to be available.

Except as otherwise provided in the Homeland Security Act, the transfer, under this act, of full-time personnel (except special government employees) and part-time personnel holding permanent positions must not cause any such employee

to be separated or reduced in grade or compensation for one year after the date of transfer to DHS. A person who, on the day preceding his or her date of transfer to the new department, held a position compensated on the Executive Schedule, and who, without a break in service, is appointed in DHS to a position having duties comparable to the duties performed immediately preceding such appointment, must continue to be compensated in the new position at not less than the rate provided for the previous position, for the duration of service in the new position. Any exercise of authority under the new Chapter 97, including under any system established under the chapter, must be in conformance with these requirements.

In authorizing the establishment of an HRM system for the new department, Congress stated that —

[I]t is extremely important that employees of the Department be allowed to participate in a meaningful way in the creation of any human resources management system affecting them; [S]uch employees have the most direct knowledge of the demands of their jobs and have a direct interest in ensuring that their human resources management system is conducive to achieving optimal operational efficiencies; [T]he 21st century human resources management system envisioned for the Department should be one that benefits from the input of its employees; and [T]his collaborative effort will help secure our homeland.

Discussion

On April 1, 2003, Secretary of Homeland Security Tom Ridge and OPM Director Kay Coles James announced that they were launching the process for designing a new HRM system for DHS. The following process is being used to create the system:

- A Design Team conducted research and outreach to provide a full range of options for a Senior Review Committee to consider. The team included DHS program managers from all directorates and disciplines, union and employee representatives, and human resource specialists from DHS and OPM. Expert consultants from the private sector also supported the team.
- A Senior Review Committee (SRC) is developing personnel system options to be considered by the Secretary and the Director and their senior staff. The committee included, among others, the Under Secretary for Management, department program leaders, officials from OPM, and major union leaders. A small number of academics and policy experts served as ex officio members who advised the committee on specific issues.

The design team began work on April 1, 2003, and conducted field meetings in several cities, including New York City, Miami, Detroit, El Paso, Atlanta, Seattle, and Salt Lake City, locales with the largest concentrations of DHS employees. Testimony was received from more than 2,000 DHS employees, including 44 employee focus groups and 10 manager focus groups. The field meetings

concluded in late June 2003. On July 25, 2003, the design team reported to the SRC on these field meetings. Pay, performance management, and labor-management relations were among the issues discussed.

On October 3, 2003, the design team presented its final report with 52 options for the new HRM to the SRC.[1065] None of the options represents the consensus of the design team and none covers the Senior Executive Service (SES). Modifications to Title 5 United States Code pay and performance management provisions for the SES will be addressed through a separate process. The options are grouped into two categories: (1) Pay, Performance Management, and Classification and (2) Labor Relations, Adverse Actions, and Appeals. Among the options in the first category are those which would continue or amend the current General Schedule pay system; establish a compensation system based on pay bands; create a system based on longevity, competency, and performance; and continue or amend the existing performance management system. Options under the second category include continuing the current labor relations procedures, providing for national level bargaining, continuing or amending the current adverse actions and appeals procedures, creating an Ombudsman Office, and establishing procedures for alternative dispute resolution. The SRC examined and deliberated the options at a public meeting conducted October 20 through October 22, 2003. A summary of the proceedings was published on December 5, 2003.[1066] The committee will "present a refined range of options to the Secretary and the Director," who will then issue proposed rules. Employee representatives and Congress will be notified, and any differences will be reconciled. The Secretary and the OPM Director jointly issued proposed regulations for the new human resources management system on February 20, 2004.[1067]

While there is consensus on the broad principles that should govern a new HRM system, DHS employees, some Members of Congress, and knowledgeable HRM observers are beginning discussions about the rules that will implement the new system. To this point, discussions have focused only on the design team process.

Selected Source Reading

Armey, Representative Dick. "Homeland Security Act of 2002." Remarks in the

---

[1065] See [http://www.opm.gov/Strategic_Management_of_Human_Capital/HC_Systems/DHS/index.asp], visited Dec. 16, 2003.

[1066] See [http://www.opm.gov/Strategic_Management_of_Human_Capital/HC_Systems/DHS/SeniorReview CommitteeMeeting.asp], visited Dec. 16, 2003.

[1067] For more information, see CRS Report RL32261, Homeland Security: Proposed Regulations on Job Evaluation, Pay, and Performance Management Compared with Current Law, by Barbara L. Schwemle.

House. Congressional Record, daily edition, vol. 148 (November 13, 2002), pp. H8595-H8645.

Daalder, Ivo H., et al. Protecting the American Homeland: One Year On. Washington: The Brookings Institution, 2003.

Partnership for Public Service. Homeland Security: Winning the War for Talent to Win the War on Terror. Washington: The Partnership, 2002.

Congress. House. Committee on Government Reform. Subcommittee on Civil Service and Agency Reorganization. Decision Time: A New Human Resources Management System at the Department of Homeland Security. Hearing. 108th Congress, 1st session, October 29, 2003. Unpublished.

General Accounting Office. Human Capital; DHS Personnel System Design Effort Provides for Collaboration and Employee Participation. GAO-03-1099. September 2003.

CRS Report RL31520. Collective Bargaining and Homeland Security, by Jon O. Shimabukuro.

CRS Report RL31548. Homeland Security Department Proposals: Scope of Personnel Flexibilities, by Thomas J. Nicola.

CRS Report RL31500. Homeland Security: Human Resources Management, by Barbara L. Schwemle.

Barbara L. Schwemle

(39) Department of Defense National Security Personnel System (Chapter 99; in Part III, Subpart I — Miscellaneous).

Statutory Intent and History

The National Defense Authorization Act for FY2004 (P.L. 108-136, Section 1101; 117 Stat. 1621) authorizes the creation of a new human resources management (HRM) system, to be called the National Security Personnel System (NSPS), for civilian employees (some 735,000) of the Department of Defense (DOD). The NSPS provisions were included in a DOD proposal entitled "The Defense Transformation for the 21st Century Act" that was submitted to Congress in April 2003.[1068] According to the proposal, DOD's responsibility to defend the security of the nation requires that the department's HRM system incorporate enhanced flexibilities to recruit, develop, assess, compensate, assign, and separate employees. With the new authority under the NSPS, DOD stated that it will be able to fold innovations from its ongoing demonstration projects as well as best practices from throughout the federal government into its strategic plan for civilian human resources management.

Major Provisions

Section 1101(a)(1) of the National Defense Authorization Act amends Part III, Subpart I, of Title 5, United States Code, by adding a new Chapter 99 entitled "Department of Defense National Security Personnel System." The new Section 9902(a) provides that notwithstanding any other provision of Part III, the Secretary of Defense may, in regulations prescribed jointly with the OPM director, establish, and from time to time adjust, an HRM system for some or all of the organizational or functional units of DOD. The system must be flexible and contemporary and, under the new Section 9902(b), cannot waive, modify, or otherwise affect:

- the public employment principles of merit and fitness at 5 U.S.C. § 2301, including the principles of hiring based on merit, fair treatment without regard to political affiliation or other non-merit considerations, equal pay for equal work, and protection of employees against reprisal for whistleblowing;
- any provision of 5 U.S.C. § 2302, relating to prohibited personnel practices;
- any provision of law referred to in 5 U.S.C. § 2302(b)(1), (8), and (9); or any provision of law implementing any provision of law referred to in 5 U.S.C. § 2302(b)(1), (8), and (9) by providing for equal employment opportunity through affirmative action; or providing any right or remedy

[1068] See [http://www.defenselink.mil/dodgc/lrs/docs/Transformation.pdf], visited Dec. 18, 2003.

available to any employee or applicant for employment in the public service.

The new Section 9902(d) lists various subparts and chapters of Part III of Title 5, United States Code (including applicable rules and regulations) which cannot be waived, modified, or otherwise affected in the new HRM system as follow:

Subpart A — General Provisions, including Chapter 21, Definitions; Chapter 23, Merit System Principles; Chapter 29, Commissions, Oaths, Records, and Reports;

Subpart B — Employment and Retention, including Chapter 31, Authority for Employment; Chapter 33, Examination, Selection, and Placement; Chapter 34, Part-time Career Employment Opportunities; Chapter 35, Retention Preference (RIF), Restoration, and Reemployment;

Subpart E — Attendance and Leave, including Chapter 61, Hours of Work; Chapter 63, Leave;

Subpart G — Insurance and Annuities, including Chapter 81, Compensation for Work Injuries; Chapters 83 and 84, Retirement; Chapter 85, Unemployment Compensation; Chapter 87, Life Insurance; Chapter 89, Health Insurance; Chapter 90, Long Term Care Insurance;

Subpart H — Access to Criminal History Record Information, including
Chapter 91 for individuals under investigation; Chapter 41 — Training; Chapter 45 — Incentive Awards;
Chapter 47 — Personnel Research Programs and Demonstration Projects; Chapter 55 — Pay Administration, including biweekly and monthly pay periods
and computation of pay, advanced pay, and withholding of taxes from pay, except that Subchapter V of Chapter 55 on premium pay (overtime, night, Sunday pay), apart from Section 5545b, may be waived or modified;
Chapter 57 — Travel, Transportation, and Subsistence; Chapter 59 — Allowances, which includes uniforms, quarters, overseas
differentials; Chapter 71 — Labor Management and Employee Relations; Chapter 72 — Antidiscrimination, Right to Petition Congress, including
minority recruitment, antidiscrimination on the basis of marital status and handicapping condition, furnishing information to Congress;

Chapter 73 — Suitability, Security, and Conduct, including security clearance, political activities (Hatch Act), misconduct (gifts, drugs, alcohol); Chapter 79 — Services to Employees, including safety program, protective clothing and equipment; or
Other requirements for the HRM system include that it shall:

- ensure that employees could organize, bargain collectively as provided for in the proposed Chapter 99, and participate through labor organizations of their own choosing in decisions that affect them, subject to the provisions

of the proposed Chapter 99 and any exclusion from coverage or limitation on negotiability established pursuant to law; and
- include a performance management system. Requirements for the system are specified in the law.

The NSPS shall not apply with respect to various DOD laboratories before October 1, 2008, and shall apply on or after October 1, 2008, only to the extent that the Secretary determines that the flexibilities provided by the NSPS are greater than the flexibilities already provided to these laboratories.

Nothing in Section 9902 shall constitute authority to modify the pay of any employee who serves in an Executive Schedule position. Except for this provision, the total amount of allowances, differentials, bonuses, awards, or other similar cash payments paid under Title 5 in a calendar year to various senior executives may not exceed the total annual compensation payable to the Vice President ($198,600 as of January 2003).

To the maximum extent practicable, the rates of compensation for civilian DOD employees shall be adjusted at the same rate, and in the same proportion, as are rates of compensation for members of the uniformed services. In addition, to the maximum extent practicable, for FY2004 through FY2008, the overall amount allocated for compensation of the civilian employees of an organizational or functional unit of DOD that is included in the NSPS shall not be less than the amount of civilian pay that would have been allocated for compensation of such employees for such fiscal year if they had not been converted to the NSPS.

The law requires the Secretary of Defense and the Director of the OPM to provide a written description of the proposed personnel system or any adjustments to such system to the labor organizations representing employees in the department. The measure identifies a collaboration procedure that must be followed by the Secretary, Director, and employee representatives. The Secretary is authorized to engage in any collaboration activities at an organizational level above the level of exclusive recognition. The Secretary is given similar authority to engage in collective bargaining with employee representatives at a level above the level of exclusive recognition. Finally, the Secretary and Director are authorized to establish and adjust a labor relations system for the department. Collaboration with employee representatives on the development of the system is required.

The new Section 9902(h) authorizes the Secretary of Defense to establish an appeals process that provides fair treatment for DOD employees who will be covered by the NSPS. Regulations for the appeals process, applicable to employee misconduct or performance that fails to meet expectations, may not be prescribed until after the Secretary consults with the Merit Systems Protections Board (MSPB) and must afford due process protections and conform to public employment principles of merit and fitness set forth in 5 U.S.C. § 2301. A qualifying employee subject to some severe disciplinary actions shall have a right

to petition the MSPB for review of the record of the department's decision. The board is authorized to dismiss any petition that does not raise a substantial question of fact or law and to order corrective action only if the board finds that the department's personnel decision did not meet some prescribed standards. An employee adversely affected by a final decision or order of the board shall be able to obtain judicial review.

A new Section 9902(i) authorizes the Secretary of Defense, without review by OPM, to offer (1) early retirement to employees who are age 50 or older with 20 years of service or any age with 25 years of service and (2) separation incentive pay of up to $25,000 to DOD employees who retire or resign. The law also includes provisions on re-employment within DOD without loss of annuity.

The Secretary may apply the NSPS (1) to an organizational or functional unit that includes up to 300,000 civilian DOD employees and (2) to more than 300,000 DOD civilian employees, if the Secretary determines that the department has in place a performance management system that meets the criteria specified in the law.

The law also allows the Secretary to appoint personnel from outside the civil service and uniformed services to positions in DOD without regard to any Title 5 provisions governing such. The Secretary may provide allowances and benefits that would be comparable to those provided to members of the Foreign Service or to personnel of the Central Intelligence Agency to certain civilian DOD employees who are engaged in hazardous activities or specialized functions and assigned to activities outside the United States.

Discussion

During testimony before the House Committee on Government Reform and the Senate Committee on Governmental Affairs and their relevant subcommittees, DOD officials discussed the department's Best Practices Initiative and referred Members of Congress to an April 2, 2003, Federal Register notice for additional details on the types of HRM flexibilities the department is implementing at its science and technology reinvention laboratories and would seek to implement under the NSPS. Authority for streamlined recruitment and candidate ranking, universal pay banding for five career groups, merit-based pay, and simplified appointment procedures were among the flexibilities DOD requested.

The General Accounting Office (GAO) testified about the NSPS proposal before the House Committee on Government Reform's Subcommittee on Civil Service and Agency Organization and the Senate Committee on Governmental Affairs' Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia. GAO emphasized that DOD's performance appraisal system, as currently designed, does not support meaningful performance-based pay; that personnel management flexibilities currently available should be used fully as appropriate; that many of the features of the

NSPS, including pay banding and pay for performance, should be considered for application government-wide; and that DOD should work together with labor representatives and stakeholders in implementing the new HRM system (something that was not done as the NSPS proposal was developed and submitted to Congress).

The conference agreement on H.R. 1588 incorporated some of the provisions of S. 1166, the National Security Personnel System Act, as reported (without written report). These provisions, among others, related to requirements for a performance management system, appellate procedures, and labor management relations and collective bargaining. All of these features were in contention and widely debated before agreement was reached. Another contentious provision that would have authorized the Secretary to waive the requirement that the HRM regulations be jointly prescribed by DOD and OPM for reasons of national security was dropped in conference. (Earlier, provisions included in H.R. 1836, the Civil Service and National Security Personnel Improvement Act, as reported, were added to H.R. 1588 during House Committee on Armed Services markup.) The conference agreement directs the Secretary to implement an evaluation system that better links individual pay to performance and provides an equitable method for appraising and compensating employees. Regulations to implement the system are, among other features, to provide for grouping employees into pay bands and establishing performance factors to be used to evaluate whether performance objectives are accomplished. The conference agreement also states that the provisions on collective bargaining should not be construed as expanding the scope of bargaining under 5 U.S.C. Chapter 71.

In a November 2003 briefing document, DOD announced that the NSPS will be built through coordination with OPM and collaboration with employee representatives. There will be a minimum 90-day period of discussion, mediation, and notification to Congress of differences. Discussions began in January 2004, and they continue. Implementation of the NSPS will begin in FY2005 and will continue for at least a two-year period.[1069]

Selected Source Reading

U.S. Congress. Conference Committees, 2003. National Defense Authorization Act for Fiscal Year 2004. Conference report to accompany H.R. 1588. 108th Congress, 1st session. H.Rept. 108-354. Washington: GPO, 2003.

——. House. Committee on Armed Services. National Defense Authorization Act for Fiscal Year 2004. Report to accompany H.R. 1588. 108th Congress, 1st session. H.Rept. 108-106. Washington: GPO, 2003.

[1069] See [http://www.cpms.osd.mil/nsps/index.html], visited Dec. 18, 2003.

——. Committee on Government Reform. Instilling Agility, Flexibility, and a Culture of Achievement in Critical Federal Agencies; A Review of H.R. 1836, the Civil Service and National Security Personnel Improvement Act of 2003. Hearing. 108th Congress, 1st session, May 6, 2003. Unpublished.

——. Subcommittee on Civil Service and Agency Reorganization. Transforming the Defense Department; Exploring the Merits of the Proposed National Security Personnel System. Hearing. 108th Congress, 1st session, April 29, 2003. Unpublished.

——. Senate. Committee on Governmental Affairs. Transforming the Department of Defense Personnel System: Finding the Right Approach. Hearing. 108th Congress, 1st session, June 4, 2003. Unpublished.

——. Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia. An Overlooked Asset: The Defense Civilian Workforce. Hearing. 108th Congress, 1st session, May 12, 2003. Unpublished.

U.S. Department of Defense. "Science and Technology (S&T) Reinvention Laboratory Personnel Management Demonstration Project; Notice of Amendment of Demonstration Project Plans." Federal Register, vol. 68, no. 63 (April 2, 2003), pp. 16119-16142.

U.S. General Accounting Office. Defense Transformation; Preliminary Observations on DOD's Proposed Civilian Personnel Reforms. GAO-03-717T. April 29, 2003.

——. Human Capital; DOD's Civilian Personnel Strategic Management and the Proposed National Security Personnel System. GAO-03-493T. May 12, 2003.

——. Posthearing Questions Related to Proposed Department of Defense (DOD) Human Capital Reform. GAO-03-965R. July 3, 2003.

CRS Report RL31954. DOD's National Security Personnel System: Provisions of Law and Implementation Plans, coordinated by Barbara L. Schwemle.

CRS Congressional Distribution Memorandum. Department of Defense Transformation Proposal (Title I, Subtitle A, Section 101) and H.R. 1588 Conference Report (Title XI, Subtitles A,B,C): A Side-by-Side Comparison, coordinated by Barbara L. Schwemle.

Barbara L. Schwemle

B. Ethics in Government Act

Statutory Intent and History

Passage of the Ethics in Government Act of 1978 (92 Stat. 1824; 5 U.S.C. App.) culminated years of efforts to provide uniform financial disclosure requirements for key officers of the federal government. These efforts gathered momentum in the 1970s, following the Watergate scandal; revelations of impropriety by a number of government officials; polls showing a lack of confidence in public officials; and publication in 1976 of the recommendations of the President's Commission on Executive, Legislative, and Judicial Salaries, which recommended salary increases for top government officials, as well as ethical reforms, including annual public financial disclosure reports.

Major provisions of the act established (1) annual public financial disclosure requirements, (2) an Office of Special Prosecutor (subsequently called the Independent Counsel) to investigate allegations of wrongdoing by top officials in the executive branch, (3) the Office of Government Ethics to monitor executive branch financial disclosure reports and potential conflicts of interest, and (4) the Office of Senate Legal Counsel.

Major Provisions

Titles I through III of the act contain the financial disclosure requirements for the three branches of government, including which officers and employees are covered, contents of the reports (including provisions for reporting the income from trusts), accessibility of reports, review procedures in each branch of government, and penalties for failure to file.[1070] Though the provisions were almost uniform, their interpretation was left to designated officials in each branch.

Title IV originally established the Office of Government Ethics (OGE) within the Office of Personnel Management. OGE became an independent agency in 1989 (102 Stat. 3031). OGE is charged with enforcement of standards of conduct, assisting in the confirmation of presidential appointees, providing guidance to agencies on procedures for monitoring financial disclosure reports, the issuance of standards of conduct and advisory opinions, and developing ongoing ethics programs to educate employees.

Title V revised 18 U.S.C. § 207 to broaden the major conflict of interest provisions governing restrictions on post-service activities by officers and employees of the executive branch by extending existing prohibitions and establishing additional ones for matters on which former employees worked. The purpose is to prevent

[1070] In the Ethics Reform Act of 1989, discussed elsewhere in this compendium, the disclosure provisions for the three branches of government were combined into one title.

former officers and employees from using information gathered during their government service, or exercising undue influence on former colleagues.

Title VI amended 18 U.S.C. § 28 (now expired) by adding provisions for the appointment and duties of a special prosecutor when the Justice Department had a conflict of interest in investigating wrongdoing by the President, Vice President, Cabinet-level officials, or senior White House or Justice Department officials. This provision was the result of the recommendations of the Senate Watergate Committee, and expired in 1999. It has not been reauthorized by Congress since that time.

Title VII established the Office of Senate Legal Counsel to defend the constitutional powers of the Senate in proceedings before the courts and conferred jurisdiction on the courts to enforce Senate subpoenas.

Discussion

Although the Ethics in Government Act was the product of long-term efforts to reform government ethics laws, and OGE has been an integral part of the executive branch ethics program, several provisions in the act have been problematic over the years. There was continuing debate over the wisdom and efficacy of the special proscecutor/independent counsel provisions. In addition, the financial disclosure provisions of the act, particularly as applied to the executive branch, have been viewed by some as making the presidential appointment process unnecessarily long, burdensome, and complex. A number of studies have shown that, in some cases, the ethics laws have been a deterrent to the recruitment of qualified appointees, and there is concern over the increasing amount of time taken to nominate and confirm high-level executive branch appointees.[1071]

Several bills have been introduced in Congress to streamline the financial disclosure requirements for high-level nominees and employees and to require new appointed officials who have not complied with an ethics agreement within the original specified time to file monthly progress reports until all terms of the agreements have been met. These include S. 1811 in the 107th Congress, and S. 765 and H.R. 1603 in the 108th Congress.

Selected Source Reading

Carroll, James D. and Roberts, Robert N. "If Men Were Angels: Assessing the Ethics in Government Act of 1978." Policy Studies Journal, vol. 17 (winter 1988-1989), pp. 435-447.

[1071] U.S. Congress, Senate Committee on Governmental Affairs, Presidential Appointments Improvement Act of 2002, report to accompany S. 1811, 107th Cong., 2nd sess., S.Rept. 107152 (Washington, GPO, 2002), pp. 2-3.

"Congressional Process Symposium." Administrative Law Review, vol. 48 (winter 1996), pp. 31-137.

Thompson, Dennis F. Ethics in Congress: From Individual to Institutional Corruption. Washington: Brookings Institution, 1995.

Congress. Conference Committees. Ethics in Government Act of 1978. Conference report to accompany S. 555. 95th Congress, 2nd session. H.Rept. 95-1756. Washington: GPO, 1978.

Congress. Senate. Senate Committee on Governmental Affairs. Presidential Appointments Improvement Act of 2002. Report to accompany S. 1811. 107th Congress, 2nd session. S.Rept. 107-152. Washington: GPO, 2002.

Congress. Senate Committee on Governmental Affairs. Public Officials Integrity Act of 1977. Report to accompany S. 555. 95th Congress, 2nd session. S.Rept. 95-170. Washington: GPO, 1977.

Mildred Amer

C. Ethics Reform Act of 1989

Statutory Intent and History

The Ethics Reform Act of 1989 (103 Stat. 1716) expanded the coverage of the earlier Ethics in Government Act (1978; 92 Stat. 1824). At the time of passage of the Ethics Reform Act, national attention was directed at what were perceived to be large honoraria earnings by some Members of Congress and the need to clarify existing ethics rules and regulations.

The impetus for the Ethics Reform Act (ERA89) was widely shared. In Congress, task forces in both the Senate and the House offered ethics recommendations. In the 1988 presidential election, candidate George H.W. Bush had promised to make ethics a top priority of his Administration. Soon after his inauguration, President Bush appointed the President's Commission on Federal Ethics Law Reform. Many of its 27 recommendations, including uniformity in ethics regulations in the three branches of government, found their way into the ERA89. Also, a number of recommendations of the private National Commission on the Public Service, established in 1987 and chaired by Paul Volcker, were considered and included. The Volcker Commission was especially concerned about provisions to develop a capable executive talent base in government.

The bill was intended to provide for automatic pay increases for Members of Congress and senior officials in the executive and judicial branches. Previously, annual congressional approval of compensation was often delayed, and compensation was often frozen due to political considerations.

Major Provisions

Major provisions of the ERA89 included:

- pay increases for Members of Congress and senior officials of the other two branches of government and provisions for a 25% adjustment in 1991, as well as annual pay adjustments for these individuals, based on Employment Cost Index (ECI);
- post-employment ("revolving door") lobbying restrictions on Members of Congress, officers, and designated employees of the legislative branch;
- elimination of the so-called "grandfather clause" in federal election law that allowed Members of Congress in office prior to 1980 to convert excess campaign contributions to personal use;
- limitations on outside earned income for Members of Congress and noncareer officers and employees in the three branches of government compensated above a GS-15 level;

- prohibition on honoraria for Members, officers, and employees of the House of Representatives, as well as officers and employees of the executive and judicial branches;[1072] and
- establishment of a Citizen's Committee on Executive, Legislative, and Judicial Salaries to make recommendations to the President for salary rates for top government officials in the three branches.

Discussion

ERA89 is probably best known for its provision on government salaries and its total prohibition on honoraria. The honoraria prohibitions applied to income from speeches and writings, even if unrelated to an official's and employee's government work. Although the provisions applied to all officers and employees in the three branches of government, the initial target was Members of Congress. They were criticized because earning honoraria was viewed as diverting Members' attention from official duties, and was perceived as a way for special interests to gain access to Members.

The automatic annual pay adjustments provided in the act for Members of Congress and other senior officials in the three branches of government were seen as a means for Members to avoid what was considered to be the "painful" act of having to vote on their own salaries. However, Congress has denied itself the annual pay adjustments five times since 1993, denials that also placed a "cap" on top executive branch officials.

Immediately after the ERA89 was enacted, several executive branch employees filed suit against the Justice Department, alleging that the honoraria ban violated the First Amendment right of free speech. In 1995, the Supreme Court overturned the provisions prohibiting honoraria for government employees (National Treasury Employees Union v. United States, 115 S.Ct. 1003 (1995)). The Senate, however, still has an honoraria ban for its officers and employees.

Selected Source Reading

"Are They More Virtuous Today? A Focus On Government Ethics." Federal Bar News and Journal, vol. 37 (September 1990), pp. 378-418.

Biskupic, Joan. "Court Allows Honoraria for Federal Rank and File." The Washington Post, February 23, 1995, p. A1.

[1072] The Senate initially exempted itself from the honoraria and compensation prohibitions. Subsequently, with the enactment of the Legislative Branch Appropriations Act of 1992 (105 Stat. 447), Members, officers, and employees of the Senate could no longer earn honoraria and were subject to the same outside earned income restrictions as the rest of the government. Note: when the House adopted the rules for the 106th Congress, it voted to permit designated employees to earn honoraria for activities not related to their official duties (House Rule XXVI).

"Congressional Process Symposium on Ethics," Administrative Law Review, vol. 48 (winter 1996), pp. 31-138.

Dunbar, Elizabeth. "Congress' Raise Not So Automatic." Minneapolis Star Tribune, September 28, 2003, p. 4A.

Lin, Judy M. "United States v. National Treasury Employees Union and the Constitutionality of the Honoraria Ban: Protecting the First Amendment Rights of Public Employees." University of Richmond Law Review, vol. 29, no. 5 (December 1995), pp. 1555-1590.

Thompson, Dennis F. Ethics in Congress: From Individual to Institutional Corruption. Washington: Brookings Institution, 1995.

Congress. House. Bipartisan Task Force on Ethics. Report of the Bipartisan Task Force on Ethics on H.R. 3660. 101st Congress, 2nd session. Washington: GPO, 1989.

President's Commission on Federal Ethics Law Reform. To Serve with Honor. Washington: The Commission, 1989.

Mildred Amer

D. Lobbying with Appropriated Monies Act

Statutory Intent and History

Many Members of Congress have long been concerned about the practice of federal agencies using appropriated funds to stimulate public support for or opposition to pending legislation. Legislators do not want to be on the receiving end of constituent pressures manufactured by agency telephone calls, telegrams, departmental threats and coercion, and other stimuli originating from within an administration.

To prohibit this practice, Congress passed legislation in 1919, and this statutory restriction (known as the Lobbying with Appropriated Moneys Act) remains part of permanent law. Debate in the House of Representatives reveals that some Members were offended by bureau chiefs and departmental heads "writing letters throughout the country, sending telegrams throughout the country, for this organization, for this man, for that company to write his Congressman, to wire his Congressman, in behalf of this or that legislation." Statutory language was drafted to "absolutely put a stop to that sort of thing."[1073]

Major Provisions

As currently codified (18 U.S.C. § 1913), the Lobbying with Appropriated Moneys Act provides that "No part of the money appropriated by any enactment of Congress shall, in the absence of express authorization by Congress, be used directly or indirectly to pay for any personal service, advertisement, telegram, telephone, letter, printed or written matter, or other device, intended or designed to influence in any manner a Member of Congress, to favor or oppose, by vote or otherwise, any legislation or appropriation by Congress, whether before or after the introduction of any bill or resolution proposing such legislation or appropriation." Section 1913 does not prevent officers or employees from communicating to Members of Congress "on the request of any Member or to Congress, through the proper official channels, requests for legislation or appropriations which they deem necessary for the efficient conduct of the public business." If an officer or employee violates or attempts to violate Section 1913, this person "shall be fined under this title or imprisoned not more than one year, or both; and after notice and hearing by the superior officer vested with the power of removing him, shall be removed from office or employment."

Discussion

The Justice Department has never prosecuted anyone for violating the Lobbying with Appropriated Moneys Act. However, the Justice Department has pointed

---

[1073] Rep. James Good, remarks in the House, Congressional Record, vol. 58 (May 29, 1919), p. 403.

out that the right of citizens to lobby Congress does not mean a right to federal funds for this purpose: "Although private persons and organizations have a right to petition Congress and to disseminate their views freely, they can be expected, within the framework established by the Constitution, to do their lobbying at their own expense. They have no inherent or implicit right to use federal funds for that purpose unless Congress has given them that right." (5 Op. Off. Legal Counsel 180, 185 (1981)).

Statutory sanctions against executive lobbying have had limited effect because of uncertainty about the law and Justice Department interpretations. Due to conflicting statutes, the General Accounting Office (GAO) has at times hesitated to find a violation of agency activity. Former Comptroller General Elmer B. Staats once explained, "The reason for this is that agencies are authorized and, in some cases, specifically directed to keep the public informed concerning their programs. Where such authorized activities involve, incidentally, reference to legislation pending before Congress, it is extremely difficult to draw a dividing line between the permissible and the prohibited."[1074]

Since Section 1913 is a criminal statute, GAO regards its enforcement as "the responsibility of the Department of Justice and the courts. Therefore, GAO will not 'decide' whether a given action constitutes a violation. GAO will, however, determine whether appropriated funds were used in a given instance, and refer matters to the Justice Department in appropriate cases."[1075] Because a violation of Section 1913 constitutes an improper use of appropriated funds, such a violation "could form the basis of a GAO exception or disallowance. However, GAO can take no action unless the Justice Department or the courts first determine that there has been a violation."[1076]

Although the Justice Department has never prosecuted anyone for violating Section 1913, it has indicated the type of executive activity that would be impermissible. A memorandum in 1977 stated that "a campaign to contact a large group of citizens by means of a form letter prepared and signed by a federal official would be improper."[1077] In 1989, the Justice Department restricted

---

[1074] Letter from Comptroller General Elmer Staats to Congressman Thomas B. Curtis, September 7, 1967, cited in Richard L. Engstrom and Thomas G. Walker, "Statutory Restraints on Administrative Lobbying — 'Legal Fiction'," Journal of Public Law, vol. 19 (1970), p. 98.

[1075] U.S. General Accounting Office, Principles of Federal Appropriations Law, 2nd ed., vol. 1 (Washington: GAO, 1991), p. 4-158.

[1076] Ibid.

[1077] Memorandum from John M. Harmon, Assistant Attorney General, Office of Legal Counsel, to Robert J. Lipshutz, Counsel to the President, "Statutory Restraints on Lobbying Activities by Federal Officials," Nov. 29, 1977, p. 10, note 21.

Section 1913 to "a significant expenditure of appropriated funds to solicit pressure on Congress" and a "substantial" grassroots lobbying campaign.[1078]

Judging from the few judicial decisions that have been handed down, it is apparent that the courts are reluctant to adjudicate in the area of executive lobbying. They seem inclined to defer to Congress and the executive branch on actions to be taken against improper lobbying by executive officials.[1079]

Selected Source Reading

Engstrom, Richard L. and Thomas G. Walker. "Statutory Restraints on Administration Lobbying — 'Legal Fiction'." Journal of Public Law, vol. 19 (1970), pp. 89-103.

Fisher, Louis. The Politics of Shared Power: Congress and the Executive, 4th ed. College Station, TX: Texas A&M University Press, 1998.

Nelsen, Ancher. "Lobbying by the Administration." In Mary McInnis, ed., We Propose: A Modern Congress, pp. 143-159. New York: McGraw-Hill, 1966.

U.S. General Accounting Office. Principles of Federal Appropriations Law, 2nd ed., vol. I, pp. 4-156 to 4-191. Washington: GAO, 1991.

Louis Fisher

[1078] Memorandum for Dick Thornburgh, Attorney General, from William P. Barr, Assistant Attorney General, Office of Legal Counsel, "Constraints Imposed by 18 U.S.C. § 1913, on Lobbying Efforts," Sept. 28, 1989; 13 Op. Off. Legal Counsel 362 (prelim. print).

[1079] Grassley v. Legal Service Corporation, 535 F.Supp. 818 (D.D.C. 1982); National Treasury Employees Union v. Campbell, 654 F.2d 784 (D.C.C. 1980); American Trucking Etc. v. Department of Transportation, 492 F.Supp. 566 (D.D.C. 1980); American Public Gas Association v. Federal Energy Administration, 408 F.Supp. 640 (D.D.C. 1976); National Association for Community Development v. Hodgson, 356 F.Supp. 1399 (D.D.C. 1973).

E. Federal Tort Claims Act

Statutory Intent and History

Until the Federal Tort Claims Act (FTCA) was enacted in 1946,[1080] a person who suffered personal injury or property damage as the result of a federal employee's negligence or misconduct had no judicial remedy. Such a person's only remedy was to seek to have a private claim bill introduced in Congress. This situation existed because of the common law doctrine of sovereign immunity, under which the United States may not be sued without its consent. Congress alone has the power to give this consent, and, by enacting the FTCA, Congress waived sovereign immunity for some tort suits. With exceptions, it made the United States liable for the torts of its employees committed in the scope of employment, just as private employers are liable for the torts of their employees committed in the scope of employment

The FTCA makes the United States liable for the torts of its employees (but not of government contractors) in accordance with the law of the state where the employee's act or omission occurred. Thus, for example, state laws placing caps on non-economic damages apply in cases brought under the FTCA. However, the FTCA contains exceptions under which the United States may not be held liable even though a private employer could be held liable under state law. And punitive damages are not permitted under the FTCA, regardless of state law.

One of these exceptions is known as the intentional tort exception; it prohibits suits "arising out of assault, battery, false imprisonment, false arrest, malicious prosecution, abuse of process, libel, slander, misrepresentation, deceit, or interference with contract rights." In 1974, in response to controversial "no-knock raids" by federal narcotics agents, Congress amended the FTCA to allow suits against the United States for the first six torts on the list of intentional torts just quoted, if they are committed by an "investigative or law enforcement officer of the United States Government."

In 1950, in Feres v. United States (340 U.S. 135), the Supreme Court held that military personnel may not sue under the FTCA for injuries sustained incident to service. Federal civilian employees also may not sue under the FTCA for on-the-job injuries, because they are covered by the Federal Employees' Compensation Act.

In 1988, the FTCA was amended to make federal employees acting within the scope of their employment immune from suit under state tort law — even in cases in which the United States may not be sued either (28 U.S.C. § 2679(b)(1)).

[1080] 60 Stat. 842; 28 U.S.C. §§ 1346(b), 2671-2680.

The most recent amendments to the FTCA provide that no person convicted of a felony who is incarcerated may sue the United States "for mental or emotional injury suffered while in custody without a prior showing of physical injury" (P.L. 104-134, § 806 (1996)), and that suits may be brought under the FTCA to recover damages to property seized under a federal forfeiture statute if the claimant is not convicted and is entitled to return of the property (P.L. 106-185, § 3 (2000)).

Major Provisions

United States district courts "shall have exclusive jurisdiction of civil actions on claims against the United States...for injury or loss of property, or personal injury or death caused by the negligent or wrongful act or omission of any employee of the government while acting within the scope of his office or employment, under circumstances where the United States, if a private person, would be liable to the claimant in accordance with the law of the place where the act or omission occurred" (28 U.S.C. § 1346).

Prior to filing suit under the FTCA, a claimant must present his claim to the federal agency out of whose activities the claim arises (28 U.S.C. § 2675). This must be done within two years after the claim accrues (28 U.S.C. § 2401). If, within six months after receiving a claim, the agency mails a denial of the claim to the claimant, then the claimant has six months to file suit in federal district court (28 U.S.C. §§ 2401, 2675). No period of limitations applies to a plaintiff if the agency fails to act within six months after receiving his claim. Suits under the FTCA are tried without a jury (28 U.S.C. § 2402).

Attorneys may not charge more than 20% of a settlement agreed to by a federal agency, or more than 25% of the amount of a court judgment or a settlement agreed to by the Attorney General (28 U.S.C. § 2678). The United States shall not be liable under the FTCA, regardless of state law, "for interest prior to judgment or for punitive damages" (28 U.S.C. § 2673).

The United States may not be held liable under the FTCA solely because the statute or regulation under which a federal employee acted was invalid. The United States may not be held liable under the FTCA, even if a federal employee engaged in a negligent or wrongful act or omission in the scope of employment, if the act or omission involved a "discretionary function," which means essentially the exercise of a policy judgment. The United States may not be held liable under the FTCA for claims that arise in a foreign country. The United States also may not be held liable for claims arising out of, among other things, "the loss, miscarriage, or negligent transmission of letters or postal matter"; "the assessment or collection of any tax or customs duty"; "the fiscal operations of the Treasury or ... the regulation of the monetary system"; or "combatant activities of the military or naval forces, or the Coast Guard, during time of war." All the exceptions to the FTCA noted in this paragraph appear at 28 U.S.C. § 2680.

Discussion

One aspect of the FTCA that has been controversial is the application of the Feres doctrine — prohibiting military personnel from suing for injuries sustained incident to service — to medical malpractice cases. One reason for the Feres doctrine is to prevent civilian courts from second-guessing military decisions, and some have argued that this rationale does not apply in medical malpractice cases, as when a military doctor is negligent in delivering a servicewoman's baby. The Supreme Court held, however, in United States v. Johnson (481 U.S. 681 (1987)), that the Feres doctrine applies even to suits brought by military personnel for injuries caused by employees of civilian federal agencies; this suggests that the "secondguessing" rationale is not crucial. More significant may be the potential effects of suits by military personnel on military discipline, and the alternative compensation system available to military personnel. Nevertheless, four dissenting justices in United States v. Johnson favored overturning Feres altogether as not mandated by Congress in the FTCA.

As noted, the FTCA, since 1988, has made federal employees immune from suits under state law for torts committed within the scope of their employment. (They may be sued for violating the Constitution or for violating a federal statute that authorizes suit against an individual.) This immunity has been extended to various volunteers in federal programs; more than fifty statutes, including those establishing VISTA and the Peace Corps, provide that volunteers in programs the statutes establish shall be considered federal employees for purposes of the FTCA.

Selected Source Reading

CRS Report 95-717A. Federal Tort Claims Act: Current Legislative and Judicial Issues, by Henry Cohen.

CRS Report 97-579A. Making Private Entities and Individuals Immune from Tort Liability by Declaring Them Federal Employees, by Henry Cohen.

Davis, Kenneth Culp, and Richard J. Pierce Jr., III. Administrative Law Treatise, 3rd ed. Boston: Little, Brown and Co., 1994.

Harper, Fowler V., James Fleming Jr., and Oscar S. Gray. The Law of Torts, 2nd ed. Boston: Little, Brown and Co., 1986; 2003 Cum. Supp. No. 2.

Jayson, Lester S. Handling Federal Tort Claims: Administrative and Judicial Remedies. New York: Matthew Bender, 2000.

Henry Cohen

TITLE 5: APPENDIX

Federal Advisory Committee Act (5 U.S.C. Appx. §§ 1-16)

Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction: Establishment and Composition, RS21758 (August 23, 2006).

STEPHANIE SMITH, CONGRESSIONAL RESEARCH SERV., COMMISSION ON THE INTELLIGENCE CAPABILITIES OF THE UNITED STATES REGARDING WEAPONS OF MASS DESTRUCTION: ESTABLISHMENT AND COMPOSITION (2006), *available at* http://www.intelligencelaw.com/library/secondary/crs/pdf/RS21758_8-23-2006.pdf.

Order Code RS21758
Updated August 23, 2006

Stephanie Smith
Analyst in American National Government
Government and Finance Division

Summary

On February 6, 2004, President George W. Bush created the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction to advise and assist him in performing his presidential duties. This report analyzes the establishment and organizational requirements set forth in the presidential mandate, and its relationship to the Federal Advisory Committee Act (FACA). On March 31, 2005, the commission submitted its final report to the President, which contained 74 recommendations for reforming the U.S. intelligence community.

Introduction

The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction was established by Executive Order 13328 of February 6, 2004.[1081] Located within the Executive Office of the President for administrative and organizational purposes, the commission was largely

[1081] E.O. 13328, Federal Register, vol. 69, Feb. 11, 2004, pp. 6901-6903.

governed by the requirements of the Federal Advisory Committee Act, unless otherwise indicated.[1082]

FACA Requirements

FACA established the first requirements for the management and oversight of federal advisory committees to ensure impartial and relevant expertise. As required by FACA, the General Services Administration (GSA) administers and provides management guidelines for advisory committees. GSA also maintains an online database to make available detailed reports covering each committee's activities during the calendar year.[1083]

Advisory committees can be designated as commissions, committees, councils, panels, or other similar groups. An advisory committee can be established by congressional legislation, by presidential executive order or directive, or by an agency head under general agency administrative authority. Excluded from the FACA definition is any commission composed entirely of full-time federal employees, or any committee established to perform primarily operational, as opposed to advisory, functions. In addition, Congress may choose to exempt an advisory committee from FACA's requirements.

FACA contains guidelines for membership in Section 5(b)(2), requiring that any advisory committee be "fairly balanced in terms of the points of view represented and the functions to be performed," and that the commission's recommendations not be inappropriately influenced by the appointing authority, or by any special interest.

Section 10(a) of FACA prescribes that each advisory committee meeting is presumptively open to the public, "except when the President determines otherwise for reasons of national security."[1084] FACA guidelines require that timely notice of each meeting open to the public be published in the Federal Register, and that detailed minutes of each meeting be taken. On May 13, 2004,

---

[1082] 5 U.S.C. Appendix — Federal Advisory Committee Act; 86 Stat. 770, as amended.

[1083] The FACA database can be found at [http://fido.gov/facadatabase].

[1084] Section 10(d) of FACA states that the President, or the head of the agency to which the advisory committee reports, may determine that a portion of a meeting be closed to the public, in accordance with 5 U.S.C. § 552(b), which identifies types of information that may be exempted from the rule of disclosure of the Freedom of Information Act. Any such determination should be written, and must state the reasons for closing the meeting. The advisory committee is also required to issue an annual report summarizing its activities, in accordance with 5 U.S.C. § 552(b).

it was announced in the Federal Register that the commission would meet in closed session on May 26 and May 27 in its offices in Arlington, VA.[1085]

Pursuant to FACA, each commission must file a charter containing its mandate and duties, frequency of meetings, membership, and the agency to which the commission reports. Section 12(a) requires each agencyto document fully the disposition of any funds that may be at the disposal of its advisory committees. With respect to advisory committees created by the President, financial records are to be maintained by GSA or by another agency designated in the authorizing presidential mandate. Each agency is also required to provide support services for each commission that it creates, or that reports to it, unless the establishing authority provides otherwise. Section 12(b) gives GSA the responsibility to provide appropriate support services for presidential advisory committees, unless the authorizing presidential mandate stipulates otherwise.

Commission Mandate

Oftentimes, one of the initial sections of a statute or executive order establishing a major advisory committee provides several statements identifying the conditions justifying the creation of a panel. Section 2(a) of E.O. 13328 stated that the commission was authorized to advise the President:

> *in the discharge of his constitutional authority under Article II of the Constitution to conduct foreign relations, protect national security, and command the Armed Forces of the United States, in order to ensure the most effective counterproliferation capabilities of the United States and response to the September 11, 2001, terrorist attacks and the ongoing threat of terrorist activity.*

Section 6(b) states that the commission is established to "solely advise and assist the President" in performing his duties. Subject to the authority of the President, the commission is authorized to be independent "from any executive department or agency, or of any officer, employee, or agent thereof."

A study commission's objectives and the scope of its activities are best stated in specific terms to guide the panel's members and staff in carrying out their responsibilities. Section 2(a) of E.O. 13328 states that the commission's primary mandate is to assess whether or not the U.S. intelligence community[1086] is adequately prepared to identify and respond to "the development and transfer of knowledge, expertise, technologies, materials, and resources" associated with the

---

[1085] Executive Office of the President, Office of Administration, "Meeting of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction," Federal Register,vol. 69, no. 93, May 13, 2004, p. 26602.

[1086] Sec. 6(h) of E.O. 13328 defines "intelligence community" the same as 50 U.S.C. § 401a(4).

threats and proliferation of weapons of mass destruction employed by foreign powers.[1087] So that the commission can better accomplish its mission, the presidential mandate prescribes the following duties in Section 2(b-d):

- examine and assess the U.S. intelligence community's body of knowledge and intelligence-gathering capabilities prior to the initiation of Operation Iraqi Freedom;
- compare this intelligence with the findings of the Iraq Survey Group, and other relevant agencies, concerning the capabilities, intentions, and activities of Iraq relating to the design and development, manufacture, acquisition, possession, proliferation, transfer, testing, potential or threatened use of weapons of mass destruction and related means of delivery;
- evaluate the challenges and difficulties of obtaining these categories of information associated with weapons of mass destruction;
- compare the U.S. intelligence community's intelligence-gathering capabilities pertaining to weapons of mass destruction and other related threats in Libya, prior to that nation's recent decision to open its programs to international scrutiny, with the current assessments of organizations examining these programs;
- compare the U.S. intelligence community's intelligence-gathering capabilities pertaining to weapons of mass destruction and other related threats in Afghanistan, prior to the removal of the Taliban government, with the current assessments of organizations examining these programs; and
- prepare a final report based on its findings by March 31, 2005, with specific recommendations.

Membership Requirements

The membership requirements of FACA are broad enough to allow a great deal of discretion in determining the composition of a commission. Therefore, the membership of an advisory committee will depend upon its legislative or presidential mandate. FACA does not provide guidance on the number of members a commission or committee should have or their terms of appointment. The membership generally should be large enough to allow for representation of differing points of view and to facilitate a quorum for commission meetings. Advisory committees of short-term existence usually keep the same members for the committee's duration, with any vacancies filled in the same manner as the original appointments were made. Some advisory panels may have staggered membership terms so that only one portion of the members will be new at any given time, thereby ensuring continuity in the committee's operations. It is also

[1087] Sec. 2(a) of E.O. 13328 defines "foreign powers" to include terrorists, terrorist organizations and private networks, or other entities or individuals.

possible for enabling legislation or a presidential mandate to specify how officers of an advisory panel are to be selected.

Section 3 of E.O. 13328 specifies that the commission was to be composed of no more than nine members, to be appointed by the President. Members were required to be
U.S. citizens, and the President designated two co-chairpersons from the membership. Two-thirds of the commission members constituted a quorum. On February 6, 2004, President George W. Bush announced the appointment of seven members to the commission, including his appointment of two co-chairpersons. Two additional members were appointed on February 12, 2004. The membership was as follows:

- former Senator Charles S. Robb (co-chairperson);
- Laurence H. Silverman, retired judge (co-chairperson);
- Senator John McCain;
- Lloyd M. Cutler, former White House counsel;
- Patricia M. Wald, former federal judge;
- Richard C. Levin, President of Yale University;
- Retired Admiral William O. Studeman, former Deputy Director of Central Intelligence;
- Charles M. Vest, President of the Massachusetts Institute of Technology; and
- Henry S. Rowen, senior fellow at the Hoover Institution.

Member Compensation and Travel Expenses

Advisory panel members who are not federal employees may or may not receive compensation for their work on a commission. Section 6(f) of E.O. 13328 specifies that members of the commission shall serve without compensation for their work. Section 6(f) also authorizes travel expenses and per diem for commission members who are not officers or employees in the executive branch, as authorized by statute.[1088]

Financial Disclosure Requirements

FACA guidelines do not contain financial disclosure requirements for members of an advisory committee. It appears from "federal law and regulation that one appointed to be a member of a federal advisory committee is required to file a financial disclosure form by virtue of his or her being either a regular federal employee or a 'special government employee,' as opposed to requiring a financial disclosure merely by virtue of his or her membership on an advisory

[1088] 5 U.S.C. § 5701-5707.

committee."[1089] Since the "fact of compensation is one of the determinate factors of whether one is or is not a federal employee," an advisory committee member serving without compensation may not be required to file a financial disclosure form. If, however, "a person is appointed on an advisory committee, and is considered a 'special government employee,' then such person must file either a public or a confidential statement, depending on his or her compensation level and the amount of days in which he or she performs the duties of that position."[1090] Even though the members of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction are serving without compensation, the White House announced on February 15, 2004, that they will file financial disclosure statements. The commission members' statements will, however, remain confidential.[1091]

Commission Staffing and Administrative Support

Section 6(g) of E.O. 13328 specifies that the commission shall have an executive director and staff. The co-chairpersons are authorized to hire and employ staff, or obtain, by assignment or detail, federal agency personnel to head and staff the commission.

The co-chairpersons are authorized by Section 4 to convene and preside at commission meetings, determine the commission's agenda, and assign work responsibilities, after consultation with other commission members. Administrative support is specified in Section 6(e) to be provided by the director of the Office of Administration within the Executive Office of the President.

Commission Funding

Commissions may be directly funded by Congress, or provided with monies indirectlythrough general agency appropriations. Although it happens rarely, an advisory committee may also receive funds from private sources. In the case of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, Section 6(e) authorizes funding to be provided by the director of the Executive Office of the President's Office of Administration, with the assistance of the director of the Office of Management and Budget, consistent with applicable law.

Commission Reports

An advisory commission may be required to prepare an interim, or a final, report for transmittal to the President, to Congress, or other department heads. These

---

[1089] CRS Congressional Distribution Memorandum, Advisory Committee Members and Financial Disclosure, by Jack Maskell, Oct. 12, 1999, p. 1.

[1090] Ibid., p. 3.

[1091] Eric Lichtblau, "Panel's Finance's Will Stay Private," New York Times, Feb. 15, 2004, p. 1.

reporting requirements usually can be found under the "duties" or "functions" sections of a panel's statutory or presidential mandate, or in a special section that mandates the production of a final report.[1092] The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction is required in Section 2(d) to make a final report to the President by March 31, 2005, based on its examination of the issues prescribed in Section 2(a-c). The commission's report is authorized to include specific recommendations for ensuring that the U.S. intelligence community is sufficiently organized, equipped, trained, and funded to respond to the proliferation of weapons of mass destruction and other related terrorist threats. On March 31, 2005, the commission transmitted its final report to the President, which included 74 recommendations for improving the U.S. intelligence community. The report also provided a comprehensive review pertaining to its findings on weapons of mass destruction.

Since the recommendations contained in a final report are only advisory, no changes in public policy occur on the authority of a commission. Therefore, the implementation of these recommendations is left to determination by a specific statute, or presidential or agency directive, where appropriate. To ensure greater accountability for, and oversight of, a commission's final report, it is often recommended that the statutory or presidential mandate include specific provisions to require follow-up or implementation of a commission's final report. Section 2(d) of E.O. 13328 authorizes the CIA, as well as the other agencies and departments within the U.S. intelligence community, to utilize the work of the commission and its final report. Within 90 days of receiving the final report, the President is required to consult with Congress on the recommendations of the commission, and propose "any appropriate legislative recommendations" based on the commission's findings.

Commission Termination

Unless statutorily mandated or otherwise extended by the President or agency head, an advisory committee will automatically terminate two years after its establishment. Consequently, most commissions must be rechartered with GSA every two years. The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction was required in Section 8 to terminate within 60 days after submitting its final report on March 31, 2005.

[1092] U.S. Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, Report to the President of the United States, Mar. 31, 2005 (Washington: 2005), at [http://www.whitehouse.gov], visited on Mar. 31, 2005.

Inspectors General Act of 1978 (5 U.S.C. Appx. §§ 1-13)

Statutory Offices of Inspector General: Past and Present, 98-379 (September 25, 2008).

FREDERICK M. KAISER, CONGRESSIONAL RESEARCH SERV., STATUTORY OFFICES OF INSPECTOR GENERAL: PAST AND PRESENT (2008), *available at* http://www.intelligencelaw.com/library/secondary/crs/pdf/98-379_9-25-2008.pdf.

Frederick M. Kaiser
Specialist in American National Government
Government and Finance Division

Summary

Statutory offices of inspector general (OIG) consolidate responsibility for audits and investigations within a federal agency. Established by public law as permanent, nonpartisan, independent offices, they now exist in more than 60 establishments and entities, including all departments and largest agencies, along with numerous boards and commissions. Under two major enactments — the Inspector General Act of 1978 and its amendments of 1988 — inspectors general are granted substantial independence and powers to carry out their mandate to combat waste, fraud, and abuse.[1093] Recent initiatives have added offices in the Architect of the Capitol Office (AOC), Government Accountability Office (GAO), and for Afghanistan Reconstruction; funding and assignments for specific operations; and mechanisms to oversee the Gulf Recovery Program. Other proposals in the 110th Congress are designed to strengthen the IGs'

[1093] 5 U.S.C. Appendix covers all but nine of the statutory OIGs. See CRS Report RL34176, Statutory Inspectors General: Legislative Developments and Legal Issues, by Vanessa K. Burrows and Frederick M. Kaiser; U.S. President's Council on Integrity and Efficiency, A Strategic Framework, 2005-2010 [http://www.ignet.gov]; Frederick Kaiser, "The Watchers' Watchdog: The CIA Inspector General," International Journal of Intelligence (1989); Paul Light, Monitoring Government: Inspectors General and the Search for Accountability (1993); U.S. Government Accountability Office, Inspectors General: Office Consolidation and Related Issues, GAO-02-575, Highlights of the Comptroller General's Panel on Federal Oversight and the Inspectors General, GAO-06-931SP, and Inspectors General: Opportunities to Enhance Independence and Accountability, GAO-07-1089T; U.S. House Subcommittee on Government Management and Organization, Inspectors General: Independence and Accountability, hearing (2007); U.S. Senate Committee on Homeland Security and Governmental Affairs, Strengthening the Unique Role of the Nation's Inspectors General, hearing (2007); Project on Government Oversight, Inspectors General: Many Lack Essential Tools for Independence (2008).

independence, add to their reports, and create new posts in the Intelligence Community.

Responsibilities

The IGs' four principal responsibilities are (1) conducting and supervising audits and investigations relating to the programs and operations of the agency; (2) providing leadership and coordination and recommending policies to promote the economy, efficiency, and effectiveness of these; (3) preventing and detecting waste, fraud, and abuse in these; and (4) keeping the agency head and Congress fully and currently informed about problems, deficiencies, and recommended corrective action.

Authority and Duties

To carry out these purposes, IGs have been granted broad authority to: conduct audits and investigations; access directly all records and information of the agency; request assistance from other federal, state, and local government agencies; subpoena information and documents; administer oaths when taking testimony; hire staff and manage their own resources; and receive and respond to complaints from agency employees, whose confidentiality is to be protected. In addition, the Homeland Security Act of 2002 gave law enforcement powers to criminal investigators in offices headed by presidential appointees. IGs, moreover, implement the cash incentive award program in their agencies for employee disclosures of waste, fraud, and abuse (5 U.S.C. 4511).

Reporting Requirements

IGs have reporting obligations regarding their findings, conclusions, and recommendations. These include reporting: (1) suspected violations of federal criminal law directly and expeditiously to the Attorney General; (2) semiannually to the agency head, who must submit the IG report (along with his or her comments) to Congress within 30 days; and (3) "particularly serious or flagrant problems" immediately to the agency head, who must submit the IG report (with comments) to Congress within seven days. The Central Intelligence Agency (CIA) IG must also report to the Intelligence Committees if the Director or Acting Director is the focus of an investigation or audit. By means of these reports and "otherwise" (e.g., testimony at hearings), IGs are to keep the agency head and Congress fully and currently informed.

Independence and Neutrality

In addition to having their own powers (e.g., to hire staff and issue subpoenas), IG independence is reinforced through protection of their budgets (in the larger establishments), qualifications for their appointment, prohibitions on interference with their activities and operations (with a few exceptions), and fixing the priorities and projects for their offices without outside direction. An exception to the IGs' rule occurs when a review is ordered in statute, although inspectors general, at their own discretion, may conduct reviews requested by the President, agency heads, other IGs, or congressional offices.

Other provisions are designed to protect the IGs' independence and ensure their neutrality. For instance, IGs are specifically prohibited from taking corrective action themselves. Along with this, the Inspector General Act prohibits the transfer of "program operating responsibilities" to an IG. The rationale for both is that it would be difficult, if not impossible, for IGs to audit or investigate programs and operations impartially and objectively if they were directly involved in making changes in them or carrying them out.

Supervision

IGs serve under the "general supervision" of the agency head, reporting exclusively to the head or to the officer next in rank if such authority is delegated. With but a few specified exceptions, neither the agency head nor the officer next in line "shall prevent or prohibit the Inspector General from initiating, carrying out, or completing any audit or investigation, or from issuing any subpoena...." Under the IG Act, the heads of only six agencies — the Departments of Defense, Homeland Security, Justice, and the Treasury, plus the U.S. Postal Service (USPS) and Federal Reserve Board — may prevent the IG from initiating, carrying out, or completing an audit or investigation, or issuing a subpoena, and then only for specified reasons: to protect national security interests or ongoing criminal investigations, among others. When exercising this power, the head must explain such action within 30 days to the House Government Oversight and Reform Committee, the Senate Homeland Security and Governmental Affairs Committee, and other appropriate panels. The CIA IG Act similarly allows the director to prohibit or halt an investigation or audit; but he or she must notify the House and Senate intelligence panels of the reasons, within seven days.

Appropriations

Presidentially appointed IGs in the establishments — but not in designated federal entities (DFEs) — are granted a separate appropriations account (a separate budget account in the case of the CIA) for their offices. This restricts agency administrators from transferring or reducing IG funding once it has been specified in law.

Appointment, Removal, and Tenure

Under the Inspector General Act, IGs in the larger establishments are appointed by the President, subject to Senate confirmation, and are to be selected without regard to political affiliation and solely on the basis of integrity and demonstrated ability in relevant fields. Two other IGs appointed by the President operate under similar but distinct requirements. The CIA IG is to be selected under these criteria as well as experience in the field of foreign intelligence. And the Special Inspector General for Afghanistan Reconstruction (SIGAR) is the only IG appointed by the President alone. Presidentially nominated and Senate-confirmed IGs can be removed only by the President; when so doing, he must notify Congress of the reasons.

By comparison, IGs in the DFEs are appointed by and can be removed by the agency head, who must notify Congress in writing when exercising this power. The USPS IG is the only IG with removal "for cause" and then with the written concurrence of at least seven of the nine governors, who also appoint the officer. Terms of office are set for three IGs, but with the possibility of reappointment: in the Postal Service (seven years), AOC (five years), and U.S. Capitol Police (five years), with selection by the Capitol Police Board. Indirectly, the Peace Corps IG faces an effective term limit, because all positions there are restricted to five to 8½ years. With regard to Special Inspector General for Iraq Reconstruction (SIGIR) and SIGAR, each post is to end 180 days after its parent entity's reconstruction funds are less than $250 million.

Coordination and Controls

Several presidential orders govern coordination among the IGs and investigating charges of wrongdoing by high-echelon officers. Two councils, governed by E.O. 12805, issued in 1992, are the President's Council on Integrity and Efficiency (PCIE) and a parallel Executive Council on Integrity and Efficiency (ECIE). Chaired by the Deputy Director of the Office of Management and Budget (OMB), each is composed of the appropriate IGs plus officials from other agencies, such as the Federal Bureau of Investigation (FBI) and Special Counsel. Investigations of alleged wrongdoing by IGs or other top OIG officials (under the IG act) are governed by a special Integrity Committee, composed of PCIE and ECIE members and chaired by the FBI representative (E.O. 12993), with investigations referred to an appropriate executive agency or to an IG unit. Other coordinative devices have been created administratively.

Establishment

Statutory offices of inspector general have been authorized in 67 current federal establishments and entities, including all 15 cabinet departments; major executive branch agencies; independent regulatory commissions; various government corporations and boards; and five legislative branch agencies. All but nine of the OIGs[1094] are directly and explicitly under the 1978 Inspector General Act. Each office is headed by an inspector general, who is appointed in one of three ways:

(1) 30 are nominated by the President and confirmed by the Senate in "establishments," including all departments and the larger agencies under the IG act, plus the CIA (Table 1).
(2) 36 are appointed by the head of the entity in 29 "designated federal entities" — usually smaller boards and commissions — and in seven other units, where the IGs operate under separate authority: SIGIR, ONDI, and five legislative agencies (Table 2).

[1094] AOC, Capitol Police, CIA, GAO, Government Printing Office (GPO), Library of Congress (LOC), Office of the Director of National Intelligence (ODNI), SIGAR, and SIGIR.

(3) One (in SIGAR) is appointed by the President alone (Sec. 1229, P.L. 110-181).

Table 1. Statutes Authorizing IGs Nominated by the President and Confirmed by the Senate, 1976-Present

(current offices in **bold**)[1095]

- 1976 P.L. 94-505
  - **Health, Education, and Welfare (now Health and Human Services)**
- 1977 P.L. 95-91
  - **Energy**
- 1978 P.L. 95-452
  - **Agriculture,**
  - **Commerce**,
  - Community Services Administration (CSA),[1096]
  - **Housing and Urban Development,**
  - **Interior,**
  - **Labor,**
  - **Transportation,**
  - **Environmental Protection Agency,**
  - **General Services Administration,**
  - **National Aeronautics and Space Administration,**
  - **Small Business Administration,**
  - **Veterans Administration (now the Veterans Affairs Department)**
- 1979 P.L. 96-88
  - **Education**
- 1980 P.L. 96-294
  - U.S. Synthetic Fuels Corporation[1097]
- 1980 P.L. 96-465
  - **State**[1098]
- 1981 P.L. 97-113

[1095] All except the CIA IG are directly under the 1978 Inspector General Act, as amended.

[1096] CSA, Synfuels Corporation, USIA, ACDA, RTC, CDFIF, and FEMA have been abolished or transferred.

[1097] CSA, Synfuels Corporation, USIA, ACDA, RTC, CDFIF, and FEMA have been abolished or transferred.

[1098] The State Department IG had also served as the IG for ACDA. In 1998, P.L. 105-277 transferred the functions of ACDA and USIA to the State Department and placed the Broadcasting Board of Governors and the International Broadcasting Bureau under the jurisdiction of the State IG.

- **Agency for International Development**[1099]

- 1982 P.L. 97-252
  - **Defense**
- 1983 P.L. 98-76
  - **Railroad Retirement Board**
- 1986 P.L. 99-399
  - U.S. Information Agency (USIA)[1100]
- 1987 P.L. 100-213
  - Arms Control and Disarmament Agency (ACDA)[1101]
- 1988 P.L. 100-504
  - **Justice**,[1102]
  - **Treasury**,
  - Federal Emergency Management Agency (FEMA),[1103]
  - **Nuclear Regulatory Commission,**
  - **Office of Personnel Management**
- 1989 P.L. 101-73
  - Resolution Trust Corporation (RTC)[1104]
- 1989 P.L. 101-193
  - **Central Intelligence Agency**[1105]
- 1993 P.L. 103-82

[1099] The Inspector General in AID may also conduct reviews, investigations, and inspections of the Overseas Private Investment Corporation (22 U.S.C. 2199(e)).

[1100] CSA, Synfuels Corporation, USIA, ACDA, RTC, CDFIF, and FEMA have been abolished or transferred. The State Department IG had also served as the IG for ACDA. In 1998, P.L. 105-277 transferred the functions of ACDA and USIA to the State Department and placed the Broadcasting Board of Governors and the International Broadcasting Bureau under the jurisdiction of the State IG.

[1101] CSA, Synfuels Corporation, USIA, ACDA, RTC, CDFIF, and FEMA have been abolished or transferred. The State Department IG had also served as the IG for ACDA. In 1998, P.L. 105-277 transferred the functions of ACDA and USIA to the State Department and placed the Broadcasting Board of Governors and the International Broadcasting Bureau under the jurisdiction of the State IG.

[1102] In 2002, P.L. 107-273 expanded the jurisdiction of the Justice OIG to cover all department components.

[1103] CSA, Synfuels Corporation, USIA, ACDA, RTC, CDFIF, and FEMA have been abolished or transferred. P.L. 107-296, which established the Department of Homeland Security, transferred FEMA's functions to it and also granted law enforcement powers to OIG criminal investigators in establishments.

[1104] CSA, Synfuels Corporation, USIA, ACDA, RTC, CDFIF, and FEMA have been abolished or transferred.

[1105] All except the CIA IG are directly under the 1978 Inspector General Act, as amended.

- **Corporation for National and Community Service**
- 1993 P.L. 103-204
  - **Federal Deposit Insurance Corporation (FDIC)**
- 1994 P.L. 103-296
  - **Social Security Administration**
- 1994 P.L. 103-325
  - Community Development Financial Institutions Fund (CDFIF)[1106]
- 1998 P.L. 105-206
  - **Treasury Inspector General for Tax Administration**[1107]
- 2000 P.L. 106-422
  - **Tennessee Valley Authority (TVA)**[1108]
- 2002 P.L. 107-189
  - **Export-Import Bank**
- 2002 P.L. 107-296
  - **Homeland Security**[1109]

Recent Initiatives

Initiatives in response to the 2005 Gulf Coast Hurricanes arose to increase OIG capacity and capabilities in overseeing the unprecedented recovery program. These include IGs or deputies from affected agencies on a Homeland Security Roundtable, chaired by the DHS IG; membership on a Hurricane Katrina Contract Fraud Task Force, headed by the Justice Department; an office in the DHS OIG to oversee disaster assistance activities nationwide; and additional funding for the OIG in Homeland Security. In the 110th Congress, the IGs in DOD and in other relevant agencies have been charged with specific duties connected with combating waste, fraud, and abuse in wartime contracting (P.L. 110-181). A new IG has been instituted in the AOC, in the GAO, and in the Afghanistan reconstruction effort, while other legislative action requires that full-agency websites link to the separate OIG "hotline" websites. Separate recommendations have arisen in the recent past, such as consolidating DFE OIGs

---

[1106] CSA, Synfuels Corporation, USIA, ACDA, RTC, CDFIF, and FEMA have been abolished or transferred.

[1107] The OIG for Tax Administration in Treasury is the only case where a separate IG, under the 1978 IG Act, exists within an establishment or entity that is otherwise covered by its own statutory IG.

[1108] P.L. 106-422, which re-designated TVA as an establishment, also created, in the Treasury Department, a Criminal Investigator Academy to train IG staff and an Inspector General Forensic Laboratory.

[1109] P.L. 107-296, which established the Department of Homeland Security, transferred FEMA's functions to it and also granted law enforcement powers to OIG criminal investigators in establishments.

under presidentially appointed IGs or under a related establishment office (GAO-02-575).

Pending proposals in the 110th Congress include the following: requiring IG annual reviews to report on program effectiveness and efficiency (H.R. 6639); and establishing IGs for the Judicial Branch (H.R. 785 and S. 461) and the Washington Metropolitan Area Transit Authority (H.R. 401). The Intelligence Authorization Act for FY2009 (H.R. 5959 and S. 2996) would create an inspector general for the entire Intelligence Community, a provision opposed by the Bush Administration; and would grant statutory recognition to specified OIGs in the Defense Department. Other bills — H.R. 928 and 2324, whose earlier versions incurred objections from OMB — have been reconciled and await chamber action. These proposals are designed to increase the IGs' independence and powers. Different versions have called for providing specifics on initial OIG budget estimates to Congress; removing an IG only for "cause"; setting a term of office for IGs; establishing a Council of Inspectors General for Integrity and Efficiency in statute; revising the pay structure for IGs; allowing for IG subpoena power in any medium; and granting law enforcement powers to qualified IGs in DFEs.

Ethics in Government Act of 1978 (5 U.S.C. Appx. §§ 101-505)

Entering the Executive Branch of Government: Potential Conflicts of Interest With Previous Employments and Affiliations, RL31822 (December 11, 2007).

JACK MASKELL, CONGRESSIONAL RESEARCH SERV., ENTERING THE EXECUTIVE BRANCH OF GOVERNMENT: POTENTIAL CONFLICTS OF INTEREST WITH PREVIOUS EMPLOYMENTS AND AFFILIATIONS (2007), *available at* http://www.intelligencelaw.com/library/secondary/crs/pdf/RL31822_12-11-2007.pdf.

Order Code RL31822
Updated December 11, 2007

Jack Maskell
Legislative Attorney
American Law Division

Summary

Ethics and conflict of interest concerns have been expressed about the impartiality, bias, or fairness of government regulators, administrators, and other executive branch decision makers who, shortly before entering government service, had represented, owned, or were employed by industries, firms, or other entities that they must now regulate and oversee. Federal conflict of interest law and regulation, for the most part, deal with the potential influence of existing and current financial assets, properties, arrangements, and relationships of the federal official. While the laws and regulations focus primarily on current economic and financial interests of a government official and those closely associated with the official, there are some limited conflict of interest regulations and ethics standards which look also to previous employment and past associations of those entering federal service.

The regulatory scheme regarding financial interests encompasses what has colloquially been called the "three-D" method of conflict of interest regulation, that is: disclosure, disqualification and divestiture. Public financial disclosure is required of in-coming federal officials who will be compensated above certain amounts, including those officials nominated by the President who must receive Senate confirmation. Disclosure information will cover not only existing assets, property, debts and income, but also certain information about past clients and employers who during the previous two years compensated the in-coming federal

official over $5,000 in a year, other past income sources, and certain past positions held in private organizations and entities in the preceding two years.

Disqualification or "recusal" is the principal statutory method of dealing with potential conflicts of interest of an executive branch officer or employee, whereby the officer or employee is prohibited from participating in any particular official governmental matter in which that official, or those close to the official whose financial interests may be "imputed" to the official, has any financial interest. While the statutory provision requiring disqualification is a criminal provision of law, and covers only current or existing financial interests of the officer or employee, there is also a "regulatory" recusal requirement that may apply to certain past affiliations and previous economic interests. Such recusals may be required in particular matters involving specific parties when organizations, entities, or clients with which the federal official had been associated during the previous one-year period are or represent parties in those matters. Additionally, executive branch regulations also provide for a two-year recusal requirement barring an official in the executive branch from participating in a particular matter in which a former employer is a party (or represents a party) when that former employer had made an "extraordinary payment" to the official prior to entering government. Aside from the specific regulatory and statutory restrictions and requirements on past associations and employments, there is no general regulation or standard on possible or perceived "philosophical" or "ideological" biases which a federal regulator or administrator may allegedly have on a subject because of the past affiliations or previous employments or professional activities of that official.

Introduction

This report examines the federal laws and regulations relevant to entering into federal government employment from the private sector, with respect particularly to the potential conflicts of interest that may arise because of the past employment, affiliations or financial interests or involvements of a nominee or new officer or employee in the executive branch of government. The report is intended to provide those conducting congressional oversight with an outline of some of the issues, rules, regulations, and oversight tools that may be available regarding this subject.

Background/Issues

There has been expressed ongoing concerns about the impartiality, bias, or fairness of government regulators, administrators and other executive branch decision makers who, shortly before entering government service, had represented, owned or were employed by industries, firms or other entities which they must now regulate and oversee, or concerning whom such officials must otherwise make or advise the government on policies directly and significantly impacting those former clients, employers or firms. Several instances of alleged conflicts of interest, "appearances" of conflicts of interest or bias, or "cozy relationships" between the regulated entities and the government official who

had formerly worked for or represented that regulated entity, have been examined in the press over the last few years.[1110] The allegations and concerns in such instances are that loyalty to private economic and business interests, rather than fealty to the general public interest, is being served by such officials in their actions.

Individuals entering federal service will, of course, bring with them existing financial investments, ownerships, properties, and other economic arrangements typical of anyone similarly placed in American society. Those entering federal service immediately from private industry will also enter with certain former affiliations, employment or other financial, economic or business associations with particular private interests. While federal conflict of interest law and regulation focuses primarily on current economic and financial interests of a government official and those closely associated with the official, there are some limited conflict of interest regulations and ethics standards which look also to previous employment and past associations of those becoming federal officers and employees.

Conflicts of Interest Generally

The term "conflict of interest" may have a broad meaning in general usage. However, under federal law and regulation a "conflict of interest," for the most part, deals with a conflict between a federal employee's official, governmental duties and responsibilities on the one hand, and the personal, financial or economic interests of the employee on the other.[1111] When the official duties of a government employee may impact upon the outside, private business or economic interests of that employee, or the economic interests of those closely associated with the employee, a conflict of interest situation presents itself.

[1110] Washington Post, "Official's Lobbying Ties Decried: Interior's Griles Defends Meetings as Social, Informational," September 25, 2002, p. A1: "Within weeks of taking office, Griles began a series of meetings with former clients and administration officials on regulatory matters important to several of his former clients"; Washington Post, "Pitt's Role in AOL Time Warner Case Uncertain," October 18, 2002, p. E1: "Pitt, who has been criticized for participating in SEC cases involving former law clients, represented [AOL's chairman] and the company on several significant accounting matters in recent years"; Washington Post, "Pentagon Official From Enron in Hot Seat," January 27, 2002, p. A8: "[White's] corporate experience - his role at ... Enron Energy Services (EES) - is raising questions of possible conflicts of interest... In his first major speech as secretary, he vowed to step up privatization of utility services at military bases. EES ... had been seeking to contract with the military."

[1111] Manning, Federal Conflict of Interest Law, at 2-3 (1964); Association of the Bar of the City of New York, Conflict of Interest and Federal Service, at 3 (1960); House Committee on Standards of Official Conduct, House Ethics Manual, 102d Cong., 2d Sess. at 87 (April 1992); see Regulations of the Office of Government Ethics, 5 C.F.R. part 2635. There may be certain so-called "conflict of interest" statutes or regulations which do not expressly deal with financial interests or compensated activities, such as, for example, 18 U.S.C. § 205, which prohibits a federal employee from acting as an agent or attorney for a private party before a federal agency, even if the activity is uncompensated.

The overall scheme of the conflict of interest laws adopted by Congress generally embodies the principle "that a public servant owes undivided loyalty to the Government,"[1112] and that advice and recommendations given to the government by its employees and officials be made in the public interest and not be tainted, even unintentionally, with influence from private or personal financial interests.[1113] The House Judiciary Committee, reporting out major conflict of interest revisions made to federal law in the 1960's found:

The proper operation of a democratic government requires that officials be independent and impartial; that Government decisions and policy be made in the proper channels of the governmental structure; ... and that the public have confidence in the integrity of its government. The attainment of one or more of these ends is impaired whenever there exists, or appears to exist an actual or potential conflict between the private interests of a Government employee and his duties as an official.[1114]

The concern in such regulation "is not only the possibility or appearance of private gain from public office, but the risk that official decisions, whether consciously or otherwise, will be motivated by something other than the public's interest. The ultimate concern is bad government..."[1115] The conflict of interest laws are thus directed not only at conduct which is improper, but rather are often preventative in nature, directed at situations which merely have the potential to tempt or subtly influence an official in the performance of official public duties. As explained by the Supreme Court with regard to a predecessor conflict of interest law requiring disqualification of officials from matters in which they have a personal financial interest:

This broad proscription embodies a recognition of the fact that an impairment of impartial judgment can occur in even the most well-meaning men when their personal economic interests are affected by the business they transact on behalf of the Government.[1116]

[1112] H.Rept. 87-748, 87th Congress, 1st Session, at 3 (1961). House Judiciary Committee report on the comprehensive amendments and revisions to conflict of interest laws in 1962.

[1113] H.Rept. 87-748, supra at 4-6; see also United States v. Mississippi Valley Generating Co., 364 U.S. 520, 549 (1960); and Conflict of Interest and Federal Service, supra at 3-4.

[1114] H.Rept. 87-748, supra at 5-6.

[1115] The Association of the Bar of the City of New York, Special Committee on Congressional Ethics, James C. Kirby, Executive Director, Congress and the Public Trust, 38-39 (1970).

[1116] United States v. Mississippi Valley Generating Co., supra at 549, concerning 18 U.S.C. § 434 (1960 Code ed.), predecessor statute to current 18 U.S.C. § 208.

Conflict of Interest Regulation

The application of federal conflict of interest laws and regulations, particularly the laws requiring an official's recusal or disqualification from certain matters, or regulations or procedures requiring the divestiture of certain assets, have traditionally been directed at current and existing financial interests and ties of that official, and those closely associated with the official. The regulatory scheme regarding financial interests encompasses what has colloquially been called the "three-D" method of conflict of interest regulation, that is: disclosure, disqualification and divestiture.

Financial Disclosure: Identifying and Deterring Potentially Conflicting Financial Interests

Upon entering the Federal Government, and then annually on May 15 thereafter, high-level government officials must file detailed, public financial disclosure statements. Public financial disclosures were first required by law with the passage of the Ethics in Government Act of 1978 (P.L. 95-521, as amended), and were intended to serve the purpose of identifying "potential conflicts of interest or situations that might present the appearance of a conflict of interest" for government officials in policy making positions.[1117]

In addition to the purpose of merely identifying potential conflicts, and then attempting to resolve such conflicts of interest, the committees considering the ethics legislation adopted in 1978 recognized the fact that there was potentially a "deterrent factor" in requiring public disclosure of a government official's personal and family financial information, — both in deterring the holding of certain assets (and thus deterring certain potential conflicts of interest), but also possibly in deterring the recruitment of certain persons into the government because of such persons' uneasiness with the required details of public financial disclosure. As noted by the Senate Committee, however, this latter deterrent effect was not necessarily a negative consequence of required public disclosures, but could be a positive consideration in the enactment of the financial disclosure requirement:

Public financial disclosure will deter some persons who should not be entering public service from doing so. Individuals whose personal finances would not bear up to public scrutiny ... will very likely be discouraged from entering public office altogether, knowing in advance that their sources of income and financial holdings will be available for public review.[1118]

[1117] S.Rept. 95-170, 95th Cong., 1st Sess. 117 (1977). The fact that the disclosures were to be made public was also seen as serving the purpose of increasing public confidence in the integrity of the institutions of government and in those who serve them.

[1118] S.Rept. 95-170, supra at 22.

Who Must File, Generally

Anyone entering the federal service who is covered by the public financial disclosure laws generally must, within 30 days of appointment, file an entry report.[1119] Thereafter, covered employees must file annual reports by May 15. Whether an employee of the Federal Government is required to file public financial disclosure statements is determined, in the first instance, by the rate of compensation that the employee receives or will receive from the Federal Government, and then, secondly, by the number of days such an employee works for the Federal Government. Any officer or employee of the executive branch of government who "occupies a position classified above GS-15," or, if "not under the General Schedule," is in a position compensated at a "rate of basic pay ... equal to or greater than 120 percent of the minimum rate of basic pay payable for GS-15," is generally subject to the public disclosure provisions.[1120] Those employees compensated at the rate of pay described above will be required to file public disclosure statements if the individual works for the government for more than 60 days in the calendar year.[1121]

This requirement for detailed, public financial disclosure under the Ethics in Government Act of 1978 currently applies to more than 20,000 officials in the Federal Government.[1122] In addition to the statutory mandate for public disclosure based on salary level, the Office of Government Ethics requires by regulation that all "Schedule C" employees, regardless of salary, file public disclosures.[1123]

[1119] 5 U.S.C. app. §§ 101(a), 102(b).

[1120] 5 U.S.C., app. § 101(f)(3). As of this writing in 2003, for example, the threshold rate of pay for 2003 will be $102,168 annually. The definition for legislative employees, it should be noted, differs slightly and covers anyone who is compensated at a rate in excess of 120% of a the base salary of a GS-15, regardless of whether or not that person is on the General Schedule or not, thus covering certain GS-15's in the legislative branch not covered in the executive branch.

[1121] 5 U.S.C., app. § 101(d). Certain exemptions and waivers may be permitted upon particular findings and determinations regarding special Government employees. See 5 U.S.C., app. § 101(i).

[1122] Statement of Amy L. Comstock, Director of the Office of Government Ethics, before the Senate Committee on Governmental Affairs, "OGE Recommendations on Streamlining Public Financial Disclosure and Other Aspects of the Presidential Appointment Process," April 5, 2001, p. 2.

[1123] 5 C.F.R. § 2634.202(e). Exceptions may be provided under some circumstances. There are also confidential reporting requirements which apply generally to certain lower-level "rank and file" employees, that is, those compensated below the threshold rate of pay for public disclosures (GS-15 or below, or less than 120% of the basic rate of pay for a GS-15), and who are determined by the employee's agency to exercise responsibilities regarding government contracting or procurement, government grants, government subsidies or licensing, government auditing, or other governmental duties which may particularly require the employee to avoid financial conflicts of interest. 5 C.F.R. §§ 2634.901-908.

Where Filed

For most incoming federal officials filing their entry report, as well as for current employees filing their annual financial disclosure statements by May 15 of each year, such reports are generally to be filed with the designated agency ethics officer (most commonly in the office of general counsel) in the agency in which the reporting officer or employee serves or is to serve.[1124] The President and the Vice President, however, file their reports with the Director of the Office of Government Ethics. All filed reports by officials are open generally for public inspection upon request made in writing, subject to rules on the impermissible commercial or political use of the information contained in the reports.[1125] The agencies having such reports are instructed to keep them as public records for six years.[1126]

Advice and Consent Positions

All presidential nominees requiring Senate confirmation must file public disclosure statements regardless of salary (but uniformed and foreign service nominees file only if they meet the pay threshold),[1127] and such reports incur other specific procedural steps. Their disclosure statements are not only filed with and reviewed by their department or agency, but are also "transmitted" to the Office of Government Ethics for review, and are "foward[ed]" for review to the Committee of the Senate with jurisdiction over the particular individual's nomination.

Once the President has transmitted to the Senate the nomination of a person required to be confirmed by the Senate, the nominee must within five days of the President's transmittal (or any time after the public announcement of the nomination, but no later than five days after transmittal), file a financial disclosure statement.[1128] This financial disclosure statement is filed with the designated agency ethics officer of the agency in which nominee will serve,[1129] and copies of the report are transmitted by the agency to the Director of the

---

[1124] 5 U.S.C. app. § 103(a).

[1125] 5 U.S.C.,app. § 105(a), (b).

[1126] 5 U.S.C. app. § 105(d).

[1127] 5 U.S.C. app. § 101(b).

[1128] 5 U.S.C. app. § 101(b); 5 C.F.R § 2634(c)(1). The disclosure report form is provided to the nominee by the Executive Office of the President. 5 C.F.R. § 2634.605(c)(1).

[1129] 5 C.F.R. §2634.602(a).

Office of Government Ethics.[1130] The Director of OGE then forwards a copy to the Senate committee which is considering the nomination of that individual.[1131] A presidential nominee must file an updated report to the Committee reviewing his nomination at or before the commencement of hearings, updating the information through the period "not more than five days prior to the commencement of the hearing," concerning specifically information related to honoraria and outside earned income.[1132]

Information to Be Reported: Current Financial Interests

Most of the information to be filed and publicly disclosed concerns current and existing financial information on assets, property, debts, income and existing associations which may present or potentially involve a conflict of interest with the officer's or employee's official responsibilities for the government. The regular annual financial disclosure reports to be filed in May of each year generally require information concerning eight different categories of financial information. The disclosure statement[1133] requires public listing of the identity and/or the value (generally in "categories of value") of such items as: (1) the official's private income of $200 or more (including earned and unearned income such as dividends, rents, interest and capital gains) and the source of income; (2) gifts received over a certain amount (including reimbursements for travel over threshold amounts); (3) the identification of assets and income-producing property (such as stocks, bonds, other securities, rental property, etc.) of over $1,000 in value (including savings accounts over $5,000); (4) liabilities owed to creditors exceeding $10,000 (but not including one's home mortgage or car loans); (5) financial transactions, including purchases, sales or exchanges exceeding $1,000 in value, of income-producing property, stocks, bonds, or other securities; (6) positions held in outside businesses and organizations; (7) agreements for future employment or leaves of absence with private entities, continuing payments from or participation in benefit plans of former employers; and (8) the cash value of the interests in a qualifying blind trust.[1134]

The incoming reports, including the reports of incoming presidential appointees requiring Senate confirmation, include most of the information required in the annual reports under § 102(a) of the Ethics Act, but does not include the

---

[1130] 5 U.S.C. app. § 103(c), 5 C.F.R. § 2634.602(c)(1)(vi),.

[1131] 5 U.S.C. app. § 103(c), 5 C.F.R. § 2634.602(c)(3).

[1132] 5 U.S.C. app. § 101(b). 5 C.F.R. § 2634.606(a).

[1133] In the executive branch, disclosure form SF 278.

[1134] 5 U.S.C. app. § 102(a)(1) - (8). For items to be disclosed in relation to the official's spouse and dependent children, see 5 U.S.C. app. § 102(e)(1)(A) - (F).

information on gifts and travel reimbursements (§ 102(a)(2)), nor does it need to include the information on financial transactions during the previous year (§ 102(a)(5) or the cash value of trusts (§ 102(a)(8)).[1135] The new entrant reports specifically require disclosure of private income received for the filing year and the preceding calendar year; ownership interests in assets and income producing property over $1,000 in value, and liabilities of over $10,000 owed, as of the date specified in the report, but which must be no more than 31 days before the filing date; the identity of positions held in private entities; and any future agreements for employment, leave of absence, continuing payments from or participation in benefit plans of former employers.[1136]

Information to Be Reported: Past Associations, Clients

While most of the financial disclosure requirements are directed at current and existing financial holdings and interests, there are certain provisions which look to past affiliations and interests. Perhaps most significantly for first-time filers, including nominees to Senate-confirmed positions, the public disclosure law requires non-elected reporting individuals to list in public reports the identity of persons, including clients, from whom the reporting official had received more than $5,000 in compensation in any of the two calendar years prior to the year in which the reporting official files his or her first disclosure report.[1137] Such listing of clients and others who paid the reporting individual compensation above the statutory threshold, should also include a statement of "the nature of the duties performed or services rendered" for such client or employer. Furthermore, new entrant reports, including reports of nominees, are to contain the required information concerning all private income received for the filing year, and additionally for the preceding calendar year; and the identity of positions held in private entities must be disclosed not only for positions held during the current calendar year, but also during the two preceding years.[1138]

Executive Branch Review and Ethics Agreements

The ethics officials to whom the annual disclosure reports are made are instructed to review the reports within 60 days to determine if the filer is in compliance with applicable conflicts of interest laws and ethical standards of conduct regulations, and if so, to sign off on such reports.[1139] If there are assets,

---

[1135] 5 U.S.C. § 102(b)(1).

[1136] 5 U.S.C. app. § 102(b)(1), referencing § 102(a)(1),(3),(4), (6) and (7).

[1137] Ethics in Government Act, Section 102(a)(6)(B); see now 5 U.S.C. app. § 102(a)(6)(B).

[1138] 5 U.S.C. app. § 102(b)(1)(C) and 102(a)(6)(A).

[1139] 5 U.S.C. app. § 106(a),(b)(1).

ownerships, income or associations which indicate a conflict of interest or ethics problem, that is, that "an individual is not in compliance with applicable laws and regulations," then after consultation with the individual, the reviewing ethics official or office may recommend several steps which may be appropriate to rectify the ethics problems, including "divestiture," "restitution," the establishment of a "blind trust," the request for a personal conflict of interest exemption under 18 U.S.C. § 208(b), or a request for a "transfer, reassignment, limitation on duties or resignation."[1140]

Presidential nominees who are subject to Senate confirmation also file with the agency or department in which they will serve. That agency or department conducts an expedited ("accelerated") review of disclosure report,[1141] and where appropriate the reviewing official is to certify that there are no problems with the private financial interests of the nominee, that is, that there are "no unresolved conflict of interest" issues.[1142] Where there are real or apparent conflict of interest problems revealed in the financial disclosure reports, the reviewing official, consulting with the reporting officer, must determine what "remedial action" is to be taken. "Remedial action" may include divestiture where appropriate, agreements to recuse, and the establishment of a qualified blind trust or a diversified trust.[1143] Subsequently, a letter to the Director of the Office of Government Ethics must be provided setting out the apparent or real conflicts of interest, the remedial measures taken to resolve those issues, and any "ethics agreements" entered into to resolve such conflicts.[1144] Ethics agreements are specific agreements between the nominee or official and the agency, as approved by OGE, as to future conduct that the nominee or official will take, such as divestiture, recusal or resignation from an outside position, to resolve a conflict of interest problem.[1145] If the Director of OGE is satisfied that all conflicts have been resolved, the Director signs and dates the report form, then submits the form and any ethics agreement, with a letter to the appropriate Senate committee expressing the Director's opinion that the nominee has complied with all conflict of interest laws and regulations.[1146]

[1140] 5 U.S.C. app. § 106(b)(3).

[1141] 5 C.F.R. § 2634.605(c).

[1142] 5 C.F.R. § 2634.605(c)(2).

[1143] 5 C.F.R. § 2634.605(b)(4) and (5).

[1144] 5 C.F.R. § 2634.605(c)(2)(iii)(B).

[1145] See, generally, 5 C.F.R. § 2634.801 et seq. Ethics agreements are monitored for future compliance by the agency and OGE. 5 C.F.R. § 2634.804; OGE Memoranda, DO-01-013, March 28, 2001, and DT-02-004, March 8, 2002, to Designated Agency Ethics Officials.

[1146] 5 C.F.R. § 2634.605(c)(3).

Committee Requirements for Advice and Consent Positions

As noted, all financial disclosure statements from presidential nominees who require Senate confirmation are forwarded to the committee of jurisdiction from the Office of Government Ethics. The nominee is also required to update the disclosure statement with respect to certain items within five days before nomination hearings. Committees of the Senate, because of the Senate's express constitutional power of approval of presidential nominations of officers of the United States,[1147] are not limited nor restrained by the disclosure forms as to the information that they may request from a nominee to assist in its constitutional "advice and consent" function; and may require any additional information from a nominee that it deems necessary or desirable. Furthermore, a Senate Committee, or the Senate, may require certain ethics agreements from the nominee as to the disposition of certain assets, or the intention to recuse oneself from certain governmental matters, even beyond any "ethics agreement" made between the nominee and agency or OGE officials.[1148]

Disqualification and Prohibited Conflicts of Interest

The principal statutory method of dealing with potential conflicts of interest of an executive branch officer or employee is to require the disqualification (or "recusal") of the officer or employee from participating in any official governmental matter in which that official, or those close to the official whose financial interests may be "imputed" to the official, has any financial interest. The statutory provision requiring disqualification and recusal is a criminal provision of law, and covers only current or existing financial interests of the officer or employee. There is also a "regulatory" recusal requirement that may be broader in some instances than the statutory restriction, and may apply to certain past affiliations and previous economic interests. Current regulations promulgated by the Office of Government Ethics expressly require in certain circumstances that the executive branch official refrain from participating in certain particular matters when businesses, entities, or economic enterprises with which the official had been affiliated in the past one year are parties to or represent parties in that matter; and require as well certain disqualifications for two years in cases where the private entity had made "extraordinary" payments to the government official upon the official's departure.

Statutory Disqualification or Recusal

The federal statutes deal with existing conflicts of interest principally by requiring the disqualification of a federal official from certain governmental

---

[1147] United States Constitution, Article II, Section 2, clause 2.

[1148] 5 U.S.C. app. § 101(b); see 5 C.F.R. § 2634.803(a)(2).

matters in which he may be financially interested, as opposed to specifically requiring the divestiture of conflicting interests. The federal statute at 18 U.S.C. § 208, which is the principal, general conflict of interest provision under federal law, thus requires an official's disqualification (recusal) from a particular governmental matter in which the officer, his or her spouse or dependent "has a financial interest," or where there is affected a financial interest of an outside entity "in which he [the government official] is serving" as an employee, officer or director, or with whom he "is negotiating or has an arrangement" for future employment.[1149] The statutory language is thus stated in the present tense and is directed only to current financial interests and existing arrangements or current understandings for future employment, and the statutory provision does not require disqualification on a matter because of a past affiliation or previous economic interest.[1150]

The statutory provision at 18 U.S.C. § 208 specifically bars a federal officer or employee in the executive branch of the Federal Government from taking official action "personally and substantially" through "decision, approval, disapproval, recommendation, the rendering of advice, investigation or otherwise," in any "particular" governmental matter, such as a proceeding, request for a ruling, claim, or a contract, which affects the financial interests of that officer or employee, that employee's spouse or dependents, or which affects the financial interests of an organization in which the employee is affiliated as an officer, director, trustee, general partner or employee, or "with whom he is negotiating or has any arrangement concerning prospective employment." While there is no de minimis exception expressly stated in the statute, the law does provide that regulations may exempt certain categories of investments and interests which are deemed too remote or inconsequential to affect the performance of an official's governmental duties.[1151] The current Office of Government Ethics regulations exempt several such interests, including all interests in "diversified" mutual funds; interests in sector funds which have some companies affected by a governmental matter but where those companies are outside of the primary sector in which that fund specializes; and other sector funds even specializing in the particular sector but where one's interest in the fund is no more than $50,000; securities, stocks and bonds in a publicly traded company which is a party to and directly affected by a governmental matter if one's ownership value is no more than $15,000; securities, stocks and bonds in such a company which is not a specific party to a matter but is in a class affected by the governmental

---

[1149] 18 U.S.C. § 208 (2000 Code ed.), emphasis added.

[1150] CACI, Inc.-Federal v. United States, 719 F.2d 1567,1578 (Fed. Cir. 1983); Center for Auto Safety v. F.T.C., 586 F. Supp. 1245, 1246 (D.D.C. 1984).

[1151] 18 U.S.C. § 208(b)(2). There may also be an individual exception for a particular government officer made in writing by the officer's appointing authority that the interest in question is "not so substantial as to … affect the integrity of the services" of that officer. 18 U.S.C. § 208(b)(1).

matter, if the employee's ownership interest is no more than $25,000 (if securities in more than one such company are owned, then the aggregate value can not exceed $50,000 to be exempt from the statute).[1152]

Regulatory Disqualification for Current Conflicts of Interest

In addition to the statutory recusal requirement, there also exists regulatory requirements for disqualification for other financial interests and connections. Although the range of private interests potentially affected by an official's governmental actions are broadened in the regulation, the regulatory recusal provision is more narrowly focused than the statutory provision as to those specific governmental matters covered. The regulations of the Office of Government Ethics provide this regulatory disqualification provision to help assure the avoidance of "an appearance of loss of impartiality in the performance of" official duties by a federal employee.[1153] The regulation, in comparison to the statutory recusal requirement, expands the persons and entities who are deemed to be so connected to the employee that their financial interests may be "imputed" to that employee (and, as such, would constitute cause for recusal or disqualification of the employee from a governmental matter affecting or involving those interests); but, as compared to the statutory disqualification, narrows those particular governmental matters that are included in the disqualification requirement. Even if covered by this particular regulatory provision, there are circumstances in which the employee may still be authorized by his or her agency to participate in the particular matter when warranted.[1154]

The regulation requires a government employee in the executive branch to recuse himself or herself from a "particular matter involving specific parties" when (1) the employee knows that the matter will have a direct and predictable effect on the financial interests of a member of his or her household, or (2) when a person or entity with whom the employee has a "covered relationship" is a party or represents a party to the matter. Such recusal should be done under those circumstances when the employee believes that his or her impartiality may be questioned, unless the employee first advises his or her agency about the matter and receives authorization to participate in the matter.[1155] As to current and existing financial interests, the regulation provides that a "covered relationship" is one with: those persons or entities with whom the employee seeks a business, contractual or other financial relationship; a member of the employee's household, or a relative with whom the employee has a close personal

---

[1152] 5 C.F.R. §§ 2640.201 (mutual funds); 2640.202 (securities in companies).

[1153] 5 C.F.R. § 2635.501(a).

[1154] 5 C.F.R. § 2635.502(c),(d).

[1155] 5 C.F.R. § 2635.502(a).

relationship; a person or entity with whom the employee's spouse, child or parent is serving or seeks to serve as an officer, director, trustee, general partner, agent, attorney, consultant, contractor, or employee; or an organization (other than a political party) in which the employee is an active participant.[1156]

As noted, the regulatory recusal requirement, although broader as to the affected financial interests, applies to a narrower range of governmental matters than the statutory provision. The regulation applies only to particular governmental matters "involving specific parties," and as such would not cover such "particular matters" as general policymaking or drafting regulations affecting an economic or business sector; while the statutory recusal requirement applies to all governmental "particular matters," including even the drafting of such regulations.[1157]

One-Year Regulatory Disqualification for Past Affiliations

In addition to the Office of Government Ethics regulations applying a recusal requirement beyond the interests and relationships set out in the criminal conflict of interest statute concerning other current or existing interests, the regulations also expand and apply a potential recusal and disqualification requirement of a federal executive branch official for certain past business and economic associations. The regulations provide that a federal official should recuse or disqualify himself or herself from working on a particular governmental matter involving specific parties if a "person for whom the employee has, within the last year, served as an officer, director, trustee, general partner, agent, attorney, consultant, contractor or employee ..."[1158] is a party or represents a party in such matter. This one-year recusal requirement as to matters involving an official's former employers, businesses, clients or partners, applies to any officer or employee of the executive branch, but applies narrowly only to "a particular matter involving specific parties" when such former employer or business associate is or represents a party to the matter. As noted above, such matters "involving specific parties" cover generally things such as contracts, investigations, or prosecutions involving specific individuals or parties, as opposed to broader "particular matters" which may involve a number of persons or entities (such as most rule making). Notwithstanding the fact that a past employer, client, or business associate with whom the employee has a "covered

---

[1156] 5 C.F.R. § 2635.502(b)(1).

[1157] The statutory disqualification requirement need not involve specific or identified parties, and therefore may apply to any "discrete and identifiable matter" such as "general rulemaking" or proposed regulations (2 Op.O.L.C. 151, 153-154 (1978); 5 C.F.R. § 2635.402(b)(3)), while the regulatory recusal applies only to particular matters involving specific parties, such as a contract or grant, or a particular investigation.

[1158] 5 C.F.R. § 2635.502(a), (b)(1)(iv).

relationship" may be a party or represent a party to such a matter, an employee may, as with the regulatory restriction on current interests, receive authorization by his or her agency to participate in the matter.[1159]

Two-Year Regulatory Disqualification for Extraordinary Payments From Past Employers

In addition to the one-year recusal requirement for particular matters involving specific parties when a former client, employer, firm, or business is or represents a party in that matter, the regulations of the Office of Government Ethics also provide for a two-year recusal requirement which bars an official in the executive branch from participating in a particular matter in which a "former employer" is or represents a party when that former employer had made an "extraordinary payment" to the official prior to entering government. An "extraordinary payment" is one in excess of $10,000 in value made by an employer after the employer has learned that the employee is to enter government service, and one which is not an ordinary payment, that is, is a payment other than in conformance with the employer's "established compensation, benefits or partnership program."[1160] This disqualification provision may be waived in writing by an agency head, or if the individual involved is the head of an agency, by the President or his designee.

Severance Payments, Generally

There is a criminal provision of federal conflict of interest law, at 18 U.S.C. §209, which prohibits a federal employee from receiving any outside, additional or supplemental compensation from a private source for his or her official government duties as a federal employee. One who has entered federal service may not, therefore, accept a salary supplementation from a business or organization intended to "make up the difference" between private sector and Federal Government salaries or to otherwise reward or compensate the new federal employee for his or her public service. This statutory restriction originated in 1917 from an initial legislative concern over private foundations paying the compensation of persons who were serving under a cooperative agreement in the Bureau of Education within the Department of Interior, and the undue and, to some, "noxious" influence of such foundations on national educational policy.[1161] The law at §209 has been described as a conflict of interest

---

[1159] 5 C.F.R. § 2635.502(c),(d).

[1160] 5 C.F.R. § 2635.503(b)(1).

[1161] Formerly 18 U.S.C. §1914; see discussion in The Association of the Bar of the City of New York, Special Committee on the Federal Conflict of Interest Laws, Conflict of Interest and Federal Service, 53-56 (Harvard University Press 1960), and Bayless Manning, Federal Conflict of Interest Law, 148-149 (Harvard University Press 1964).

statute "in the strictest sense," that is, an "employee does not have to do anything improper in his office to violate the statute," but rather his or her special status as a government employee "makes an unexceptionable act wrongful — wrongful because of the potential dangers in serving two paymasters."[1162] The law thus seeks to assure that a federal employee is compensated for his or her services to the government only by the government, is not placed in a position of "serving two masters," and is not, nor appears to be, beholden or grateful to any outside group or private interest which "could affect the independent judgment of the employee."[1163]

This provision might come into play, therefore, regarding certain "severance" payments, packages, or plans from a former private employer to an individual who has entered federal service if there is evidenced an "intent to compensate" an individual for that person's federal employment.[1164] The provision is not as broad in application to severance payments, however, as it may seem at first glance, since the language of the statute applies expressly only to "an officer or employee of the executive branch of the United States Government," and has been interpreted by the courts as applying only to persons who at the time payments were received were federal employees, that is, the restriction does not apply to severance payments which are made at the time one leaves private employment but before the individual actually becomes an officer or employee of the government.[1165] Even if made to reward the employee for taking a public service job, or is intended to or has the effect of instilling in the about-to-become-official a sense of gratitude or goodwill towards the private employer, there is no violation of this criminal conflict of interest provision for severance payments made before one is a federal official, since federal employment status is an express element of the statute. Of course, as noted above, "extraordinary payments" from a private employer to an incoming federal official, even if made before the person is actually a federal employee (and thus not within §209), may still encounter the two-year disqualification requirement under OGE regulations, requiring the recusal of the employee for two years from any particular governmental matter involving that former employer as a party.

[1162] Conflict of Interest and Federal Service, supra at 55-56. There needs to be no wrongful or "corrupt" intent or motivation in the payment of private compensation to an employee for his or her public duties for a violation of the law.

[1163] Roswell B. Perkins, "The New Federal Conflict of Interest Law," 76 Harvard Law Review 1113, 1137 (1963), discussing 18 U.S.C. §209.

[1164] United States v. Muntain, 610 F.2d 964, 969-970 (D.C.Cir. 1979). "Buyouts" of ownership interests, even those made on an installment basis over a few years after the recipient becomes a federal official, may thus not violate the provision since such buyouts are generally moneys received for past interests and work, and as such would lack the "intent to compensate" an employee for current federal duties for the government.

[1165] Crandon v. United States, 494 U.S. 152, 159 (1990).

Pensions: Past or Present Financial Interest?

One of the issues that arises with respect to current or past associations under the statutory recusal or disqualification requirement is the treatment of pensions from outside entities. Pensions generally involve current payments or vested interests from a fund controlled by an outside entity, but in recognition of or as compensation for past services. There are thus questions raised as to whether an employee's vested interest in a pension is a current financial interest or association with or in the entity making the payment, subject to all of the disqualification restrictions and limitations on current and existing financial interests, or whether pensions are excluded from being a disqualifying interest of an employee. The issue under the statutory recusal requirement is, as stated by the Office of Government Ethics, the concern "about an employee's participation in a Government matter that could have an effect on the sponsoring organization that is responsible for funding or maintaining the Government employee's pension plan."[1166]

In interpreting the law at 18 U.S.C. § 208 and the regulations under it, the Office of Government Ethics has distinguished between two common types of pension plans, the "defined benefit plan," and the "defined contribution plan." In a "defined benefit plan," the employer typically "makes payments to an investment pool which it holds and invests for all participating employees"; and such plans are the "obligation of the employer" which pays the former employee an amount generally based on some percentage of what the employee's compensation had been.[1167] A "defined contribution plan," however, typically involves contributions by the employer and/or the employee to a specific, individual retirement account, and the payout of income or annuity is based on the amounts, earnings, gains or losses generated by such account.

The expressed conflict of interest concerns thus generally arise more typically with a "defined benefit plan" type of pension where the employer itself is obligated to make the pension payments, but not so in a "defined contribution plan" where the pension payments come out of an already established and funded retirement account. For purposes of the statutory disqualification requirement, therefore, the Office of Government Ethics would not consider a "defined contribution plan" as a "disqualifying" financial interest of the employee: "For matters affecting the sponsor of a defined contribution plan, an employee's

[1166] OGE Memorandum, 99 x 6, to Designated Agency Ethics Officials, April 14, 1999.

[1167] Id.

interest is not ordinarily a disqualifying financial interest under section 208 because the sponsor is not obligated to fund the employee's pension plan."[1168]

If the employee's pension is based on a "defined benefits plan," then the Office of Government Ethics would consider such a pension as a current, disqualifying interest under 18 U.S.C. § 208, in some circumstances. A defined benefit plan will be considered a disqualifying interest in governmental matters relating to the sponsor of the employee's pension if the governmental matter involved is so significant to the pension's sponsor that it could actually affect employee's pension plan, that is, that "the matter would have a direct and predictable effect on the sponsor's ability or willingness to pay the employee's pension benefit," such as if the matter could result in "the dissolution of the sponsor organization."[1169] OGE notes that in a practical sense, it is unlikely that a governmental matter will have such an effect on a private pension sponsor, since even large contracts worth, for example, $500,000 to a firm, would not materially affect a sizable corporation's ability to pay its pension obligations to former employees.

In most cases it is therefore unlikely that a current interest in or receipt of payment from a pension plan, either a defined benefit or defined contribution plan, would trigger the broad statutory, criminal recusal or disqualification requirement of 18 U.S.C. §208, for a federal employee as to the sponsor of his or her private pension; and the Office of Government Ethics has advised agencies to no longer "automatically presume that employees have a conflict of interest in matters affecting the sponsor of their defined benefit plans."[1170] The private sponsor of a defined benefit pension plan would, however, for purposes of the regulatory "impartiality" requirement, be one with whom the federal employee has a "covered relationship."[1171] In such a case, absent a disclosure to and authorization from the agency, the employee should therefore disqualify himself or herself concerning any official governmental matter which involves the sponsor of the pension plan as a "specific party."[1172]

[1168] Id. It may be noted that stocks, bonds or other securities being held in an employee benefit plan or other retirement plan, such as an IRA or 401(k), are not disqualifying interests if the plan is "diversified," as long as the plan is administered by an independent trustee and the employee does not choose the specific assets in the plan, and the plan is not a profit sharing or stock bonus plan. 5 C.F.R. § 2640.210(c).

[1169] Id.

[1170] Id.

[1171] 5 C.F.R. §2635.502(b)(1)(i), see OGE Memorandum, 99 x 6, supra at n.3

[1172] 5 C.F.R. §2635.502(a).

Divestiture

There is no federal statute which expressly implements a general requirement for federal employees to divest particular private assets or holdings to resolve likely or potential conflicts of interest with employees' public duties. Occasionally, a statutory provision, often the organic act establishing an agency, bureau or commission, will provide expressly that the directors or board members of such entities shall have no financial interests in the business or sector which the agency, bureau or commission is to regulate or oversee. Furthermore, an agency may by regulation prohibit or restrict the ownership of certain financial assets or class of assets by its officers and employees where, because of the mission of the agency, such interests would "cause a reasonable person to question the impartiality and objectivitywith which agency programs areadministered."[1173] In such instances, these statutory and regulatory provisions would, in their effect, require the divestiture of particular assets and holdings of certain individuals to be appointed to such positions or who are incumbents in such positions.

While there is no general statutory divestiture requirement, the divestiture of assets, properties or holdings may be required as a conflict of interest avoidance mechanism by administrative provisions and oversight, as well as by a Senate committee or the Senate as a whole as a condition of favorable action on a presidential nominee requiring Senate confirmation. As noted earlier, the principal statutory method of conflict of interest avoidance, with respect to particular assets and holdings of a federal official, is to require the disqualification of that official from a governmental matter affecting those financial interests. However, under current regulations of the Office of Government Ethics, as part of the ethics review process, an agency may require the divestiture of certain assets of an individual employee where those interests would require the employee's disqualification from matters so central to his or her job that it would impair the employee's ability to do perform his or her duties, or where it could adversely affect the agency's mission because another employee could not easily be substituted for the disqualified employee.[1174] When divestiture is required for ethics reasons, a current employee should be afforded a "reasonable amount of time" to effectuate the disposal of the asset; furthermore, it is possible to ameliorate potential unfair tax burdens that may arise because of such required sale of an asset by receiving a certificate of divestiture and postponing capital gains taxes.[1175]

In some instances, the establishment of a "qualified blind trust" may be used as a conflict of interest avoidance device as an alternative "divestiture" of conflicting

---

[1173] 5 C.F.R. § 2635.403(a).

[1174] 5 C.F.R. § 2635.403(b).

[1175] See 5 C.F.R. §§ 2635.403(d),(e), and 2634.1001 et. seq.

assets. While the underlying assets in a trust in which one has a beneficial interest must normally be disclosed in annual public financial disclosure reports,[1176] and would under conflict of interest law generally be "financial interests" of the employee/beneficiary for disqualification purposes, federal officials may, as a conflict of interest avoidance measure, place certain assets with an independent trustee in what is called a "qualified blind trust."[1177] The nature of a "blind trust," generally, is such that the official will have no control over, will receive no communications about, and will (eventually as existing assets are sold and new ones obtained by the trustee) have no knowledge of the identity of the specific assets held in the trust. As such, an official will not need to identify and disclose the particular assets in the corpus of a "blind trust" in future financial disclosure reports,[1178] and such assets will not be "financial interests" of the employee for disqualification purposes.[1179] The conflict of interest theory under which the blind trust provisions operate is that since the official will not know the identity of the specific assets in the trust, those assets and financial interests could not influence the official decisions and governmental duties of the reporting official, thus avoiding potential conflict of interest problems or appearances.[1180] Assets originally placed into the trust by the official will, of course, be known to that official, and therefore will continue to be "financial interests" of the public official for conflict of interest purposes until the trustee notifies the official "that such asset has been disposed of, or has a value of less than $1,000."[1181]

[1176] 5 U.S.C. app. §102(f)(1).

[1177] See, generally, 5 U.S.C. app. § 102(f). Assets of an official may also be in a qualified "diversified trust" which has been established for the benefit of the official, the official's spouse or children, and may avoid disclosure and conflict of interest disqualification requirements. 5 U.S.C. app. § 102(f)(4)(B). However, in addition to being required to be well-diversified, such a trust may not consist of the assets of entities "having substantial activities in the area of the [official's] primary area of responsibility." 5 U.S.C. app. § 102(f)(4)(B)(i)(II). Such well-diversified portfolios of assets with an independent trustee, with no conflicting assets in the trust portfolio, are not considered "financial interests" of the employee for conflict of interest purposes at any time. 5 C.F.R. § 2634.401(a)(1)(iii).

[1178] 5 U.S.C. app. §102(f)(2)(A).

[1179] 5 U.S.C. app. § 102(f)(4)(A); 5 C.F.R. § 2634.401(ii).

[1180] S.Rept. 95-639, 95th Cong., 2d Sess., Report of the Committee on Governmental Affairs, "Blind Trusts," at 13 (1978).

[1181] 5 U.S.C. app. §102(f)(4)(A); 401(a)(1)(ii). One of the requirements of a blind trust is that there can be no conditions placed on the independent judgment of the trustee to dispose of any assets in the corpus of the trust. 5 U.S.C. app. §102(f)(3)(B).

A Note on General "Impartiality," Alleged "Bias," and Past Affiliations or Activities

The standards of conduct regulations promulgated by the Office of Government Ethics and derived from Executive Order, provide generally that an employee in the executive branch must "act impartially and not give preferential treatment to any organization or individual."[1182] As to past associations, the Office of Government Ethics has noted that "It has long been recognized that former employment with a private organization can raise impartiality concerns. Members of the public, the press, and even the Congress sometimes have questioned whether a particular public official might be subject to continuing influence by a former employer."[1183]

The "general principles" in the OGE regulations regarding financial interests and connections, outside employment or activities, and "impartiality," are fleshed out and covered in the more specific regulations promulgated by OGE.[1184] Although the basic impartiality language is fairly broad on its face, the "impartiality" actually required of a federal employee in a governmental matter by the specific conflict of interest and federal ethics standards, is a disinterestedness in the matter from the point of view of any financial impact that such a matter may have upon the employee personally, or upon certain entities or persons which are closely associated with the employee, that is, those whose financial interests may be fairly "imputed" to the employee.[1185] As noted by the Office of Government Ethics:

Questions regarding impartiality necessarily arise when an employee's official duties impact upon the employee's own financial interests or those of certain other persons, such as the employee's spouse or minor child.[1186]

Thus, while past employment or other past professional affiliations or connections to private entities may implicate conflict of interest concerns and trigger certain restrictions under regulations, the current ethical standards of conduct and conflict of interest rules do not necessarily imply a prohibited "favoritism" or "impartiality" by the mere fact of past employments or past professional associations or positions beyond those past employment

---

[1182] 5 C.F.R. § 2635.101(b)(8).

[1183] OGE Letter Opinion, 01 x 5, July 9, 2001.

[1184] 5 C.F.R. § 2635.101(b): "Where a situation is not covered by the standards set forth in this part, employees shall apply the principles set forth in this section in determining whether their conduct is proper."

[1185] "Impartiality in Performing Official Duties," 5 C.F.R. part 2635, subpart E, §§ 2635.501 et seq.

[1186] 5 C.F.R. § 2635.501, note.

connections that are specifically covered and dealt with in the regulatory disqualification restrictions.[1187] That is, no matter how philosophically pre-disposed an administrative official may arguably seem towards an issue because of his or her professional or employment background, a specific "bias" or "partiality" in a decision cannot be gleaned, as a matter of federal law, merely by the past associations and /or past employment of a federal regulatory or administrative official beyond the specific regulatory restrictions.

In general, the "impartiality" required of a federal employee in a matter clearly does not mean that every federal employee must be completely "neutral" on an issue or matter before him or her, in the sense that the employee has no opinion, view, position or predilection on a matter based either on past associations of the employee, or based upon current non-economic factors such as the ethical, religious, ideological, or political beliefs in the background or in the current affiliations of the employee. In the specific regulations on "impartiality" and participation in outside organizations, in fact, the Office of Government Ethics notes that "Nothing in this section shall be construed to suggest that an employee should not participate in a matter because of his political, religious or moral views."[1188]

As to the issue of "bias" or "impartiality" generally in decision making of federal officials, federal cases dealing with the alleged bias of a federal official have arisen on occasion in a due process context with respect to rule making of an agency, in that there had been alleged a lack of due process or fairness in the agency proceeding because of some claimed "bias" of a federal agency official. In those cases, the courts have noted that when a federal official is not acting in an adjudicatory capacity, that is, in a similar position as a judge, then judicial standards of impartiality need not apply.[1189] The Court of Appeals for the District of Columbia Circuit has noted: "We must not impose judicial roles upon administrators when they perform functions very different from those of judges."[1190] The disqualification requirement for those who are part of formal

---

[1187] In addition to bias because of past employment affiliations, it should be noted that federal employees are specifically prohibited by ethics regulations from using their public office for the financial gain of themselves, their personal friends or for entities with which they are currently affiliated. 5 C.F.R. § 2635.702.

[1188] 5 C.F.R. § 2635.502(b)(1)(v), note.

[1189] Association of National Advertisers, Inc. v. F.T.C., 627 F.2d 1151 (D.C. Cir. 1979), cert. denied, 447 U.S. 921 (1980). The "judicial standard" cited involves such factors as "would lead a reasonable person with the knowledge of all the facts to conclude that [an official's] impartiality might reasonably be questioned." Note discussion in Center for Auto Safety v. F.T.C., 586 F. Supp. 1245, 1248-1249 (D.D.C. 1984); United States v. Halderman, 559 F.2d 31, 132-133 n. 274 (D.C.Cir. 1976); Cinderella Career & Finishing Schools, Inc. v. F.T.C., 425 F.2d 583 (D.C.Cir. 1970).

[1190] Association of National Advertisers, Inc. v. F.T.C., supra at 1168.

adjudications was "never intended ... to apply in a rulemaking procedure," even a formal rulemaking procedure.[1191] In an earlier case in the District of Columbia Circuit, the court had explained:

Agencies are required to consider in good faith, and to objectively evaluate, arguments presented to them; agency officials, however, need not be subjectively impartial.[1192]

Going beyond specific statutory or regulatory restrictions on employees' economic interests and attempting to judicially apply very broad bias or impartiality standards upon regulators and administrators beyond those standards, noted one court, "is to invite challenges to officials based not upon true conflicts of interest but upon their philosophical or ideological leanings ...."[1193] While there could, of course, be legitimate questions raised about general notions of "bias" or partiality in a governmental function based on alleged conflicts or associations of particular employees involved in a certain matter, issues involving the ethics and conflict standards in internal governmental standards of conduct regulations are generally not amenable to legal resolution by private litigants, that is, those regulations do not raise an actionable standard for litigation by outside private parties, but rather are generally considered internal, discretionary or disciplinary matters within the agency.[1194]

[1191] Id.

[1192] Carolina Environmental Study Group v. United States, 510 F.2d 796, 801 (D.C.Cir. 1975).

[1193] Center for Auto Safety v. Federal Trade Commission, 586 F.Supp. 1245, 1248 (D.D.C. 1984).

[1194] Note, Wathan v. United States, 527 F.2d 1191, 1200-1201,1203 (Ct. Claims 1975), rehearing denied, January 30, 1976; Wild v. HUD, 692 F.2d 1129,1131,1133 (7th Cir. 1982). No private cause of action, CACI, Inc.-Federal v. United States, 719 F.2d 1567,1581 (Fed. Cir. 1983); Center for Auto Safety v. Federal Trade Commission, supra.

TITLE 18: CRIMES AND CRIMINAL PROCEDURE

Introduction

Extraterritorial Application of American Criminal Law, 94-166 (March 26, 2010).

CHARLES DOYLE, CONGRESSIONAL RESEARCH SERV., EXTRATERRITORIAL APPLICATION OF AMERICAN CRIMINAL LAW, (2010), *available at* http://www.intelligencelaw.com/library/secondary/crs/pdf/94-166_3-26-2010.pdf.

Charles Doyle
Senior Specialist in American Public Law

Order Code 94-166
March 26, 2010

Summary

Crime is usually territorial. It is a matter of the law of the place where it occurs. Nevertheless, a surprising number of American criminal laws apply outside of the United States. Application is generally a question of legislative intent, expressed or implied. In either case, it most often involves crimes committed aboard a ship or airplane, crimes condemned by international treaty, crimes committed against government employees or property, or crimes that have an impact in this country even if planned or committed in part elsewhere.

Although the crimes over which the United States has extraterritorial jurisdiction may be many, so are the obstacles to their enforcement. For both practical and diplomatic reasons, criminal investigations within another country require the acquiescence, consent, or preferably the assistance, of the authorities of the host country. The United States has mutual legal assistance treaties with several countries designed to formalize such cooperative law enforcement assistance. Searches and interrogations carried out jointly with foreign officials, certainly if they involve Americans, must be conducted within the confines of the Fourth and Fifth Amendments. And the Sixth Amendment imposes limits upon the use in American criminal trials of depositions taken abroad.

The nation's recently negotiated extradition treaties address some of the features of the nation's earlier agreements which complicate extradition for extraterritorial offenses, i.e., dual criminality requirements, reluctance to recognize extraterritorial jurisdiction, and exemptions on the basis of nationality or political offenses. To further facilitate the prosecution of federal crimes with extraterritorial application Congress has enacted special venue, statute of

limitations, and evidentiary statutes. To further cooperative efforts, it recently enacted the Foreign Evidence Request Efficiency Act, P.L. 111-79 (S. 1289) which authorizes federal courts to issue search warrants, subpoenas and other orders to facilitate criminal investigations in this country on behalf of foreign law enforcement officials.

This report is available in an abridged version, stripped of its attachments, bibliography, footnotes, and most of its citations to authority, as CRS Report RS22497, Extraterritorial Application of American Criminal Law: An Abbreviated Sketch.

Introduction

Crime is ordinarily proscribed, tried, and punished according to the laws of the place where it occurs.[1195] American criminal law applies beyond the geographical confines of the United States, however, under certain limited circumstances. State prosecution for overseas misconduct is limited almost exclusively to multi-jurisdictional crimes, i.e., crimes where some elements of the offense are committed within the state and others are committed beyond its boundaries. A surprising number of federal criminal statutes have extraterritorial application, but prosecutions have been few. This may be because when extraterritorial criminal jurisdiction does exist, practical and legal complications, and sometimes diplomatic considerations, may counsel against its exercise.

Constitutional Considerations

Legislative Powers

The Constitution does not forbid either Congressional or state enactment of laws which apply outside the United States. Nor does it prohibit either the federal government or the states from enforcing American law abroad. Several passages suggest that the Constitution contemplates the application of American law beyond the geographical confines of the United States. It speaks, for example, of "felonies committed on the high seas," "offences against the law of nations," "commerce with foreign nations," and of the impact of treaties.

More specifically, it grants Congress the power "[t]o define and punish Piracies and Felonies committed on the high Seas, and Offences against the Law of Nations."[1196] Although logic might point to international law or some other

---

[1195] "The general and almost universal rule is that the character of an act as lawful or unlawful must be determined wholly by the law of the country where the act is done," American Banana Co v. United Fruit Co., 213 U.S. 347, 356 (1909).

[1196] U.S. Const. Art.I, §8, cl. 10; see generally, The Offences Clause After Sosa v. Alvarez-Machain, 118 HARVARD LAW REV. 2378 (2005); Stephens, Federalism and Foreign Affairs: Congress's Power to "Define and Punish . . . Offenses Against the Law of Nations," 42 WILLIAM & MARY LAW REVIEW 447 (2000).

embodiment of "the law of nations" as a source of the dimensions of Congress's authority to define and punish crimes against the law of nations, in reality the courts have done little to identify such boundaries, and until recently Congress seems to have relied exclusively on the law of nations clause only upon rare occasions.

In instances when the law of nations might have been thought to suffice, Congress has, instead, often relied upon a high seas component which, when coupled with its authority to define the admiralty and maritime jurisdictions of the federal courts, permits the application of federal criminal law even to an American vessel at anchor well within the territory of another nation.[1197]

The enactment of maritime statutes is reinforced by Congress's power "[t]o regulate Commerce with foreign Nations."[1198] The same prerogative supports legislation regulating activities in the air when they involve commerce with foreign nations. The commerce power includes the authority "[t]o regulate Commerce with foreign Nations, and among the several States, and with the Indian Tribes." It is a power of exceptional breadth domestically.[1199] Its reach may be even more extraordinary in an international context,[1200] although there is certainly support for a contrary view.[1201] In one of few recent cases to address the

---

[1197] United States v. Flores, 289 U.S. 137, 159 (1933)(Flores, an American seaman, was convicted of murdering another American aboard an American ship moored 250 miles up the Congo River (well within the territorial jurisdiction of the then Belgian Congo) under the federal statute proscribing murder committed within the special maritime jurisdiction of the United States).

[1198] U.S. Const. Art. I, §8, cl.3.

[1199] See e.g., Perez v. United States, 402 U.S. 146, 156-57 (1971); Heart of Atlanta Motel v. United States, 379 U.S. 241, 255-58 (1964).

[1200] California Bankers Ass'n v. Shultz, 416 U.S. 21, 46 (1974)("the plenary authority of Congress over both interstate and foreign commerce is not open to dispute"); United States v. 12,200-Ft. Reels of Film, 413 U.S. 123, 125 (1973)("The Constitution gives Congress broad, comprehensive powers 'to regulate Commerce with foreign Nations'").

[1201] United States v. Yunis, 681 F.Supp. 896, 907 n.24 (D.D.C. 1988)("Rather than relying on Congress's direct authority under Art. I Section 8 to define and punish offenses against the law of nations, the government contends that Congress has authority to regulate global air commerce under the commerce clause. U.S. Const. art. I, § 8, c. 3. The government's arguments based on the commerce clause are unpersuasive. Certainly Congress has plenary power to regulate the flow of commerce within the boundaries of United States territory. But it is not empowered to regulate foreign commerce which has no connection to the United States. Unlike the states, foreign nations have never submitted to the sovereignty of the United States government nor ceded their regulatory powers to the United States"). See also, Colangelo, Constitutional Limits on Extraterritorial Jurisdiction: Terrorism and the Intersection of National and International Law, 48 HARVARD INTERNATIONAL LAW JOURNAL 121, 149-50 (2007)(emphasis in the original) ("Furthermore, as a matter of original intent, the idea that the Foreign Commerce Clause might license Congress with the broad ability to extend U.S. laws extraterritorially into the jurisdictions

issue directly, the court opted for a middle ground. It found that Congress did indeed have the legislative power to proscribe illicit overseas commercial sexual activity by an American who had traveled from the United States to the scene for the crime.[1202] Confronted with a vigorous dissent, the panel's majority expressly chose to avoid the issue of whether it would have reached the same result if the defendant had not agreed to pay for his sexual misconduct.[1203]

In any event, it does not necessarily mean that every statute enacted in the exercise of Congress' power to regulate commerce with foreign nations is intended to have extraterritorial scope. Some do; [1204] others do not.[1205]

Congress has resorted on countless occasions to its authority to enact extraterritorial legislation not only in reliance on its own enumerated powers but also, through the necessary and proper clause on the powers vested in one of the other branches or on powers it shares with one of the other branches.[1206] It has,

---

of other nations would have been anathema to the founders given their driving belief in the sovereign equality of states and its accompanying rigid concept of territoriality – which to borrow yet again from Chief Justice Marshall held that 'no [state] can rightfully impose a rule on another[,] [each] legislates for itself, but its legislation can operate on itself alone.' Recall the reason why Congress was allowed to legislate extraterritorially over piracy absent a U.S. connection even though the act technically occurred within another state's territory: the conduct was prohibited as a matter of the law of nations, not of U.S. law, and thus the United States was not imposing its own rule on other nations, but merely enforcing (on their behalf) a universal norm when it prosecuted pirates. No such analysis applies to extraterritorial projections of Congress' Foreign Commerce Clause power").

[1202] United States v. Clark, 435 F.3d 1100, 1103 (9th Cir. 2006)("Instead of slavishly marching down the path of grafting the interstate commerce framework onto foreign commerce, we step back and take a global, commonsense approach to the circumstances presented here: The illicit sexual conduct reached by the state expressly includes commercial sex acts performed by a U.S. citizen on foreign soil. This conduct might be immoral and criminal, but it is also commercial. Where, as in this appeal, the defendant travels in foreign commerce to a foreign country and offers to pay a child to engage in sex acts, his conduct falls under the broad umbrella of foreign commerce and consequently within congressional authority under the Foreign Commerce Clause").

[1203] Id. at 1109-110 ("At the outset, we highlight that §2423(c) contemplates two types of 'illicit sexual conduct': noncommercial and commercial. Clark's conduct falls squarely under the second prong of the definition, which criminalizes 'any commercial sex act . . . with a person under 18 years of age.' §2423(f)(2). In view of this factual posture, we abide by the rule that courts have a 'strong duty to avoid constitutional issues that need not be resolved in order to determine the rights of the parties to the case under consideration, and limit our holding to §2423(c)'s regulation of commercial sex acts").

[1204] Steele v. Bulova Watch Co., 344 U.S. 280, 285-87 (1952).

[1205] EEOC v. Arabian American Oil Co., 499 U.S. 244, 259 (1991).

[1206] U.S.Const. Art.I, §8, cl.18 ("The Congress shall have Power . . . To make all Laws which shall be necessary and proper for carrying into Execution the foregoing Powers, and all other Powers

for instance, regularly called upon the authority deposited with the President and the Congress in the fields of foreign affairs and military activities,[1207] powers which the courts have described in particularly sweeping terms.[1208]

Constitutional Limitations

Nevertheless, the powers granted by the Constitution are not without limit. The clauses enumerating Congress's powers carry specific and implicit limits which govern the extent to which the power may be exercised overseas.[1209] Other

---

vested by this Constitution in the Government of the United States, or in any Department or Officer thereof").

[1207] See e.g., "The President shall be Commander in Chief of the Army and Navy of the United States, and of the Militia of the several States . . . . He shall have Power, by and with the Advice and Consent of the Senate, to make Treaties, provided two thirds of the Senators present concur; and he shall nominate, and by and with the Advice and Consent of the Senate, shall appoint Ambassadors . . . . He . . . shall receive Ambassadors and other public Ministers; [and] he shall take Care that the Laws be faithfully executed . . . ." U.S. Const. Art.II, §§2, 3.

"The Congress shall have Power To lay and collect Taxes, Duties, Imposts and Excises . . . ; To establish an uniform Rule of Naturalization . . . ; To declare War, grant Letters of Marque and Reprisal, and make Rules concerning Captures on Land and Water; To raise and support Armies . . .; To provide and maintain a Navy; To make Rules for the Government and Regulation of the land and naval Forces; . . . [and] To make all Laws which shall be necessary and proper for carrying into Execution the foregoing Powers, and all other Powers vested by this Constitution in the Government of the United States, or in any Department or Officer thereof." U.S. Const. Art.I, §8, cls.1, 4, 11-14, 18.

[1208] United States v. Curtiss-Wright Corp., 299 U.S. 304, 315-18 (1936); Ex parte Quirin, 317 U.S. 1, 28-9 (1942); Parker v. Levy, 417 U.S. 733, 756-57 (1974).Some judicial authorities have suggested that in the area of foreign affairs the Constitution's establishment of the federal government as a sovereign entity vested it with authority, defined by standards recognized by the law of nations, beyond its constitutionally enumerated powers. United States v. Rodriguez, 182 F.Supp. 479, 490-91 (S.D.Cal. 1960), aff'd sub nom., Rocha v. United States, 288 F.2d 545 (9th Cir. 1961)("The powers of the government and the Congress in regard to sovereignty are broader than the powers possessed in relation to internal matters, United States v. Curtiss-Wright Export Corp., 1936, 299 U.S. 304: 'The broad statement that the federal government can exercise no powers except those specifically enumerated in the Constitution, and such implied powers as are necessary and proper to carry into effect the enumerated powers, is categorically true only in respect to our internal affairs.' Id., 299 U.S. at page 315. . . . 'It results that the investment of the federal government with the powers of external sovereignty did not depend upon the affirmative grants of the Constitution. Id. 299 U.S. at page 318.' . . . To put it in more general terms, the concept of essential sovereignty of a free nation clearly requires the existence and recognition of an inherent power in the state to protect itself from destruction. This power exists in the United States government absent express provision in the Constitution and arises from the very nature of the government which was created by the Constitution").

[1209] Toth v. Quarles, 350 U.S. 11, 13-4 (1955) (court martial trial of a civilian for crimes he allegedly committed in Korea while in the military exceeded the authority granted Congress by Art.I, §8, cl.14 and Art.III, §2); Kinsella v. Singleton, 361 U.S. 234, 247-48 (1960)(holding that

limitations appear elsewhere in the Constitution, most notably in the due process clauses of the Fifth and Fourteenth Amendments. Some limitations are a product of the need to harmonize potentially conflicting grants of authority. For example, although the Constitution reserves to the states the residue of governmental powers which it does not vest elsewhere, the primacy it affords the federal government in the area of foreign affairs limits the authority of the states in the field principally to those areas where they are acting with federal authority or acquiescence.[1210]

In the area of extraterritorial jurisdiction, the most often cited limitation resides in the due process clauses of the Fifth and Fourteenth Amendments. While the enumerated powers may carry specific limits which govern the extent to which the power may be exercised overseas, the general restrictions of the due process clauses, particularly the Fifth Amendment due process clause, have traditionally been mentioned as the most likely to define the outer reaches of the power to enact and enforce legislation with extraterritorial application.[1211]

Unfortunately, most of the cases do little more than note that due process restrictions mark the frontier of the authority to enact and enforce American law abroad.[1212] Even the value of this scant illumination is dimmed by the realization that the circumstances most likely to warrant such due process analysis are the

---

Congressional authority under Art.I, §8, cl.14 to make rules and regulations governing the land and naval forces did not include authority for the court martial trial of civilian dependents for offenses committed overseas); consider, Lowenfeld, U.S. Law Enforcement Abroad: The Constitution and International Law, 83 AMERICAN JOURNAL OF INTERNATIONAL LAW 880, 891-92 (1989) (asserting that the creation of subject matter and personal jurisdiction over an alien defendant for an offense committed overseas and not otherwise connected to the United States by forcibly bringing him into the United States is "not clearly within any constitution grant of power to Congress, and in particular, . . . does not, as written, come within the power to define and punish offenses against the law of nations").

[1210] Cf., Skiriotes v. Florida, 313 U.S. 69, 77 (1941)("[W]e see no reason why the State of Florida may not likewise govern the conduct of its citizens upon the high seas with respect to matters in which the State has a legitimate interest and where there is no conflict with acts of Congress"); American Insurance Ass'n v. Garamendi, 539 U.S. 396, 413 (2003)("There is, of course, no question that at some point an exercise of state power that touches on foreign relations must yield to the National Government's policy, given the concern for uniformity in this country's dealing with foreign nations that animated the Constitution's allocation of the foreign relations power to the National Government in the first place").

[1211] "No person shall . . . be deprived of life, liberty, or property, without due process of law. . . ." U.S. Const. Amend.V. ". . . [N]or shall any State deprive any person of life, liberty, or property, without due process of law . . . ." U.S. Const. Amend.XIV, §1.

[1212] See e.g., United States v. Yousef, 327 F.3d 56, 86 (2d Cir. 2003); United States v. Thomas, 893 F.2d 1066, 1068 (9th Cir. 1990); United States v. Quemener, 789 F.2d 145, 156 (2d Cir. 1986); United States v. Henriquez, 731 F.2d 131, 134-35 n.4, 5(2d Cir. 1984); United States v. Pinto-Mejia, 720 F.2d 248, 259 (2d Cir. 1983); United States v. Howard-Arias, 679 F.2d 363, 371 (4th Cir. 1982).

very ones for which the least process is due. Although American courts that try aliens for overseas violations of American law must operate within the confines of due process,[1213] the Supreme Court has observed that the Constitution's due process commands do not protect aliens who lack any "significant voluntary connection[s] with the United States."[1214]

Moreover, the Court's more recent decisions often begin with the assumption that the issues of extraterritorial jurisdiction come without constitutional implications.[1215]

The handful of lower courts to consider due process issues take one of two tracks. Some describe a due process requirement that demands some nexus between the United States and the circumstances of the offense.[1216] In some instances they

---

[1213] United States v. Verdugo-Urquidez, 494 U.S. 259, 278 (1990) (Kennedy, J., concurring) ("I do not mean to imply, and the Court has not decided, that persons in the position of the respondent have no constitutional protection. The United States is prosecuting a foreign national in a court established under Article III, and all of the trial proceedings are governed by the Constitution. All would agree, for instance that the dictates of the Due Process Clause of the Fifth Amendment protect the defendant").

[1214] "The global view . . . of the Constitution is also contrary to this Court's decisions in the Insular Cases, which held that not every constitutional provision applies to governmental activity even where the United States has sovereign power. . . . [I]t is not open to us in light of the Insular Cases to endorse the view that every constitutional provision applies wherever the United States Government exercises its power. Indeed, we have rejected the claim that aliens are entitled to Fifth Amendment rights outside the sovereign territory of the United States." United States v. Verdugo-Urquidez, 494 U.S. at 268-71.

[1215] EEOC v. Arabian American Oil Co., 499 U.S. at 248 ("Both parties concede, as they must that Congress has the authority to enforce its laws beyond the territorial boundaries of the United States. Whether Congress has in fact exercised that authority in this case is a matter of statutory construction").

[1216] United States v. Medjuck, 156 F.3d 916, 918 (9th Cir. 1998)("to satisfy the strictures of due process, the Government [must] demonstrate that there exists a sufficient nexus between the conduct condemned and the United States such that the application of the statute [to the overseas conduct of an alien defendant] would not be arbitrary or fundamentally unfair to the defendant"), citing, United States v. Davis, 905 F.2d at 248-49; see also, United States v. Perlaza, 439 F.3d 1149, 1160-161 (9th Cir. 2006); United States v. Moreno-Morillo, 334 F.3d 819, 828 (9th Cir. 2003); United States v. Klimavicius-Viloria, 144 F.3d 1249, 1256 (9th Cir. 1998); United States v. Greer, 956 F.Supp. 531, 534-36 (D.Vt. 1997); United States v. Aikens, 946 F.2d 608, 613-14 (9th Cir. 1990); United States v. Robinson, 843 F.2d 1, 5-6 (1st Cir. 1988); United States v. Peterson, 812 F.2d 486, 493 (9th Cir. 1987); United States v. Gonzalez, 776 F.2d 931, 938-41 (11th Cir. 1985).

These "subject matter" or "legislative" jurisdiction due process questions have arisen more often from attempts to impose civil liability or regulatory obligations, particularly at the state level, see e.g., Gerling Global Reinsurance Corp. v. Gallagher, 267 F.3d 1228, 1234-238 (11th Cir. 2001)(due process precludes application of Florida's Holocaust Victims Insurance Act to insurance policies issued outside the state, to persons outside the state, and covering individuals outside the state);

look to international law principles to provide a useful measure to determine whether the nexus requirement has been met;[1217] in others they consider principles at work in the minimum contacts test for personal jurisdiction.[1218] At the heart of these cases is the notion that due process expects that a defendant's conduct must have some past, present, or anticipated locus or impact within the United States before he can fairly be held criminal liable for it in an American court. The commentators have greeted this analysis with hesitancy at best,[1219] and other courts have simply rejected it.[1220]

---

see also, Gerling Global Reinsurance Corp. v. Low, 240 F.3d 739, 753 (9th Cir. 2001); Watson v. Employers Liability Assurance Corp., 348 U.S. 66, 70-1 (1954)("because the policy was bought, issued and delivered outside of Louisiana, Employers invokes the due process principle that a state is without power to exercise 'extra territorial jurisdiction' that is, to regulate and control activities wholly beyond its boundaries").

[1217] United States v. Davis, 905 F.2d 245, 249 n.2 (9th Cir. 1990) ("International law principles may be useful as a rough guide of whether a sufficient nexus exists between the defendant and the United States so that application of the statute in question would not violate due process. However, danger exists that emphasis on international law principles will cause us to lose sight of the ultimate question: would application of the statute to the defendant be arbitrary or fundamentally unfair?"); cf., United States v. Caicedo, 47 F.3d 370, 372-73 (9th Cir. 1995).

[1218] United Sates v. Clark, 435 F.3d 1100, 1108 (9th Cir. 2006)("Although Clark's citizenship alone is sufficient to satisfy due process concerns, his U.S. investments, ongoing receipt of federal retirement benefits and use of U.S. military flights also underscore his multiple and continuing ties with this country"); United States v. Zakharov, 468 F.3d 1171, 1177 (9th Cir. 2006)("Nexus is a constitutional requirement analogous to 'minimum contacts' in personal jurisdiction analysis"); United States v. Klimavicius-Viloria, 144 F.3d at 1257 (citing World-Wide Volkswagen Corp. v. Woodson, 444 U.S. 286, 297 (1980)); United States v. Aikens, 946 F.2d 608, 613-14 (9th Cir. 1990); United States v. Robinson, 843 F.2d 1, 5-6 (1st Cir. 1988); United States v. Peterson, 812 F.2d 486, 493 (9th Cir. 1987); United States v. Gonzalez, 776 F.2d 931, 938-41 (11th Cir. 1985).

[1219] Brilmayer & Norchi, Federal Extraterritoriality and Fifth Amendment Due Process, 105 HARVARD LAW REVIEW 1217 (1992); Weisburd, Due Process Limits on Federal Extraterritorial Legislation? 35 COLUMBIA JOURNAL OF TRANSNATIONAL LAW 379 (1997); Due Process and True Conflicts: The Constitutional Limits on Extraterritorial Federal Legislation and the Cuban Liberty and Democratic Solidarity (Libertad) Act of 1996, 46 CATHOLIC UNIVERSITY LAW REVIEW 907 (1997); Colangelo, Constitutional Limits on Extraterritorial Jurisdiction: Terrorism and the Intersection of National and International Law, 48 HARVARD INTERNATIONAL LAW JOURNAL 121 (2007).

[1220] United States v. Suerte, 291 F.3d 366, 375 (5th Cir. 2002)("[T]o the extent the Due Process Clause may constrain the MDLEA's extraterritorial reach, that clause does not impose a nexus requirement, in that Congress has acted pursuant to the Piracies and Felonies Clause"); United States v. Perez-Oviedo, 281 F.3d 400, 403 (3d Cir. 2002)(internal citations omitted)("[N]o due process violation occurs in an extraterritorial prosecution under MDLEA when there is no nexus between the defendant's conduct and the United States. Since drug trafficking is condemned universally by law-abiding nations . . . there is no reason for us to conclude that it is 'fundamentally unfair' for Congress to provide for the punishment of a person apprehended with narcotics on the high seas. . . Perez-Oviedo's state of facts presents an even stronger case for concluding that no due process violation occurred. The Panamanian government expressly consented to the application of the MDLEA. . . Such consent from the flag nation eliminates a concern that the application of the MDLEA may be arbitrary or fundamentally unfair"); United

The second, less traveled track sees the due process component at issue as one of notice. It is akin to the proscriptions against secret laws and vague statutes, the exception to the maxim that ignorance of the law is no defense.[1221] Under this view, indicia of knowledge, of reason to know, of an obligation to know, or of reasonable ignorance of the law's requirements – some of which are reflected in international standards – seem to be the most relevant factors. Citizens, for instance, might be expected to know the laws of their own nation; seafarers to know the law of the sea and consequently the laws of the nation under which they sail; everyone should be aware of the laws of the land in which they find themselves and of the wrongs condemned by the laws of all nations.[1222] On the other hand, the application of American criminal statute to an alien in a foreign country under whose laws the conduct is lawful would seem to evidence a lack of notice sufficient to raise due process concerns.[1223]

States v. Cardales, 168 F.3d 548, 553 (1st Cir. 1999) ("[D]ue process does not require the government to prove a nexus between a defendant's criminal conduct and the United States in a prosecution under the MDLEA when the flag nation has consented to the application of United States law to the defendants").

[1221] "The rule that ignorance of the law will not excuse is deep in our law, as is the principle that of all the powers of local government, the police power is one of the least limitable. On the other hand, due process places some limits on its exercise. Ingrained in our concept of due process is the requirement of notice. . . . As Holmes wrote in the Common Law, 'A law which punished conduct which would not be blameworthy in the average member of the community would be too severe for that community to bear.' Its severity lies in the absence of an opportunity either to avoid the consequences of the law or to defend any prosecution brought under it. Where [as here] a person did not know of the duty to register and where there was no proof of the probability of such knowledge, he may not be convicted consistently with due process. Were it otherwise, the evil would be as great as it is when the law is written in print too fine to read or in a language foreign to the community." Lambert v. California, 355 U.S. 225, 228-30(1957)(emphasis added)(citations omitted); accord, United States v. Vasarajs, 908 F.2d 443, 448-49 (9th Cir. 1990); Griffin v. Wisconsin, 483 U.S. 868, 875 n.3 (1987); United States v. Shi, 525 F.3d 709, 722 (9th Cir. 2008)("The Due Process Clause requires that a defendant prosecuted in the United States should reasonably anticipate being haled into court in this country").

[1222] United States v. Bin Laden, 92 F.Supp.2d 189, 218 (S.D.N.Y. 2000)("Odeh argues that application of Sections 844(f), (h), and (n); 924(c); 930(c); and 2155 to the extraterritorial conduct he is alleged to have engaged in would violate his due process right to a fair warning. . . .The Government responds that while Odeh may not have known that breadth of the statutory framework that would serve as the basis for the charges against him . . . there is no room for him to suggest that he has suddenly learned that mass murder was illegal in the United States or anywhere else. . . . The Government also argues that Odeh cannot be surprised to learn that his conduct was criminal under the laws of every civilized nation, and thus he has no right to complain about the particular forum in which he is brought to trial. We likewise find this argument persuasive").

[1223] Consider e.g., United States v. Henriquez, 731 F.2d 131, 134 n.5 (2d Cir. 1984) ("It is also argued that 21 U.S.C. §955a(a) as applied [possession of marijuana with intent to distribute by Colombian nationals aboard a non-American vessel in international waters] violates the notice requirement of the due process clause of the Fifth Amendment. See Lambert v. California . . . . The argument is based not only on the claim that the statute is unprecedented in international

Conceding this outer boundary, however, the courts fairly uniformly have held that questions of extraterritoriality are almost exclusively within the discretion of Congress; a determination to grant a statutory provision extraterritorial application – regardless of its policy consequences – introduces no new constitutional infirmities.

Statutory Construction

For this reason, the question of the extent to which a particular statute applies outside the United States has generally been considered a matter of statutory, rather than constitutional, construction.[1224] General rules of statutory construction have emerged which can explain, if not presage, the result in a given case. The first of these holds that a statute will be construed to have only territorial application unless there is a clear indication of some broader intent.[1225]

---

law and the proposition that marijuana trafficking itself is not universally condemned, but also on the alleged vagueness of the definition of 'vessel without nationality' in 21 U.S.C. §955b(d) [upon which federal jurisdiction was based]. On this point, however, we agree with the Eleventh Circuit . . . that the term 'vessel without nationality' clearly encompasses vessels not operating under the authority of any sovereign nation"); United States v. Alvarez-Mena, 765 F.2d 1259, 1267 n.11 (5th Cir. 1985) ("[n]evertheless, we observe that we are not faced with a situation where the interests of the United States are not even arguably potentially implicated. The present case is not remotely comparable to, for example, the case of an unregistered small ship owned and manned by Tanzanians sailing from that nation to Kenya on which a crew member carries a pound of marihuana to give to a relative for his personal consumption in the latter country")(example offered in discussion of presumption of Congressional intent).

[1224] EEOC v. Arabian American Oil Co., 499 U.S. at 248; Foley Brothers v. Filardo, 336 U.S. 281, 284-85 (1949)("The question before us is not the power of Congress to extend the eight hour law to work performed in foreign countries. Petitioners concede that such power exists. The question is rather whether Congress intended to make the law applicable to such work"); United States v. Yousef, 327 F.3d 56, 86 (2d. Cir. 2003)("It is beyond doubt that, as a general proposition, Congress has the authority to enforce its laws beyond the territorial boundaries of the United States"); United States v. Gatlin, 216 F.3d 207, 211 (2d Cir. 2000); United States v. Martinez, 599 F.Supp.2d 784, 79697 (W.D.Tex. 2009).

[1225] "It is a long-standing principle of American law that legislation of Congress, unless a contrary intent appears, is meant to apply only within the territorial jurisdiction of the United States." EEOC. v. Arabian American Oil Co., 499

U.S. at 248 (1991); Argentine Republic v. Amerada Hess Shipping, 488 U.S. 428, 440 (1989); Sale v. Haitian Centers Council, Inc., 509 U.S. 155, 173 (1993); Smith v. United States, 507 U.S. 197, 203 (1993); Small v. United States, 544 U.S. 385, 388-89 (2005); cf., The Antelope, 23 U.S. 30, 53-4 (10 Wheat. 66, 123) (1825)("The courts of no country will execute the penal laws of another"). The principle has a corollary, the so-called revenue rule, which precludes judicial enforcement of a foreign tax laws, Pasquantino v. United States, 544 U.S. 349, 360-61 (2005). The rule, however, does not preclude enforcement of a federal criminal statute which proscribes defrauding a foreign country of its tax revenues, id. at 354-55 ("the common-law revenue rule, rather than barring any recognition of foreign revenue law, simply allow[s] courts to refuse to enforce the tax judgments of foreign nations, and therefore [does] not preclude the Government from prosecuting. . .").

A second rule of construction states that the nature and purpose of a statute may provide an indication of whether Congress intended a statute to apply beyond the confines of the United States. Although hints of it can be found earlier,[1226] the rule was first clearly announced in United States v. Bowman, 260 U.S. 94, 97-98, 102 (1922).[1227]

[1226] See e.g., American Banana Co. v. United Fruit Co., 213 U.S. at 355-56, "It is obvious that, however stated, the plaintiff's case depends on several rather startling propositions. In the first place the acts causing the damage were done so far as appears, outside the jurisdiction of the United States and within that of other states. It is surprising to hear it argued that they were governed by the act of Congress.

"No doubt in regions subject to no sovereign, like the high seas, or to no law that civilized countries would recognize as adequate, such countries may treat some relations between their citizens as governed by their own law, and keep to some extent the old notion of personal sovereignty alive. They go further at times and declare that they will punish any one, subject or not, who shall do certain things, if they can catch him, as in the case of pirates on the high seas. In cases immediately affecting national interests they may go further still and may make, and, if they get the chance, execute similar threat as to acts done within another recognized jurisdiction. An illustration from our statutes is found with regard to criminal correspondence with foreign governments. . ."

[1227] "We have in this case a question of statutory construction. The necessary locus, when not specifically defined, depends upon the purpose of Congress as evinced by the description and nature of the crime and upon the territorial limitations upon the power and jurisdiction of a government to punish crime under the law of nations. Crimes against private individuals or their property, like assaults, murder, burglary, larceny, robbery, arson, embezzlement and frauds of all kinds, which affect the peace and good order of the community, must of course be committed within the territorial jurisdiction of the government where it may properly exercise it. If punishment of them is to be extended to include those committed outside the strict territorial jurisdiction, it is natural for Congress to say so in the statute, and failure to do so will negate the purpose of Congress in this regard. We have an example of this in the attempted application of the prohibitions of the Anti-Trust Law to acts done by citizens of the United States against other such citizens in a foreign country. American Banana Co. v. United Fruit Co., 213 U.S. 347. That was a civil case, but as the statute is criminal as well as civil, it presents an analogy.

"But the same rule of interpretation should not be applied to criminal statutes which are, as a class, not logically dependent on their locality for the government's jurisdiction, but are enacted because of the right of the government to defend itself against obstruction, or fraud wherever perpetrated, especially if committed by its own citizens, officers or agents. Some such offenses can only be committed within the territorial jurisdiction of the Government because of the local acts required to constitute them. Others are such that to limit their locus to the strictly territorial jurisdiction would be greatly to curtail the scope and usefulness of the statute and leave open a large immunity for frauds as easily committed by citizens on the high seas and in foreign countries as at home. In such cases, Congress has not thought it necessary to make specific provision in the law that the locus shall include the high seas and foreign countries, but allows it to be inferred from the nature of the offense. . . . Clearly it is no offense to the dignity or right of sovereignty of Brazil [– where the fraud of which the United States government was the target occurred –] to hold [these American defendants] for this crime against the government to which they owe allegiance." See also, United States v. Delgado-Garcia, 374 F.3d 1337, 1344-350 (D.C.

The final rule declares that unless a contrary intent is clear, Congress is assumed to have acted so as not to invite action inconsistent with international law.[1228] At one time, the cases seemed to imply the existence of another rule, that is that, unless Congress declared that it intended a statute to apply overseas to both aliens and American nationals, it would be presumed to apply only to Americans.[1229] In the eyes of the community of nations, a jurisdictional claim over misconduct based solely on the nationality of the victim continues to be among the more tenuous. Yet as discussed below, the challenge seems less compelling in light of the generous reading of the internationally recognized grounds upon which to stake a claim.[1230]

Cir. 2004); United States v. Villanueva, 408 F.3d 193, 197-98 (5th Cir. 2005); United States v. Lopez-Vanegas, 493 F.3d 1305, 1311-312 (11th Cir. 2007).

[1228] "It has been a maxim of statutory construction since the decision in Murray v. The Charming Betsy, 2 Cranch [6 U.S.] 64, 118 (1804), that an act of Congress ought never to be construed to violate the law of nations, if any other possible construction remains," Weinberger v. Rossi, 456 U.S. 25, 32 (1982); The Apollon, 22 U.S. (9 Wheat.) 362, 370-71 (1824)("It cannot be presumed, that Congress would voluntarily justify . . . a clear violation of the law of nations").

[1229] E.g., The Apollon, 22 U.S. (9 Wheat.) at 370 ("The laws of no nation can justly extend beyond its own territories, except so far as regards its own citizens")(emphasis added); American Banana Co. v. United Fruit Co., 213 U.S. at 355-6 ("No doubt in regions subject to no sovereign, like the high seas, or to no law that civilized countries would recognize as adequate, such countries may treat some relations between their citizens as governed by their own law, and keep to some extent the old notion of personal sovereignty alive. . . . And the notion that English statutes bind British subjects everywhere has found expression in modern times and has had some startling applications"); United States v. Bowman, 260 U.S. at 102 ("Section 41 of the Judicial Code provides that 'the trial of all offenses committed on the high seas, or elsewhere out of the jurisdiction of any particular State or district, shall be in the district where the offender is found, or into which he is first brought.' The three defendants who were found in New York were citizens of the United States and were certainly subject to such laws as it might pass to protect itself and its property. Clearly it is no offense to the dignity or right of sovereignty of Brazil to hold them for this crime against the government to which they owe allegiance. The other defendant is a subject of Great Britain. He has never been apprehended, and it will be time enough to consider what, if any, jurisdiction the District Court below has to punish him when he is brought to trial"); United States v. Columba-Colella, 604 F.2d 356, 360 (5th Cir. 1979) ("Congress [is] not competent to attach criminal sanctions to the murder of an American by a foreign national in a foreign country. . .").

[1230] E.g., United States v. Vasquez-Velasco, 15 F.3d 833, 839-41 (9th Cir. 1994)(prosecution under 18 U.S.C. 1959 for the murder of two American tourists in Mexico by Mexican nationals acting under the mistaken belief that the Americans were DEA agents came within the principle recognized in international law as permitting the exercise of extraterritorial jurisdiction in the name of a nation's security); United States v. Yunis, 924 F.2d 1086, 1091 (D.C.Cir. 1991); United States v. Felix-Gutierrez, 940 F.2d 1200, 1205-206 (9th Cir. 1991)(murder of an American agent overseas); United States v. Benitez, 741 F.2d 1312, 1316-317 (11th Cir. 1986); see also, United States v. Bin Laden, 92 F.Supp.2d 189, 194-95 (S.D.N.Y.2000) (concluding that Bowman applies regardless of the nationality of the offender).

International Law

International law supports rather than dictates decisions in the area of the overseas application of American law. Neither Congress nor the courts are bound to the dictates of international law when enacting or interpreting statutes with extraterritorial application.[1231]

Yet Congress looks to international law when it evaluates the policy considerations associated with legislation that may have international consequences. For this reason, the courts interpret legislation with the presumption that Congress or the state legislature intends its laws to be applied within the bounds of international law, unless it indicates otherwise.

To what extent does international law permit a nation to exercise extraterritorial criminal jurisdiction? The question is essentially one of national interests. What national interest is served by extraterritorial application and what interests of other nations suffer by an extraterritorial application?

The most common classification of these interests dates to a 1935 Harvard Law School study which divided them into five categories or principles corresponding to the circumstances under which the nations of the world had declared their criminal laws applicable: (1) the territorial principle which involves crimes occurring or having an impact within the territory of a country; (2) the nationality principle which involves crimes committed by its nationals; (3) the passive personality principle which involves crimes committed against its nationals; (4) the protection principle which involves the crimes which have an impact on its interests as a nation; and (5) the universal principle which involves crimes which are universally condemned.[1232]

[1231] "Yunis seeks to portray international law as a self-executing code that trumps domestic law whenever the two conflict. That effort misconceives the role of judges as appliers of international law and as participants in the federal system. Our duty is to enforce the Constitution, laws, and treaties of the United States, not to conform the law of the land to norms of customary international law," United States v. Yunis, 924 F.2d 1086, 1091 (D.C.Cir. 1991); United States v. Yousef, 327 F.3d 56, 86 (2d Cir. 2003)("In determining whether Congress intended a federal statute to apply to overseas conduct, an act of Congress ought never to be construed to violate the law of nations if any other possible construction remains. Nonetheless, in fashioning the reach of our criminal law, Congress is not bound by international law. If it chooses to do so, it may legislate with respect to conduct outside the United States in excess of the limits posed by international law"); United States v. Felix-Gutierrez, 940 F.2d 1200, 1203 (9th Cir. 1991); United States v. Henriquez, 731 F.2d 131, 134 (2d Cir. 1984).

[1232] "An analysis . . . discloses five general principles on which a more or less extensive penal jurisdiction is claimed by States at the present time. These five general principles are: first, the territorial principle, determining jurisdiction by reference to the place where the offence is committed; second, the nationality principle, determining jurisdiction by reference to the nationality or national character of the person committing the offence; third, the protective principle, determining jurisdiction by reference to the national interest injured by the offence;

The American Law Institute's Third Restatement of the Foreign Relations Law of the United States contains perhaps the most comprehensive, contemporary statement of international law in the area. It indicates that the latitude international law affords a country to enact, try, and punish violations of its law extraterritorially is a matter of reasonableness, and its assessment of reasonableness mirrors a balancing of the interests represented in the principles.[1233]

---

fourth, the universality principle, determining jurisdiction by reference to the custody of the person committing the offence; and fifth, the passive personality principle, determining jurisdiction by reference to the nationality or national character of the person injured by the offence. Of these five principles, the first is everywhere regarded as of primary importance and of fundamental character. The second is universally accepted, though there are striking differences in the extent to which it is used in different national systems. The third is claimed by most States, regarded with misgivings in a few, and generally ranked as the basis for an auxiliary competence. The fourth is widely though by no means universally accepted as the basis of an auxiliary competence, except for the offence of piracy, with respect to which it is the generally recognized principle of jurisdiction. The fifth, asserted in some form by a considerable number of States and contested by others, is admittedly auxiliary in character and is probably not essential for any State if the ends served are adequately provided for on other principles." Harvard Research in International Law, Jurisdiction with Respect to Crime, 29 AMERICAN JOURNAL OF INTERNATIONAL LAW (Supp.)(Harvard Study) 439, 445 (1935) (emphasis added).

[1233] "The rules in this Restatement governing jurisdiction to prescribe, as well as those governing jurisdiction to adjudicate and to enforce, reflect development in the law as given effect by United States courts. The courts appear to have considered these rules as a blend of international law and domestic law, including international 'comity' as part of that law. Increasingly, however, these rules, notably the principle of reasonableness (§§403, 421, 431), have been followed by other states and their courts and by international tribunals, and have emerged as principles of customary law." American Law Institute, 1 RESTATEMENT OF THE LAW THIRD: THE FOREIGN RELATIONS LAW OF THE UNITED STATES, 231 (1985).

Section 403 of the Restatement provides:

"(2) Whether exercise of jurisdiction over a person or activity is unreasonable is determined by evaluating all relevant factors, including, where appropriate: (a) the link of the activity to the territory of the regulated state, i.e., the extent to which the activity takes place within the territory, or has substantial, direct, and foreseeable effect upon or in the territory; (b) the connections, such as nationality, residence, or economic activity, between the regulating state and the person principally responsible for the activity to be regulated, or between that state and those whom the regulation is designed to protect; (c) the character of the activity to be regulated, the importance of regulation to the regulating state, the extent to which other states regulate such activities, and the degree to which the desirability of such regulation is generally accepted; (d) the existence of justified expectations that might be protected or hurt by the regulation; (e) the importance of the regulation to the international political, legal, or economic system; (f) the extent to which the regulation is consistent with the traditions of the international system; (g) the extent to which another state may have an interest in regulating the activity; and (h) the likelihood of conflict with regulation by another state.

"(3) When it would not be unreasonable for each of two states to exercise jurisdiction over a person or activity, but the prescriptions by the two states are in conflict, each state has an obligation to evaluate its own as well as the other state's interest in exercising jurisdiction, in light

---

While the Restatement's views carry considerable weight with both Congress and the courts,[1234] the courts have traditionally ascertained the extent to which international law would recognize extraterritorial application of a particular law by citing the Harvard study principles, read expansively.[1235]

Even by international standards, however, the territorial principle applies more widely than its title might suggest. It covers conduct within a nation's geographical borders. Yet, it also encompasses laws governing conduct on its territorial waters, conduct on its vessels on the high seas, conduct committed only in part within its geographical boundaries, and conduct elsewhere that has an impact within its territory.[1236] Congress often indicates within the text of a statute when it intends a provision to apply within its territorial waters and upon its vessels.[1237] Although rarely mentioned in the body of a statute, the courts have long and regularly acknowledged the "impact" basis for a claim of extraterritorial application.[1238] This is particularly so, when the facts in a case suggest other principles of international law in addition to the territorial principle.[1239]

---

of all the relevant factors, Subsection (2); a state should defer to the other state if that state's interest is clearly greater." Id. at 244-45. The remainder of section 403 and other portions of the RESTATEMENT appear as an attachment to this report.

[1234] E.g., United States v. MacAllister, 160 F.3d 1304, 1308 (11th Cir. 1998).

[1235] Gibney, The Extraterritorial Application of U.S. Law: The Perversion of Democratic Governance, the Reversal of Institutional Roles, and the Imperative of Establishing Normative Principles, 19 BOSTON COLLEGE INTERNATIONAL & COMPARATIVE LAW REVIEW 297 (1996); Abramovsky, Extraterritorial Jurisdiction: The United States Unwarranted Attempt to Alter International Law in United States v Yunis, 15 YALE JOURNAL OF INTERNATIONAL LAW 121 (1990); Exporting United States Drug Law: An Example of the International Legal Ramifications of the "War on Drugs," 1992 BRIGHAM YOUNG UNIVERSITY LAW REVIEW 165.

[1236] Harvard Study at 480-509.

[1237] E.g., 18 U.S.C. 81 (arson within the maritime and territorial jurisdiction of the United States), 113 (assaults within the maritime and territorial jurisdiction of the United States).

[1238] Ford v. United States, 273 U.S. 593, 623 (1927)("a man who outside of a country willfully puts in motion a force to take effect in it is answerable at the place where the evil is done"); United States v. Yousef, 327 F.3d 56, 96-7 (2d Cir. 2003)("Moreover, assertion of jurisdiction is appropriate under the 'objective territorial principle' because the purpose of the attack was to influence United States foreign policy and the defendants intended their actions to have an effect – in this case, a devastating effect – on and within the United States"); United States v. Neil, 312 F.3d 419, 422 (9th Cir. 2002); United States v. MacAllister, 160 F.3d 1304, 1308 (11th Cir. 1998); United States v. Goldberg, 830 F.2d 459, 463-64 (3d Cir. 1987).

[1239] United States v. Felix-Gutierrez, 940 F.2d 1200, 1205 (9th Cir. 1991)("Felix's actions created a significant detrimental effect in the United States and adversely affected the national interest. In helping to prevent the United States from apprehending Caro-Quintero, Felix directly hindered United States efforts to prosecute an alleged murderer of a government agent. Furthermore that agent was a United States citizen. We need not decide whether any one of these facts or

If the territorial principle is more expansive than its caption might imply, the protective principle is less so. It is confined to crimes committed outside a nation's territory against its "security, territorial integrity or political independence."[1240] As construed by the courts, however, it is understood to permit the application abroad of statutes which protect the federal government and its functions.[1241] And so, it covers the overseas murder or attempted murder of federal officers or those thought to be federal officers;[1242] acts of terrorism calculated to influence American foreign policy;[1243] conduct which Congress has characterized as a threat to U.S. national security;[1244] or false statements or forgery designed to frustrate the administration of U.S. our immigration laws.[1245]

The nationality principle rests the exercise of extraterritorial criminal jurisdiction on the citizenship of accused.[1246] It is the principle mirrored in the Supreme Court's statements in Blackmer, following the contempt conviction of an American living in Paris who ignored a federal court subpoena.[1247] As in the case

---

principles, standing alone, would be sufficient. Rather, we hold that cumulatively applied they require the conclusion that giving extraterritorial effect to the accessory after the act statute in Felix's case does not violate international law principles"); United States v. Suerte, 291 F.3d 366, 370 (5th Cir. 2002); United States v. Cardales, 168 F.3d 548, 553 (1st Cir. 1999); United States v. Benitez, 741 F.2d 1312, 1316 (11th Cir. 1984).

[1240] Harvard Study at 543.

[1241] United States v. Vilches-Navarrete, 523 F.3d 1, 21-2 (1st Cir. 2008)("Under the protective principle of international law, Congress can punish crimes committed on the high seas regardless of whether a vessel is subject to the jurisdiction of the United States. Under the protective principle, a state has jurisdiction to prescribe a rule of law attaching legal consequences to conduct outside its territory that threatens its security as a state or the operation of its governmental functions, provided the conduct is generally recognized as a crime under the law of states that have reasonably developed legal systems").

[1242] United States v. Vasquez-Velasco, 15 F.3d 833, 841 (9th Cir. 1994); United States v. Felix-Gutierrez, 940 F.2d 1200, 1206 (9th Cir. 1991); United States v. Benitez, 741 F.2d 1312, 1316 (11th Cir. 1984).

[1243] United States v. Yousef, 327 F.3d 56, 97 (2d Cir. 2003) ("Finally, there is no doubt that jurisdiction is proper under the protective principle because the planned attacks were intended to affect the United States and to alter its foreign policy").

[1244] United States v. Romero-Galue, 757 F.2d 1147, 1154 (11th Cir. 1985).

[1245] United States v. Marino-Garcia, 679 F.2d 1373, 1381 fn. 14 (11th Cir. 1982) (citing cases in accord).

[1246] Harvard Study at 519; United States v. Clark, 435 F.3d 1100, 1106 (9th Cir. 2006); United States v. Martinez, 599 F.Supp.2d 784, 797 (W.D.Tex. 2009).

[1247] Blackmer v. United States, 284 U.S. 421, 437 (1932)("With respect to such exercise of authority, there is no question of international law, but solely of the purport of municipal law

of Blackmer, which evidenced both the nationality and the protective principles, cases involving the nationality principle often involve other principles as well.[1248]

The passive personality principle recognizes extraterritorial criminal jurisdiction based on the nationality of the victim of the offense.[1249] It, too, has been asserted most often in the presence of facts suggesting other principles.[1250]

The universal principle is based on the premise that offenses against all nations may be punished by any nation where the offender is found.[1251] At a minimum, it applies to piracy and offenses committed on the high seas on "stateless" vessels.[1252]

Current Extent of American Extraterritorial Criminal Jurisdiction

Federal Law

Express

Congress' declaration that a particular statute is to apply outside of the United States is the most obvious evidence of an intent to create extraterritorial jurisdiction.[1253] Congress has expressly provided for the extraterritorial application of federal criminal law most often by outlawing various forms of

---

which establishes the duties of the citizen in relation to his own government. While the legislation of the Congress, unless the contrary intent appears, is construed to apply only within the territorial jurisdiction of the United States, the question of its application so far as citizens of the United States in foreign countries are concerned is one of construction, not of legislative power").

[1248] United States v. Plummer, 221 F.3d 1298, 1305-307(11th Cir. 2000)(nationality and territorial principles); Chua Han Mow v. United States, 730 F.2d 1308, 1312 (9th Cir. 1984)(territorial, protective and nationality principles); United States v. Smith, 680 F.2d 255, 257-58 (1st Cir. 1982)(territorial and nationality principles); United States v. Martinez, 599 F.Supp.2d 784, 800 (W.D.Tex. 2009)(nationality, passive personality, and territorial principles).

[1249] Harvard Study at 445.

[1250] United States v. Yousef, 327 F.3d 56, 96 (2d Cir. 2003)(passive personality and territorial principles)("consistent with the passive personality principle of customary international jurisdiction because each of these counts involved a plot to bomb United States-flag aircraft that would have been carrying United States citizens and crews and that were destined for cities in the United States"); United States v. Hill, 279 F.3d 731, 739 (9th Cir. 2002)("In the instance case, the territorial, national, and passive personality theories combine to sanction extraterritorial jurisdiction"); United States v. Rezaq, 134 F.3d 1121, 1133 (D.C.Cir. 1998)(protective and passive personality principles).

[1251] United States v. Shi, 525 F.3d 709, 722 (9th Cir. 2008); Harvard Study at 445.

[1252] United States v. Caicedo, 47 F.3d 370, 372 (9th Cir. 1995).

[1253] A list of the citations to such federal statutes is attached.

misconduct when they occur "within the special maritime and territorial jurisdiction of the United States."[1254] The concept of special maritime and territorial jurisdiction, if not the phrase, dates from the First Congress,[1255] and encompasses navigable waters and federal enclaves within the United States as well as areas beyond the territorial confines of the United States. Although the concept of the special maritime and territorial jurisdiction of the United States once embraced little more than places over which the United States enjoyed state-like legislative jurisdiction, U.S. navigable territorial waters, and vessels of the United States, its application has been statutorily expanded. It now supplies an explicit basis for the extraterritorial application of various federal criminal laws relating to:

- air travel (special aircraft jurisdiction of the United States);[1256]
- customs matters (customs waters of the U.S.);[1257]

[1254] The text of 18 U.S.C. 7 which defines the term "special maritime and territorial jurisdiction of the United States" is attached.

[1255] 1 Stat. 113 (1790)(outlawing manslaughter committed in a place "under the sole and exclusive jurisdiction of the United States" and murder committed "upon the high seas").

[1256] "In this chapter –

"(1) 'aircraft in flight' means an aircraft from the moment all external doors are closed following boarding—(A) through the moment when one external door is opened to allow passengers to leave the aircraft; or (B) until, if a forced landing, competent authorities take over responsibility for the aircraft and individuals and property on the aircraft.

"(2) 'special aircraft jurisdiction of the United States' includes any of the following aircraft in flight: (A) a civil aircraft of the United States. (B) an aircraft of the armed forces of the United States. (C) another aircraft in the United States. (D) another aircraft outside the United States—(i) that has its next scheduled destination or last place of departure in the United States, if the aircraft next lands in the United States; (ii) on which an individual commits an offense (as defined in the Convention for the Suppression of Unlawful Seizure of Aircraft) if the aircraft lands in the United States with the individual still on the aircraft; or (iii) against which an individual commits an offense (as defined in subsection (d) or (e) of article I, section I of the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation) if the aircraft lands in the United States with the individual still on the aircraft. (E) any other aircraft leased without crew to a lessee whose principal place of business is in the United States or, if the lessee does not have a principal place of business, whose permanent residence is in the United States.

"(3) an individual commits an offense (as defined in the Convention for the Suppression of Unlawful Seizure of Aircraft) when the individual, when on an aircraft in flight—(A) by any form of intimidation, unlawfully seizes, exercises control of, or attempts to seize or exercise control of, the aircraft; or (B) is an accomplice of an individual referred to in subclause (A) of this clause," 49 U.S.C. 46501.

[1257] "The term 'customs waters' means, [1] in the case of a foreign vessel subject to a treaty or other arrangement between a foreign government and the United States enabling or permitting the authorities of the United States to board, examine, search, seize, or otherwise to enforce upon such vessel upon the high seas the laws of the United States, the waters within such distance of

- U.S. spacecraft in flight; [1258]
- overseas federal facilities and overseas residences of federal employees;[1259]
- members of U.S. armed forces overseas and those accompanying them;[1260]
- overseas human trafficking and sex offenses by federal employees, U.S. military personnel, or those accompanying them.[1261]

---

the coast of the United States as the said authorities are or may be so enabled or permitted by such treaty or arrangement and, [2] in the case of every other vessel, the waters within four leagues of the coast of the United States," 19 U.S.C. 1709(c).

[1258] 18 U.S.C. 7(6)("Any vehicle used or designed for flight or navigation in space and on the registry of the United States pursuant to the Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies and the Convention on Registration of Objects Launched into Outer Space, while that vehicle is in flight, which is from the moment when all external doors are closed on Earth following embarkation until the moment when one such door is opened on Earth for disembarkation or in the case of a forced landing, until the competent authorities take over the responsibility for the vehicle and for persons and property aboard").

[1259] "With respect to offenses committed by or against a national of the United States as that term is used in section 101 of the Immigration and Nationality Act – (A) the premises of United States diplomatic, consular, military or other United States Government missions or entities in foreign States, including the buildings, parts of buildings, and land appurtenant or ancillary thereto or used for purposes of those missions or entities, irrespective of ownership; and (B) residences in foreign States and the land appurtenant or ancillary thereto, irrespective of ownership, used for purposes of those missions or entities or used by United States personnel assigned to those missions or entities," 18 U.S.C. 7(9).

[1260] "(a) Whoever engages in conduct outside the United States that would constitute an offense punishable by imprisonment for more than 1 year if the conduct had been engaged in within the special maritime and territorial jurisdiction of the United States – (1) while employed by or accompanying the Armed Forces outside the United States; or (2) while a member of the Armed Forces subject to chapter 47 of title 10 (the Uniform Code of Military Justice), shall be punished as provided for that offense.

"(b) No prosecution may be commenced against a person under this section if a foreign government, in accordance with jurisdiction recognized by the United States, has prosecuted or is prosecuting such person for the conduct constituting such offense, except upon the approval of the Attorney General or the Deputy Attorney General (or a person acting in either such capacity), which function of approval may not be delegated.

"(c) Nothing in this chapter may be construed to deprive a court-martial, military commission, provost court, or other military tribunal of concurrent jurisdiction with respect to offenders or offenses that by statute or by the law of war may be tried by a court-martial, military commission, provost court, or other military tribunal.

"(d) No prosecution may be commenced against a member of the Armed Forces subject to chapter 47 of title 10 (the Uniform Code of Military Justice) under this section unless – (1) such member ceases to be subject to such chapter; or

(2) an indictment or information charges that the member committed the offense with one or more other defendants, at least one of whom is not subject to such chapter," 18 U.S.C. 3261.

The obligations and principles of various international treaties, conventions, or agreements to which the United States is a party supply the theme for a second category of federal criminal statutes with explicit extraterritorial application.[1262] The range of these treaty-based federal crimes differs. Some have extraterritorial application only when the offender is an American.[1263] Some address misconduct so universally condemned that they fall within federal jurisdiction regardless of any other jurisdictional considerations as long as the offender flees to the United States, is brought here for prosecution, or is otherwise "found in the United States" after the commission of the offense.[1264] Some enjoy extraterritorial application under any of a number of these and other explicit jurisdictional circumstances.[1265]

Members of a final category of explicit extraterritorial federal criminal statutes either cryptically declare that their provisions are to apply overseas[1266] or describe a series of jurisdictional circumstances under which their provisions

---

[1261] "(a) Whoever, while employed by or accompanying the Federal Government outside the United States, engages in conduct outside the United States that would constitute an offense under chapter 77 [relating to peonage, slavery and trafficking] or 117 [relating to transportation for illegal sexual activity] of this title if the conduct had been engaged in within the United States or within the special maritime and territorial jurisdiction of the United States shall be punished as provided for that offense.

"(b) No prosecution may be commenced against a person under this section if a foreign government, in accordance with jurisdiction recognized by the United States, has prosecuted or is prosecuting such person for the conduct constituting such offense, except upon the approval of the Attorney General or the Deputy Attorney General (or a person acting in either such capacity), which function of approval may not be delegated," 18 U.S.C. 3271.

[1262] E.g., 18 U.S.C. 1203 (hostage taking); 18 U.S.C. 175 (biological weapons); 18 U.S.C. 1091 (genocide); 18 U.S.C. ch.113C (torture).

[1263] E.g.,18 U.S.C. 1091(d)(2)("the alleged offender is a national of the United States. . .").

[1264] E.g., 18 U.S.C. 2340A(b)(2)("There is jurisdiction over the activity prohibited in subsection(a) if . . .(2) the alleged offender is present in the United States, irrespective of the nationality of the victim or alleged offender").

[1265] E.g., 18 U.S.C. 1203 (It is not an offense under this section [relating to hostage taking] if the conduct required for the offense occurred outside the United States unless – (A) the offender or the person seized or detained is a national of the United States; (B) the offender is found in the United States; or (C) the governmental organization sought to be compelled is the Government of the United States").

[1266] E.g., 18 U.S.C. 351(i)(relating to crimes of violence committed against Members of Congress, Supreme Court justices, and certain senior executive officials) ("There is extraterritorial jurisdiction over the conduct prohibited by this section").

have extraterritorial application, not infrequently involving the foreign commerce of the United States in conjunction with other factors.[1267]

Implied

The natural implications of Bowman[1268] and Ford[1269] are that a substantial number of other federal crimes operate overseas by virtue of the implicit intent of Congress. In fact, the lower federal courts have read Bowman and Ford to suggest that American extraterritorial criminal jurisdiction includes a wide range of statutes designed to protect federal officers, employees and property, to prevent smuggling and to deter the obstruction or corruption of the overseas activities of federal departments and agencies.[1270] They have held, for instance, that the statute outlawing the assassination of Members of Congress may be applied against an American for a murder committed in a foreign country,[1271] and that statutes prohibiting the murder or kidnaping of federal law enforcement officials apply in other countries even if the offenders are not Americans,[1272] and even if the offenders incorrectly believed the victims were federal law enforcement officers.[1273] They have also considered extraterritorial jurisdiction appropriate to (1) cases where aliens have attempted to defraud the United States in order to

---

[1267] E.g., 18 U.S.C. 175c (variola virus)(committed by or against a U.S. national; committed in or affecting interstate or foreign commerce; committed against federal property).

[1268] United States v. Bowman, 260 U.S. 94 (1922)(the nature and purpose of a statute indicate whether Congress intended it to apply outside of the United States).

[1269] Ford v. United States, 273 U.S. 593, 623 (1927)("a man who outside of a country willfully puts in motion a force to take effect in it is answerable at the place where the evil is done").

[1270] United States v. MacAllister, 160 F.3d 1304, 1308 n.8 (11th Cir. 1998)("On authority of Bowman, courts have routinely inferred congressional intent to provide for extraterritorial jurisdiction over foreign offenses that cause domestic harm").

[1271] United States v. Layton, 855 F.2d 1388, 1395-397 (9th Cir. 1988) (At the time of the murder of Congressman Ryan for which Layton was convicted the statute was silent as to its extraterritorial application; several years later Congress added an explicit extraterritorial provision, 18 U.S.C. 351(i)).

[1272] United States v. Felix-Guiterrez, 940 F.2d 1200, 1204-206 (9th Cir. 1991); United States v. Benitez, 741 F.2d 1312, 1316-317 (11th Cir. 1984).

Attached is a list of citations to statutes that condemn acts of violence against officers and officials of the United States, that contain no express provisions concerning their geographical application but that apply overseas, if the same logic evidenced in the cases noted above is followed.

[1273] United States v. Vasquez-Velasco, 15 F.3d 833, 839 (9th Cir. 1994).

gain admission into the United States;[1274] (2) false statements made by Americans overseas;[1275] (3) the theft of federal property by Americans abroad;[1276] and (4) counterfeiting, forging or otherwise misusing federal documents or checks overseas by either Americans or aliens.[1277]

A logical extension would be to conclude that statutes enacted to prevent and punish the theft of federal property apply world-wide. And there seems to be no obvious reason why statutes protecting the United States from intentional deprivation of its property by destruction should be treated differently than those where the loss is attributable to theft.[1278]

Finally, there are the "piggyback statutes" whose provisions are necessarily related to some other crime. An individual may be guilty of conspiracy to violate a federal law within the United States notwithstanding the fact he never enters the United States; it is sufficient that he is a member of a conspiracy to violate the American law.[1279] The rationale should apply with equal force to the case of any accessory to the violation of any federal crime.[1280] Nevertheless, a few recent statutes make the coverage of piggyback offenses explicit.[1281]

[1274] United States v. Pizzarusso, 388 F.2d 8, 9-10 (2d Cir. 1968); Rocha v. United States, 288 F.2d 545, 549 (9th Cir. 1961); United States v. Khale, 658 F.2d 90, 92 (2d Cir. 1981); United States v. Castillo-Felix, 539 F.2d 9, 12-3 (9th Cir. 1976).

[1275] United States v. Walczak, 783 F.2d 852, 854-55 (9th Cir. 1986).

[1276] United States v. Cotten, 471 F.2d. 744, 749 (9th Cir. 1973).

[1277] United States v. Birch, 470 F.2d 808, 810-11 (4th Cir. 1972); United States v. Fernandez, 496 F.2d 1294, 1296 (5th Cir. 1954); United States v. Aguilar, 756 F.2d 1418, 1425 (9th Cir. 1985); United States v. Castillo-Felix, 539 F.2d 9, 12-3 (9th Cir. 1976).

[1278] Attached are lists of the citations to the theft of federal property statutes, the destruction of federal property statutes, the federal false statement statutes, and the federal counterfeiting statutes.

[1279] United States v. MacAllister, 160 F.3d 1304, 1307-308 (11th Cir. 1998); Ford v. United States, 273 U.S. 593, 620-24 (1927); United States v. Inco Bank & Trust Corp., 845 F.2d 919, 920 (11th Cir. 1988); United States v. Manuel, 371 F.Supp.2d 404, 409 (S.D.N.Y. 2005).

[1280] United States v. Felix-Gutierrez, 940 F.2d 1200, 1204-207 (9th Cir. 1991)(accessory after the fact violation committed overseas). A list of citations to the piggyback offense statutes is attached.

[1281] E.g., 18 U.S.C. 2339D(b)(6) (relating to receipt of military training from a foreign terrorist organization)("(b) Extraterritorial jurisdiction – there is extraterritorial federal jurisdiction over an offense under this section. There is jurisdiction over an offense under subsection (a) if . . . (6) an offender aids or abets any person over whom jurisdiction exists under this paragraph in committing an offense under subsection (a) or conspires with any person over whom jurisdiction exist under this paragraph to commit an offense under subjection (a)").

A number of statutes condemn both a substantive offense and the piggy-back crimes (conspiracy or attempt) associated with the substantive offense. A statute which applies overseas carries with it the application of provisions which prohibit attempts or conspiracies to violate the underlying statute.[1282]

Maritime Drug Law Enforcement Act

The Maritime Drug Law Enforcement Act (MDLEA) is somewhat unusual in that it expressly authorizes extraterritorial coverage of federal criminal law predicated on nothing more than the consent of the nation with primary criminal jurisdiction.[1283] MDLEA outlaws the manufacture, distribution, or possession with intent to manufacture or distribute controlled substances aboard vessels within the jurisdiction of the United States.[1284] It defines vessels within the jurisdiction of the United States not only in terms of ordinary U.S. maritime jurisdiction, but envelops the maritime jurisdiction of other countries as long as they have consented to the application of the U.S. law aboard the vessel.[1285] The definition also encompasses "vessels without nationality" sometimes referred to as "stateless" vessels, that is, vessels for which no national registry is effectively claimed.[1286]

[1282] United States v. Davis, 905 F.2d 245, 249 (9th Cir. 1990); United States v. Villanueva, 408 F.3d 193, 197-99 (5th Cir. 2005).

[1283] 46 U.S.C. 70501-70507.

[1284] 46 U.S.C. 70503.

[1285] "In this chapter, the term 'vessel subject to the jurisdiction of the United States' includes – (A) a vessel without nationality; (B) a vessel assimilated to a vessel without nationality, in accordance with paragraph (2) of article 6 of the 1958 Convention on the High Seas; (C) a vessel registered in a foreign nation where the flag nation has consented or waived objection to the enforcement of United States law by the United States; (D) a vessel located within the customs waters of the United States; (E) a vessel located in the territorial waters of another nation, where the nation consents to the enforcement of United States law by the United States; and (F) a vessel located in the contiguous zone of the United States, as defined in Presidential Proclamation 7219 of September 2, 1999, and (i) is entering the United States, (ii) has departed the United States, or (iii) is a hovering vessel as defined in section 491 of the Tariff Act of 1930 (19 U.S.C. 1401)," 46 U.S.C. 70502(c)(1).

[1286] "In this chapter, the term, "vessel without nationality" includes – (A) a vessel aboard which the master or person in charge makes a claim of registry, which claim is denied by the flag nation whose registry is claimed; (B) any vessel aboard which the master or person in charge fails, upon request of an officer of the United States empowered to enforce applicable provisions of United States law, to make a claim of nationality or registry for that vessel; and (C) a vessel aboard which the master or person in charge makes a claim of registry and the claimed nation of registry does not affirmatively and unequivocally assert that the vessel is of its nationality," 46 U.S.C. 70502(d)(1).

MDLEA provides the basis for Coast Guard drug interdiction efforts in the Caribbean and in the eastern Pacific off the coast of Central and South America.[1287] The courts have concluded that MDLEA constitutes a valid exercise of Congress' constitutional authority to define and punish offenses against the law of nations, U.S. Const. Art.I, §8, cl.10.[1288] They are divided over whether the prosecution must show some nexus between the United States and the offense[1289] and over the application of the subsection of the Act that assigns jurisdictional determinations to the court rather than to the jury, 46 U.S.C. 70504(a).[1290]

State Law

State criminal laws are less likely to apply overseas than federal laws.[1291] State law produces fewer instances where a statute was clearly enacted with an eye to its application overseas and fewer examples where frustration of legislative purpose is the logical consequence of purely territorial application. The Constitution seems to have preordained this result when it vested responsibility for protecting

---

[1287] E.g., United States v. Olave-Valencia, 371 F.Supp.2d 1224, 1226 (S.D. Cal. 2005)(Coast Guard interdiction 250 miles from the Honduras/Costa Rica border); United States v. Valencia-Aguirre, 409 F.Supp.2d 1358, 1360 (M.D.Fla. 2006)(Coast Guard interdiction from a Navy frigate off the Coast of Colombia); United States v. Perlaza, 439 F.3d 1149, 1152 (9th Cir. 2006) (Navy and Coast Guard ships engaged in drug interdiction in Pacific off the coasts of Ecuador, Colombia and Peru).

[1288] United States v. Ledesma-Cuesta, 347 F.3d 527, 532 (3d Cir. 2003); United States v. Moreno-Morillo, 334 F.3d 819, 824 (9th Cir. 2003).

[1289] United States v. Suerte, 291 F.3d 366, 375 (5th Cir. 2002); United States v. Cardales, 168 F.3d 548, 552-53 (1st Cir. 1999); United States v. Perez Oviedo, 281 F.3d 400, 402-3 (3d Cir. 2002); contra, United States v. Klimavicius-Viloria, 144 F.3d 1249, 1257 (9th Cir. 1998).

[1290] United States v. Perlaza, 439 F.3d 1149, 1165-166 (9th Cir. 2006)("After hearing all the evidence as to its status at a pretrial hearing, the district court determined that the Go-Fast was a stateless vessel. We find that by not submitting this issue to the jury, the district court erred. The evidence relating to the Go-Fast's statelessness presents precisely the kind of disputed factual question that Smith [United States v. Smith, 282 F.3d 758 (9th Cir. 2002)] requires a jury to resolve"); contra, United States v. Tinoco, 304 F.3d 1088, 1110-111 and n.22 (11th Cir. 2002)("Hence, although fact-bound determinations may be involved, that does not automatically mean that the 46 U.S.C.App. 1903 jurisdictional issue has to be decided by the jury. . . Consequently, even if questions under the 46 U.S.C.App. 1903 jurisdictional requirement may have a factual component, that component does not have to be resolved by the jury, given that, as we have explained, the jurisdictional requirement goes only to the court's subject matter jurisdiction and does not have to be treated as an element of a MDLEA substantive offense. . . We also note that our rejection of the appellant's argument concerning the fact-bound nature of 46 U.S.C.App. 1903 jurisdictional determinations appears to put us in conflict with one of our sister circuits. . . In United States v. Smith . . . [t]he Ninth Circuit concluded that the district court erred by taking the issue of whether the §1903 jurisdictional requirement had been met completely away from the jury").

[1291] The comparable question under state law is the extent to which a state's criminal law applies to activities occurring in another state.

American interests and fulfilling American responsibilities overseas in the federal government.[1292]

The primacy of the federal government in foreign affairs might suggest that the Constitution precludes the application of state law in other countries, but courts and commentators have recognized a limited power of the states to enact law governing conduct outside the United States.[1293] Obviously, Congress may, by preemptive action, extinguish the legislative authority of a state in any area over which Congress has plenary powers. And the Supremacy Clause also renders treaties to which the United States is a party binding upon the states and therefore beyond their legislative reach.[1294] Beyond the constitutional limitations, however, "the question . . . is one of whether the state actually intended to legislate extraterritorially, not whether it has the power to do so."[1295]

[1292] See e.g., U.S. Const. Art.II, §2, cl.2 ("[t]he President . . . shall have power, by and with the advice and consent of the Senate, to make treaties, provided two thirds of the Senators present concur; and he shall nominate, and by and with the advice and consent of the Senate, shall appoint Ambassadors, [and] other public ministers and consuls . . . ."); U.S. Const. Art.II, §3, cl.3 (". . . he shall receive Ambassadors and other public ministers. . . ."); U.S. Const. Art.II, §2, cl.1 ("[he] shall be commander in chief of the Army and Navy of the United States . . . ."); U.S. Const. Art.I, §8, cl.18 ("[t]he Congress shall have power . . . to make all laws which shall be necessary and proper for carrying into execution [its] powers, and all other powers vested by this Constitution in the Government of the United States, or in any Department or Officer thereof"); U.S. Const. Art.I, §8, cl.10 ("[t]he Congress shall have power . . . to define and punish piracies and felonies committed on the high seas, and offences against the law of nations"); U.S. Const. Art.I, §8, cl.3 ("[t]he Congress shall have power . . . to regulate commerce with foreign nations . . . ."); U.S. Const. Art.I, §8, cl.1 ("[t]he Congress shall have power to lay and collect . . . duties, imposts and excises, to pay the debts and provide for the common defence and general welfare . . . ."); U.S. Const. Art.I, §8, cls.11, 12, 13, 14 ("[t]he Congress shall have power . . . to declare war. . . ; to raise and support armies . . . ; to provide and maintain a navy . . . ; [and] to make rules for the government and regulation of the land and naval forces. . . .").

[1293] Skiriotes v. Florida, 313 U.S. 69, 77 (1941)("If the United States may control the conduct of its citizens upon the high seas, we see no reason why the State of Florida may not likewise govern the conduct of its citizens upon the high seas with respect to matters in which the State has a legitimate interest and where there is no conflict with acts of Congress"); State v. Flores, 218 Ariz. 407, 413-16, 188 P.3d 706, 712-15 (Ariz.App. 2009); State v. Jack, 125 P.3d 311, 318-19 (Alaska 2005); Colangelo, Constitutional Limits on Extraterritorial Jurisdiction: Terrorism and the Intersection of National and International Law, 48 HARVARD INTERNATIONAL LAW JOURNAL 121, 128 (2007).

[1294] "This Constitution, and the Laws of the United States which shall be made in pursuance thereof; and all treaties made, or which shall be made, under the authority of the United States, shall be the supreme law of the land; and the judges in every state shall be bound thereby; any thing in the constitution or laws of any state to the contrary notwithstanding," U.S. Const. Art.VI, cl.2.

[1295] George, Extraterritorial Application of Penal Legislation, 64 MICHIGAN LAW REVIEW 609, 617 (1966); RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW §402 comment k, n.5 (1987).

The states have chosen to make their laws applicable beyond their boundaries in only a limited set of circumstances and ordinarily only in cases where there is some clear nexus to the state.[1296] Perhaps the most common state statutory provision claiming state extraterritorial criminal jurisdiction is one which asserts jurisdiction in cases where some of the elements of the offense are committed within the state or others are committed outside it.[1297] Another common claim is where an individual outside the state attempts or conspires to commit a crime within the state;[1298] or one within the state attempts or conspires to commit a crime beyond its boundaries.[1299] Still others define the state's extraterritorial

---

[1296] The Model Penal Code section (attached) exemplifies the standards found in most state extraterritorial criminal jurisdiction provisions. Several states have no general extraterritorial statute, but instead have statutory venue provisions indicating where criminal offenses with extraterritorial components may be tried, e.g., Ala.Code §15-2-3 ("When the commission of an offense commenced in the State of Alabama is consummated without the boundaries of the state, the offender is liable to punishment therefor in Alabama; and venue in such case is in the county in which the offense was commenced, unless otherwise provided by law").

[1297] *Ala.Code §§15-2-3, 15-2-4; *Alaska Stat. §12.05.010; Ariz.Rev.Stat.Ann. §13-108(A)(1); Ark.Code Ann. §5-1104(a)(1); Cal.Penal Code §27(a)(1); Colo.Rev. Stat. §18-1-201(1)(a); Del.Code tit.11 §204(a)(1); Fla.Stat.Ann. §910.005(1)(a); Ga.Code §17-2-1(b)(1); Hawaii Rev.Stat. §701-106(1)(a); Idaho Code §18-202(1); Ill.Comp.Stat.Ann. ch.720, §5/1-5(a)(1); Ind. Code Ann. §35-41-1-1(b)(1); Iowa Code Ann. §803.1(1)(a); Kan.Stat.Ann. §21-3104; Ky.Rev.Stat. §500.060(1)(a); La.Code Crim.Pro. art. 611; Me.Rev.Stat.Ann. tit.17-A §7(1)(A); Minn.Stat.Ann. §609.025(1); *Miss.Code §§99-11-15, 99-11-17; Mo.Ann. Stat. §541.191(1)(1); Mont.Code Ann. §46-2-101; *Nev.Rev. Stat. §§170. 015, 170.020; N.H. Rev.Stat.Ann. §625:4(I)(a); N.J.Stat.Ann. §2C:1-3(a)(1); N.Y.Crim. Pro.Law §20.20(1)(a); *N.C.Gen.Stat. §15A-134; *N.D.Cent.Code §29-03-01; Ohio Rev.Code §2901.11(A)(1); Okla. Stat.Ann. tit.21 §151(1); Ore.Rev.Stat. §131.215(1); Pa.Stat.Ann. tit. 18 §102(a)(1); *S.D.Codified Laws §23A-16-2; *Tenn.Code Ann. §39-11-103(b); Tex. Penal Code §1.04 (a)(1); Utah Code Ann. §76-1-201(1)(a); Vt.Stat.Ann. tit.13 §2; Wash.Rev. Code Ann. §9A.04.030; Wis.Stat.Ann. §939.03 (1)(a).*Statutes which phrase the extraterritorial jurisdiction statement in terms of offenses commenced in one state and consummated in another state, rather than in terms of elements.

[1298] Ariz.Rev.Stat.Ann. §13-108(A)(2)(attempt and conspiracy); Ark.Code Ann.§5-1-104(a)(2),(3)(attempt and conspiracy); Colo. Rev.Stat. §18-1-201(1)(b),(c)(attempt and conspiracy); Del.Code tit.11 §204(a)(2)(conspiracy); Fla.Stat.Ann. §910.005 (1)(b),(c) (attempt and conspiracy); Ga.Code §17-2-1(b)(2)(attempt); Hawaii Rev.Stat. §701106(1)(b),(c)(attempt and conspiracy); Ill.Comp.Stat.Ann. ch.720 §5/1-5(a)(2),(3) (attempt and conspiracy); Ind.Code Ann. §35-41-1-1(b)(2),(3)(attempt and conspiracy); Iowa Code Ann. §803.1(1)(b),(c)(attempt and conspiracy); Kan.Stat.Ann. §21-3104(1)(b),(c) (attempt and conspiracy); Ky.Rev.Stat. §500.060(1)(b),(c) (attempt and conspiracy); Me.Rev.Stat. Ann. tit.17-A, §7(1)(B), (C) (attempt and conspiracy); Mo.Ann.Stat. §541.191(1)(2) (attempt and conspiracy); Mont.Code Ann. §46-2-101(b)(attempt); N.H.Rev.Stat.Ann. §625:4(I)(b), (c) (attempt and conspiracy); N.J.Stat.Ann. §2C:1-3(a)(2),(3) (attempt and conspiracy); Ohio Rev.Code §2901.11 (A)(3) (attempt and conspiracy); Ore.Rev.Stat. §131.215(2), (3) (attempt and conspiracy); Pa. Stat.Ann. tit.18 §102(a)(2), (3) (attempt and conspiracy); Tex.Penal Code §1.04(a)(2), (3) (attempt and conspiracy); Utah Code Ann. §76-1-201(1)(b), (c) (attempt and conspiracy); Wis.Stat.Ann. §939.03(1)(b)(conspiracy).

[1299] Ariz.Rev.Stat.Ann. §13-108(A)(3)(attempt and conspiracy); Ark.Code Ann.§5-1-104 (a)(4)(attempt and conspiracy); Colo. Rev.Stat. §18-1-201(1)(d)(attempt and conspiracy);

jurisdiction to include instances where the victim of homicide, fatally wounded outside of the state, dies within it;[1300] where property stolen elsewhere is brought into the state;[1301] or where conduct outside the state constitutes the failure to comply with a legal duty imposed by state law.[1302]

Investigation and Prosecution

Although a substantial number of federal criminal statutes have undisputed extraterritorial scope and a great many more have apparent extraterritorial range, prosecutions are few. Investigators and prosecutors face legal, practical, and often diplomatic obstacles that can be daunting. Some of these are depicted in the description that follows of some of procedural aspects of the American investigation and prosecution of a crime committed abroad.

With respect to diplomatic concerns, the Restatement observes:

Del.Code tit.11 §204(a)(3)(attempt and conspiracy); Fla.Stat.Ann. §910.005 (1)(d)(attempt and conspiracy); Ga.Code §17-2-1(b)(3)(attempt); Hawaii Rev.Stat. §701-106(1)(d) (attempt and conspiracy); Ill.Comp.Stat.Ann. ch.720 §5/1-5(1)(d)(attempt and conspiracy); Ind.Code Ann. §35-41-1-1(b)(4)(attempt and conspiracy); Iowa Code Ann. §803.1(1)(e) (attempt and conspiracy); Ky.Rev.Stat. §500.060(1)(d)(attempt and conspiracy); Me.Rev.Stat.Ann. tit.17-A, §7(1)(D) (attempt and conspiracy); Mo.Ann.Stat. §541.191(1)(3)(attempt and conspiracy); Mont.Code Ann. §46-2-101(c)(attempt and conspiracy); N.H.Rev. Stat.Ann. §625:4(I) (c); N.J.Stat.Ann. §2C:1-3(a)(4) (attempt and conspiracy); Ohio Rev.Code §2901.11(A)(2) (attempt and conspiracy); Ore.Rev.Stat. §131.215(4) (attempt and conspiracy); Pa. Stat.Ann. tit.18 §102(a)(4)(attempt and conspiracy); R.I.Gen.Laws §11-1-7 (conspiracy); Tex.Penal Code §1.04(a) (3); Utah Code Ann. §76-1201(1)(d)(attempt and conspiracy).

[1300] Ariz.Rev.Stat.Ann. §13-108(B); Ark.Code Ann. §5-1-104(b); Colo.Rev.Stat. §18-1-201(2); Del.Code tit.11 §204(c); Fla.Stat.Ann. §910.005(2); Ga.Code §17-2-1(c); Hawaii Rev.Stat. §701-106(4); Ill.Comp.Stat.Ann. ch.720 §5/1-5(b); Ind.Code Ann. §35-41-1-1(c); Iowa Code Ann. §803.1(2); Kan.Stat.Ann. §21-3104(2); Ky.Rev.Stat. §500.060(3); La.Code Crim.Pro. art. 611; Me. Rev.Stat.Ann. tit.17-A §7(3); Miss.Code §99-11-21; Mo. Ann.Stat. §541.191(2); Mont.Code Ann. §46-2-101(2); N.H.Rev.Stat.Ann. §625:4 (III); N.J.Stat. Ann.§2C:1-3(d); N.Y.Crim. Pro.Law §20.20(2)(a); Ohio Rev.Code §2901.11 (B); Ore.Rev. Stat. §131.235; Pa.Stat. Ann. tit.18 §102(c); Tex.Penal Code §1.04(b); Utah Code Ann. §76-1-201(3).

[1301] Ala.Code §15-2-5; Cal.Penal Code §27(a)(2); Idaho Code §18-202(2); Miss.Code §99-11-23; N.D.Cent.Code. §2903-01.1; Ohio Rev.Code §2901.11(A)(5); Okla.Stat.Ann. tit.21 §151(2); R.I.Gen.Laws §12-3-7; Wash.Rev.Code Ann. §9A.04.030(2); Wis.Stat.Ann. §939.03(1)(d).

[1302] Ariz.Rev.Stat.Ann. §13-108(A)(4); Ark.Code Ann. §5-1-104(a)(5); Colo. Rev.Stat. §18-1-201(3); Del.Code tit.11 §204(4); Fla.Stat.Ann. §910.005(3); Ga. Code §17-2-1(d); Hawaii Rev.Stat. §701-106(1)(e); Ill.Comp.Stat.Ann. ch.720 §5/1-5(c); Ind. Code Ann. §35-41-1-1(b)(5); Iowa Code Ann. §803.1(3); Kan.Stat.Ann. §21-3104 (3); Ky.Rev.Stat. §500.060(1) (e); Me.Rev.Stat.Ann. tit.17-A §7(1)(E); Mo.Ann.Stat. §541.191(1)(4); Mont.Code Ann. §46-2-101(3); N.H.Rev.Stat.Ann. §625:4(I) (e); N.J.Stat.Ann. §2C:1-3(a)(5); Ohio Rev. Code §2901.11(A)(4); Ore.Rev.Stat. §131.215(5); Pa.Stat.Ann. tit.18 §102(a)(5); Tex.Penal Code §1.04(c); Utah Code Ann. §76-1-201(4).

> *It is universally recognized, as a corollary of state sovereignty, that officials of one state may not exercise their functions in the territory of another state without the latter's consent. Thus, while a state may take certain measures of nonjudicial enforcement against a person in another state, . . . its law enforcement officers cannot arrest him in another state, and can engage in criminal investigation in that state only with that state's consent. RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW §432 cmt. b (1986).*

Failure to comply can result in strong diplomatic protests, liability for reparations, and other remedial repercussions, to say nothing of the possible criminal prosecution of offending foreign investigators.[1303] Consequently, investigations within another country of extraterritorial federal crimes without the consent or at least acquiescence of the host country are extremely rare.

Mutual Legal Assistance Treaties and Agreements

Congress has endorsed diplomatic efforts to increase multinational cooperative law enforcement activities. The United States has over fifty mutual legal assistance treaties in force.[1304] Their benefits are typically available to state and federal law enforcement investigators though the Department of Justice's Office of International Affairs.[1305] Initially negotiated to overcome impediments posed

---

[1303] RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW §432 cmt. c and rptrs.' n.1 (1986) ("In a case that received wide attention, two French customs officials traveled to Switzerland on several occasions in 1980 to interrogate a former official of a Swiss bank, with a view to gaining information about French citizens believed to be hiding funds from the French tax and exchange control authorities. The person interrogated informed the Swiss federal prosecutor's office, which caused the Swiss police to arrest the French officials on their next visit. The officials were convicted of committing prohibited acts in favor of a foreign state, as well as of violation of the Swiss banking and economic intelligence laws. Even though the two French defendants were engaged in official business on behalf of the government of a friendly foreign state, they were given substantial sentences").

[1304] See generally, Abbell, OBTAINING EVIDENCE ABROAD IN CRIMINAL CASES, ch.4 (2004 & 2008 Supp.). Jurisdictions with whom the United States has a bilateral mutual legal assistance treaty in force include Antigua and Barbuda, Argentina, Australia, Austria, Bahamas, Barbados, Belize, Belgium, Brazil, Canada, China, Cyprus, the Czech Republic, Dominica, Egypt, Estonia, France, Greece, Grenada, Hong Kong, Hungary, Israel, Italy, India, Jamaica, Japan, Korea, Latvia, Liechtenstein, Lithuania, Luxembourg, Mexico, Morocco, the Netherlands, Nigeria, Panama, the Philippines, Poland, Romania, Russia, St. Kitts & Nevis, St. Lucia, St. Vincent & the Grenadines, South Africa, Spain, Switzerland, Thailand, Trinidad and Tobago, Turkey, the United Kingdom, the Cayman Islands, Anguilla, the British Virgin Islands, Montserrat, the Turks and Caicos Islands, Ukraine, Uruguay, and Venezuela, United States Department of State, TREATIES IN FORCE. (Jan. 1, 2009).

[1305] 28 C.F.R. §0.64-1; Treaty on Mutual Legal Assistance in Criminal Matters, U.S.-Egypt, Arts. 1(3), S.Treaty Doc. 106-19 ("Assistance shall be provided in connection with any conduct that is the subject of the investigation, prosecution, or proceeding under the laws of the Requesting

by foreign bank secrecy laws,[1306] the treaties generally offer more than the collection and delivery of documents. They ordinarily provide similar clauses, with some variations, for locating and identifying persons and items;[1307] service of process;[1308] executing search warrants;[1309] taking witness depositions;[1310]

State"); Treaty on Mutual Legal Assistance in Criminal Matters, U.S.-Greece, Arts. 1(3), S.Treaty Doc. 106-18; Treaty on Mutual Legal Assistance in Criminal Matters, U.S.Cyprus, Arts. 1(3), S.Treaty Doc. 106-20; Treaty on Mutual Legal Assistance in Criminal Matters, U.S.-Cyprus, Arts. 1(3),S.Treaty Doc. 106-35; Treaty on Mutual Legal Assistance in Criminal Matters, U.S.-S.Afr., Arts. 1(3), S.Treaty Doc. 106-36. Under a few agreements, treaty benefits may not be available during preliminary investigations or for want of dual criminality, e.g., Treaty on Mutual Legal Assistance in Criminal Matters, U.S.-Fr., Art. 1, S.Treaty Doc. 106-7 (". . . mutual assistance in investigations and proceedings in respect of criminal offenses the punishment of which, at the time of the request for assistance, is a matter for the judicial authorities of the Requesting State"); Treaty on Mutual Legal Assistance in Criminal Matters, U.S.-Liech., Arts. 1, S.Treaty Doc. 107-16 ("Assistance shall be provided without regard to whether the conduct that is the subject of the investigation, prosecution, or proceeding in the Requesting State would constitute an offense under the laws of the Requested State, except that the Requested State may refuse to comply in whole or in part with a request for assistance to the extent that the conduct would not constitute an offense under its laws and the execution of the request would require a court order for search and seizure or other coercive measures").

[1306] Ellis & Pisani, The United States Treaties on Mutual Assistance in Criminal Matters: A Comparative Analysis, 19 INTERNATIONAL LAWYER 189, 196-98 (1985); Nadelmann, Negotiations in Criminal Law Assistance Treaties, 33 AMERICAN JOURNAL OF COMPARATIVE LAW 467, 470-74 (1985).

[1307] E.g., Treaty on Mutual Legal Assistance in Criminal Matters, U.S.-Liech., Art. 13, S. Treaty Doc. 106-16 ("If the Requesting State seeks the location or identity of persons or items in the Requested State, the Requested State shall use its best efforts to ascertain the location or identity"); Treaty on Mutual Legal Assistance in Criminal Matters, U.S.Greece, Art. 13, S.Treaty Doc. 106-18; Treaty on Mutual Legal Assistance in Criminal Matters, U.S.-Egypt, Art. 12, S.Treaty Doc. 106-19; Treaty on Mutual Legal Assistance in Criminal Matters, U.S.-Rom., Art. 13, S.Treaty Doc. 10620; Treaty on Mutual Legal Assistance in Criminal Matters, U.S.-Cyprus, Art. 13, S.Treaty Doc. 106-35; Treaty on Mutual Legal Assistance in Criminal Matters, U.S.-S.Afr., Art. 14, S.Treaty Doc. 106-36.

[1308] E.g., Treaty on Mutual Legal Assistance in Criminal Matters, U.S.-Fr., Art. 15, S. Treaty Doc. 106-17 ("The Requested State shall serve procedural documents and judicial decisions sent to it for this purpose by the Requesting State. . . ."); Treaty on Mutual Legal Assistance in Criminal Matters, U.S.-Liech., Art. 14, S.Treaty Doc. 106-16; Treaty on Mutual Legal Assistance in Criminal Matters, U.S.-Greece, Art. 14, S.Treaty Doc. 106-18; Treaty on Mutual Legal Assistance in Criminal Matters, U.S.-Egypt, Art. 13, S.Treaty Doc. 106-19; Treaty on Mutual Legal Assistance in Criminal Matters, U.S.-Rom., Art. 14, S.Treaty Doc. 106-20; Treaty on Mutual Legal Assistance in Criminal Matters, U.S.-Cyprus, Art. 14, S.Treaty Doc. 106-35; Treaty on Mutual Legal Assistance in Criminal Matters, U.S.-S.Afr., Art. 15, S.Treaty Doc. 106-36.

[1309] E.g., Treaty on Mutual Legal Assistance in Criminal Matters, U.S.-Greece, Art. 15, S.Treaty Doc. 106-18 (2000); ("The Requested State shall execute a request that it search for, seize, and transfer any item to the Requesting State if the request justifies such action under the laws of the Requested State. . . ."); Treaty on Mutual Legal Assistance in Criminal Matters, U.S.-Liech., Art. 15, S.Treaty Doc. 106-16; Treaty on Mutual Legal Assistance in Criminal Matters, U.S.-Fr., Art. 10, S. Treaty Doc. 106-17; Treaty on Mutual Legal Assistance in Criminal Matters, U.S.-Egypt, Art. 14, S.Treaty Doc. 106-19; Treaty on Mutual Legal Assistance in Criminal Matters, U.S.-Rom., Art. 15,

persuading foreign nationals to come to the United States voluntarily to present evidence here;[1311] and forfeiture related seizures.[1312]

Letters Rogatory

Witness depositions may be taken in a foreign country cooperatively using letters rogatory in the case of nations with whom the United States has no MLAT or similar agreement. Letters rogatory involve the formal request from the courts of one country to those of another asking that a witness' statement be taken. The procedure is governed by statute and rule.[1313] It is often a resource of last resort. The process, through diplomatic channels, is time consuming, cumbersome, and lies within the discretion of the foreign court to which it is addressed.[1314]

S.Treaty Doc. 10620 (2000); Treaty on Mutual Legal Assistance in Criminal Matters, U.S.-Cyprus, Art. 15, S.Treaty Doc. 106-35; Treaty on Mutual Legal Assistance in Criminal Matters, U.S.-S.Afr., Art. 16, S.Treaty Doc. 106-36.

[1310] E.g., Treaty on Mutual Legal Assistance in Criminal Matters, U.S.-Egypt, Art. 8, S.Treaty Doc. 106-19;("A person in the Requested State from whom testimony or evidence is requested pursuant to this Treaty shall be compelled, if necessary, under the laws of the Requested State to appear and testify or produce items, including documents, records, and articles of evidence . . ."); Treaty on Mutual Legal Assistance in Criminal Matters, U.S.-Liech., Art. 8, S.Treaty Doc. 106-16; Treaty on Mutual Legal Assistance in Criminal Matters, U.S.-Fr., Art. 9(2), S. Treaty Doc. 106-17; Treaty on Mutual Legal Assistance in Criminal Matters, U.S.-Greece, Art. 8, S.Treaty Doc. 106-18; Treaty on Mutual Legal Assistance in Criminal Matters, U.S.-Rom., Art. 8, S.Treaty Doc. 106-20; Treaty on Mutual Legal Assistance in Criminal Matters, U.S.-Cyprus, Art. 8, S.Treaty Doc. 106-35; Treaty on Mutual Legal Assistance in Criminal Matters, U.S.-S.Afr., Art. 9, S.Treaty Doc. 106-36.

[1311] E.g., Treaty on Mutual Legal Assistance in Criminal Matters, U.S.-Belize, Art. 10, S.Treaty Doc. 106-19 ("1. When the Requesting State requests the appearance of a person in that State, the Requested State shall invite the person to appear before the appropriate authority in the Requesting State . . ."); see also, Treaty on Mutual Legal Assistance in Criminal Matters, U.S.-Liech., Art. 10, S.Treaty Doc. 107-16 (person may be served or detained except as stated in the request); Treaty on Mutual Legal Assistance in Criminal Matters, U.S.-Venez., Art. X, S.Treaty Doc. 105-38.

[1312] E.g., Treaty on Mutual Legal Assistance in Criminal Matters, U.S.-Cyprus, Art. 17(2), S.Treaty Doc. 106-35 (2000) ("The Parties shall assist each other to the extent permitted by their respective laws in proceedings relating to the forfeiture of the proceeds and instrumentalities of offense, restitution to the victims of crime, and the collection of fines imposed as sentences in criminal prosecutions. This may include action to temporarily immobilize the proceeds or instrumentalities pending further proceedings"); Treaty on Mutual Legal Assistance in Criminal Matters, U.S.-Greece, Art. 17, S.Treaty Doc. 106-18 ; Treaty on Mutual Legal Assistance in Criminal Matters, U.S.-Liech., Art. 17, S.Treaty Doc. 106-16; Treaty on Mutual Legal Assistance in Criminal Matters, U.S.-Fr., Art. 11, S. Treaty Doc. 106-17; Treaty on Mutual Legal Assistance in Criminal Matters, U.S.-Egypt, Art. 16, S.Treaty Doc. 106-19; Treaty on Mutual Legal Assistance in Criminal Matters, U.S.-Rom., Art. 17, S.Treaty Doc. 106-20; Treaty onMutual Legal Assistance in Criminal Matters, U.S.-S.Afr., Art. 18, S.Treaty Doc. 106-36.

[1313] 28 U.S.C. 1781, 1782; F.R.Civ.P. 28(b).

[1314] See generally, Abbell, OBTAINING EVIDENCE ABROAD IN CRIMINAL CASES §3-3 (2004 & 2008 Supp.); United States Department of State, Preparation of Letters Rogatory, available on

Cooperative Efforts

American law enforcement officials have historically used other, often less formal, cooperative methods overseas to investigate and prosecute extraterritorial offenses. In the last few decades the United States has taken steps to facilitate cooperative efforts. Federal law enforcement agencies have assigned an increasing number of personnel overseas. For example, the Justice Department's Criminal Division has resident legal advisors in 37 countries abroad;[1315] and the Federal Bureau of Investigation now operates legal attache offices in 75 foreign cities;[1316] the Drug Enforcement Administration has offices in 87;[1317] the U.S. Immigration and Customs Enforcement agency in 54;[1318] the Secret Service in 20.[1319]

A few regulatory agencies with law enforcement responsibilities have working arrangements with their foreign counterparts. The Securities and Exchange Commission, for instance, has bilateral enforcement memoranda of understanding with 20 foreign securities commissions and, with 62 others, is a signatory of the International Organization of Securities Commissions' multilateral memorandum of understanding (IOSCO MMOU).[1320]

December 7, 2009 at http://www.travel.state.gov/ law/info/judicial/judicial_683.html. One commentator has observed that, "parties utilizing letters rogatory must simply cross their fingers and hope that the foreign nation will provide the evidence in a timely fashion and in an admissible form. Historically, the absence of a reliable evidence-gathering mechanism often stymied prosecutorial efforts, making it not unusual for the U.S. government to simply forgo transnational prosecutions," Richardson, Due Process for the Global Crime Age: A Proposal, 41 CORNELL INTERNATIONAL LAW JOURNAL 347 (2008); Intel Corp. v. Advanced Micro Devices, Inc., 542 U.S. 241, 247 (2004).

[1315] Ass't Att'y Gen. Lanny A. Breuer, The Global Case for Justice: Protecting Human Rights and Promoting the Rule of Law at http://www.justice.gov/criminal/pr/speeches/2009/10/10-07-09/breuer-speech.pdf.

[1316] Federal Bureau of Investigation, Legal Attache Offices at http://www.fbi.gov/contact/legat/legat.htm.

[1317] Drug Enforcement Administration, DEA Office Locations at http://www.justice.gov/dea/agency/domestic.htm.

[1318] U.S. Immigration and Customs Enforcement, The ICE International Presence at http://www.ice.gov/internationalaffairs/presence.htm.

[1319] U.S. Secret Service, U.S. Secret Service Field Offices at http://www.secretservice.gov/field_offices.shtml.

[1320] U.S. Securities and Exchange Commission, International Enforcement Assistance at http://www.sec.gov/about/offices/oia/oia_crossborder.htm#mechanisms. See also, http://www.iosco.org/library/index.cfm?section=mou_siglist.

Congress has enacted several measures to assign foreign law enforcement efforts in this country in anticipation of reciprocal treatment. For instance, the Foreign Evidence Request Efficiency Act of 2009 authorizes Justice Department attorneys to petition federal judges for any of a series of orders to facilitate investigations in this country by foreign law enforcement authorities.[1321] The authorization extends to the issuance of:

- search warrants;
- court orders for access to stored electronic communications and to communications records;
- pen register or trap and trace orders; and
- subpoena authority, both testimonial and for the production of documents and other material.[1322]

Search and Seizure Abroad

Overseas cooperative law enforcement assistance occasionally has either Fourth or Fifth Amendment implications. In the case of the Fourth Amendment, the relatively limited lower federal court case law has remained fairly uniform, although the diversity of views reflected in the Supreme Court's Verdugo-Urquidez decision in 1990[1323] lends an air of uncertainty to the matter. Prior to Verdugo-Urquidez, it seems to have been generally agreed that the Fourth Amendment governed the overseas search and seizure of the person or property of Americans by American law enforcement officials.[1324] On the other hand, neither the Fourth Amendment[1325] nor its exclusionary rule[1326] were considered applicable to overseas searches and seizures conducted by foreign law

---

[1321] P.L. 111-79, 123 Stat. 2086 (2009), 18 U.S.C. 3512.

[1322] 18 U.S.C. 3512(a)(2). In the absence of a treaty nexus, the reach of the authority may be subject to constitutional limitations, see U.S. Const. Art. III, §2.

[1323] United States v. Verdugo-Urquidez, 494 U.S. 259 (1990).

[1324] United States v. Conroy, 589 F.2d 1258, 1264 (5th Cir. 1979); Berlin Democratic Club v. Rumsfeld, 410 F.Supp. 144, 157 (D.D.C. 1976).

[1325] Birdsell v. United States, 346 F.2d 775, 782 (5th Cir. 1965).

[1326] United States v. Janis, 428 U.S. 433, 455-56 n.31 (1976)(". . . It is well established, of course, that the exclusionary rule, as a deterrent sanction, is not applicable where a private party or foreign government commits the offending act"); United States v. Callaway, 446 F.2d 753, 755 (3d Cir. 1971); United States v. Morrow, 537 F.2d 120, 139 (5th Cir. 1976); Stowe v. Devoy, 588 F.2d 336, 341 (2d Cir. 1978); United States v. Marzano, 537 F.2d 257, 269-71 (7th Cir. 1976); United States v. Rose, 570 F.2d 1358, 1361-362 (9th Cir. 1978); United States v. Hensel, 699 F.2d 18, 25 (1st Cir. 1983); United States v. Mount, 757 F.2d 1315, 1317-318 (D.C.Cir. 1985); United States v. Delaplane, 778 F.2d 570, 573 (10th Cir. 1985); United States v. Rosenthal, 793 F.2d 1214, 1231 (11th Cir. 1986).

enforcement officials,[1327] except under two circumstances. The first exception covered foreign conduct which "shocked the conscience of the court."[1328] The second reached foreign searches or seizures in which American law enforcement officials were so deeply involved as to constitute "joint ventures" or some equivalent level of participation.[1329] The cases seldom explained whether these exceptions operated under all circumstances or only when searches or seizures involved the person or property of Americans. In the days when MLATs were scarce, however, the courts rarely, if ever, encountered circumstances sufficient to activate either exception.

Verdugo-Urquidez may suggest a more narrow application of the Fourth Amendment than was previously contemplated. It holds that "the Fourth Amendment [does not] appl[y] to the search and seizure by United States agents of property that is owned by a nonresident alien and located in a foreign country," 494 U.S. at 261. The majority opinion is grounded not in the principles previously announced by the lower courts but in its reading of the history of the Amendment and of the Court's earlier treatment of the Constitution's application overseas and to aliens.[1330] Earlier lower court jurisprudence is neither mentioned nor cited. Moreover, one of the Justices in the five member majority and a sixth Justice authored concurrences in which they indicated that Fourth Amendment reasonableness abroad may be very different from the Amendment's demands domestically.[1331]

[1327] Stonehill v. United States, 405 F.2d 738, 743 (9th Cir. 1969)("Neither the Fourth Amendment to the United States Constitution nor the exclusionary rule of evidence, designed to deter federal officers from violating the Fourth Amendment, is applicable to the acts of foreign officials").

[1328] United States v. Callaway, 446 F.2d 753, 755 (3d Cir. 1971); United States v. Morrow, 537 F.2d 120, 139 (5th Cir. 1976); Stowe v. Devoy, 588 F.2d 336, 341 (2d Cir. 1978); United States v. Rose, 570 F.2d 1358, 1362 (9th Cir. 1978); United States v. Hensel, 699 F.2d 18, 25 (1st Cir. 1983); United States v. Delaplane, 778 F.2d 570, 573-74 (10th Cir. 1985); United States v. Rosenthal, 793 F.2d 1214, 1231-232 (11th Cir. 1986).

[1329] Stonehill v. United States, 405 F.2d 738, 743 (9th Cir. 1969); United States v. Callaway, 446 F.2d 753, 755 (3d Cir. 1971); United States v. Morrow, 537 F.2d 120, 139 (5th Cir. 1976); United States v. Rose, 570 F.2d 1358, 1362 (9th Cir. 1978); United States v. Hensel, 699 F.2d 18, 25 (1st Cir. 1983); United States v. Mount, 757 F.2d 1315, 1317-318 (D.C.Cir. 1985); United States v. Delaplane, 778 F.2d 570, 573-74 (10th Cir. 1985); United States v. Rosenthal, 793 F.2d 1214, 1231-232 (11th Cir. 1986).

[1330] "We think that the text of the Fourth Amendment, its history, and our cases discussing the application of the Constitution to aliens and extraterritorially require rejection of respondent's claim. At the time of the search, he was a citizen and resident of Mexico with no voluntary attachment to the United States and the place searched was located in Mexico. Under these circumstances, the Fourth Amendment has no application," 494 U.S. 274-75.

[1331] 494 U.S. at 278 (Kennedy, J., concurring)("The absence of local judges or magistrates available to issue warrants, the differing and perhaps unascertainable conceptions of reasonableness and privacy that prevail abroad, and the need to cooperate with foreign officials

One commentator argues that the concurrences should be read as confining rather than expanding the impact of the majority decision:

> *Given Verdugo-Urquidez, it might understandably be thought that the issue discussed herein – when, if ever, a United States connection with a search in a foreign country is substantial enough to make the Fourth Amendment and its exclusionary rule applicable – is of no relevance whenever that search is directed at an alien not then in the United States. But, an examination of the positions of the two concurring and three dissenting Justices suggests otherwise. The dissenters. . . are of the view that if the foreign search is properly characterized as United States activity . . . then the Fourth Amendment applies if the defendant is being subjected to a U.S. criminal prosecution. . . . Thus, the most that can be definitely concluded from Verdugo-Urquidez is that the Fourth Amendment's warrant clause is inapplicable to a search conducted under the circumstances present in that case. Beyond that, much depends upon the exact positions of the two [cryptic] concurring Justices. 1 LaFave, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT 325-26 (4th ed. 2004)(emphasis in the original).*

Subsequent case law in the lower federal courts acknowledges Verdugo-Urquidez and molds the principles of the opinion for the Court into the body of pre-existing law. Although limited, it indicates that the Fourth Amendment does not apply to a search conducted overseas of the property of a foreign national with no voluntary connection to the United States.[1332] As for overseas searches of the property of Americans or aliens permanently resident in the United States, the Fourth Amendment is said not to apply to a search by foreign officials unless conducted as a "joint venture" with American authorities or unless the conduct of the foreign officials "shocks the conscience of the court."[1333] Nevertheless, "the

---

all indicate that the Fourth Amendment's warrant requirement should not apply in Mexico as it does in this country"); id. at 279 (Stevens, J., concurring in the judgment)("I do agree, however, with the Government's submission that the search conducted by the United States agents with the approval and cooperation of the Mexican authorities was not 'unreasonable' as that term is used in the first Clause of the Amendment. I do not believe the Warrant Clause has any application to searches of noncitizens' homes in foreign jurisdictions because American magistrates have no power to authorize such searches").

[1332] United States v. Valencia-Trujillo, 573 F.3d 1171, 1183 (11th Cir. 2009); United States v. Bravo, 489 U.S. 1, 8-9 (1st Cir. 2007); United States v. Zakharov, 468 F.3d 1171, 1179-180 (9th Cir. 2006); United States v. Inigo, 925 F.3d 641, 656 (3d Cir. 1991); United States v. Suchit, 480 F.Supp. 39, 51 n.18 (D.C.Cir. 2007).

[1333] United States v. Emmanuel, 565 F.3d 1324, 1330 (11th Cir. 2009); United States v. Barona, 56 F.3d 1087, 1090-93 (9th Cir. 1995); United States v. Behety, 32 F.3d 503, 510-11 (11th Cir.

Fourth Amendment's reasonableness standard applies to United States officials conducting a search affecting a United States citizen in a foreign country."[1334] On the other hand, even under such circumstances, "a foreign search is reasonable if it conforms to the requirements of foreign law," and "such a search will be upheld under the good faith exception to the exclusionary rule when United States officials reasonably rely on foreign officials' representations of foreign law."[1335]

Self-Incrimination Overseas

Like the Fourth Amendment protection against unreasonable searches and seizures, the Fifth Amendment self-incrimination clause and its attendant Miranda warning requirements do not apply to statements made overseas to foreign officials[1336] subject to the same "joint venture"[1337] and "shocked conscience" exceptions.[1338] The Fifth Amendment and Miranda requirements do apply to custodial interrogations conducted overseas by American officials regardless of the nationality of the defendant.[1339] Of course as a general rule to be admissible at trial in this country, any confession must have been freely made.[1340]

1994)(the Fourth Amendment does not apply to the search and seizure of alien property abroad by foreign officials subject to conscience shocking and joint venture exceptions); United States v. Castro, 175 F.Supp.2d 129, 132-33 (D.P.R. 2001); United States v. Marzook, 435 F.Supp.2d 708, 774 (N.D. Ill. 2006).

[1334] In re Terrorist Bombings of U.S. Embassies in East Africa, 552 F.3d 157, 167-72 (2d Cir. 2008); United States v. Barona, 56 F.3d 1087, 1094 (9th Cir. 1995).

[1335] United States v. Juda 46 F.3d 961, 968 (9th Cir. 1995); United States v. Castro, 175 F.3d 129, 133-34 (D.P.R. 2001).

[1336] United States v. Abu Ali, 528 F.3d 210, 227-28 (4th Cir. 2008); United States v. Yousef, 327 F.3d 56, 145 (2d Cir. 2003); United States v. Martindale, 790 F.2d 1129, 1131-132 (4th Cir. 1986); United States v. Heller, 625 F.2d 594, 599 (5th Cir. 1980); United States v. Mundt, 508 F.2d 904, 906 (10th Cir. 1974); United States v. Karake, 443 F.Supp.2d 8, 49 (D.D.C. 2006).

[1337] United States v. Abu Ali, 528 F.3d 210, 227-28 (4th Cir. 2008); United States v. Yousef, 327 F.3d 56, 145-46 (2d Cir. 2003); United States v. Heller, 625 F.2d 594, 599 (5th Cir. 1980); United States v. Covington, 783 F.2d 1052, 1056 (9th Cir. 1986); United States v. Mundt, 508 F.2d 904, 906-907 (10th Cir. 1974); United States v. Karake, 443 F.Supp.2d 8, 49 (D.D.C. 2006); United States v. Hensel, 509 F.Supp. 1364, 1375 (D. Me. 1981).

[1338] United States v. Abu Ali, 528 F.3d 210, 227-28 (4th Cir. 2008); United States v. Yousef, 327 F.3d 56, 145-46 (2d Cir. 2003), citing, United States v. Cotroni, 527 F.2d 708, 712 n.10 (2d Cir. 1975); United States v. Heller, 625 F.2d 594, 599 (5th Cir. 1980).

[1339] In re Terrorist Bombings of U.S. Embassies in East Africa, 552 F.3d 177, 201-2 (2d Cir. 2008); United States v. Clarke, 611 F.Supp.2d 12, 28-9 (D.D.C. 2009); United States v. Yousef, 327 F.3d 56, 145-46 (2d Cir. 2003).

[1340] Schneckloth v. Bustamonte, 412 U.S. 218, 225-26 (1973)("the ultimate test remains that which has been the only clearly established test in Anglo-American courts for two hundred years: the test of voluntariness. Is the confession the product of an essentially free and unconstrained choice by its maker? If it is, if he has will to confess, it may be used against him. If it is not, if his will has

Statute of Limitations: 18 U.S.C. 3292 and Related Matters

As a general rule, prosecution of federal crimes must begin within 5 years.[1341] Federal capital offenses and certain federal terrorist offenses, however, may be prosecuted at any time,[1342] and prosecution of nonviolent federal terrorism offenses must begin within 8 years.[1343] Moreover, the statute of limitations is suspended or tolled during any period in which the accused is a fugitive.[1344] Whatever the applicable statute of limitations, section 3292 authorizes the federal courts to suspend it in order to await the arrival of evidence requested of a foreign government:

> *Upon application of the United States, filed before return of an indictment, indicating that evidence of an offense is in a foreign country, the district court before which a grand jury is impaneled to investigate the offense shall suspend the running of the statute of limitations for the offense if the court finds by a preponderance of the evidence that an official request has been made for such evidence and that it reasonably appears, or reasonably appeared at the time the request was made, that such evidence is, or was, in such foreign country. 18 U.S.C. 3292(a)(1).*

Section 3292 suspensions may run for no more than six months if the requested foreign assistance is provided before the time the statute of limitations would

---

been overborne and his capacity for self-determination critically impaired, the use of confession offends due process"); United States v. Abu Ali, 528 F.3d 210, 232 (4th Cir. 2008); United States v. Lopez, 437 F.3d 1059, 1063-64 (10th Cir. 2006); United States v. Jacobs, 431 F.3d 99, 108 (3d Cir. 2005); United States v. Thompson, 422 F.3d 1285, 1295-296 (11th Cir. 2005); United States v. Garcia Abrego, 141 F.3d 142, 170-71 (5th Cir. 1998); United States v. Karake, 443 F.Supp.2d 8, 85-6 (D.D.C. 2006); United States v. Marzook, 435 F.Supp.2d 708, 741 (N.D.Ill. 2006)("interrogation accompanied by physical violence is presumptively involuntary").

[1341] 18 U.S.C. 3282.

[1342] 18 U.S.C. 3281 (capital offenses); 18 U.S.C. 3286(b)(prosecution of any of the offenses listed in 18 U.S.C. 2332b(g)(5)(B) whose commission created a foreseeable risk of serious injury or resulted in such injury). Section 2332b(g)(5)(B) lists more than 40 federal criminal offenses including crimes such as violence in international airports (18 U.S.C. 37), assassination of the President (18 U.S.C. 1751), providing material support to terrorist organizations (18 U.S.C. 2339B).

[1343] 18 U.S.C. 3286(a)(violation of an offense listed in 18 U.S.C. 2332b(g)(5)(B) whose commission does not create a foreseeable risk of serious injury or result in such injury).

[1344] 18 U.S.C. 3290. Most courts construe section 3290 to require flight with an intent to avoid prosecution or a departure from the place where the offense occurred with the knowledge that an investigation is pending or being conducted, United States v. Florez, 447 F.3d 145, 150-52 (2d Cir. 2006)(citing authority in accord). Thus, a suspect in the case of an federal extraterritorial offense is not likely to be considered a fugitive if he simply remains in the country were of the offense was committed.

otherwise have expired and for no more than three years in other instances.[1345] The suspension period begins with the filing of the request for foreign assistance and ends with final action by the foreign government upon the request.[1346] Because of the built-in time limits, the government need not show that it acted diligently in its attempts to gather overseas evidence.[1347] The circuits are divided over whether the section may be used to revive a statute of limitations by filing a request after the statute has run,[1348] and over whether the section can be used to extend the statute of limitations with respect to evidence that the government has already received at the time it filed the request.[1349] At least one circuit has held that the statutory reference to "the district court before which a grand jury is impaneled to investigate the offense" is intended to identify the court that may issue the suspension order and does not limit the statute to requests filed in aid of a pending grand jury investigation.[1350]

Extradition

Extradition is perhaps the oldest form of international law enforcement assistance. It is a creature of treaty by which one country surrenders a fugitive to another for prosecution or service of sentence.[1351] The United States has bilateral extradition treaties with roughly two-thirds of the nations of the world.[1352] Treaties negotiated before 1960 and still in effect reflect the view then held by the United States and other common law countries that criminal jurisdiction was territorial and consequently extradition could not be had for extraterritorial

---

[1345] 18 U.S.C. 3292(c)("The total of all periods of suspension under this section with respect to an offense – (1) shall not exceed three years; and (2) shall not extend a period within which a criminal case must be initiated for more than six months if all foreign authorities take final action before such period would expire without regard to this section"); United States v. Baldwin, 414 F.3d 791, 795 (7th Cir. 2005); United States v. Grenoble, 413 F.3d 569, 574-75 (6th Cir. 2005).

[1346] 18 U.S.C. 3292(b).

[1347] United States v. Hagege, 437 F.3d 943, 955 (9th Cir. 2006).

[1348] An application for suspension must be filed before the statute has run, United States v. Brody, 621 F.Supp.2d 1196, 1199-1200 (D.Utah 2009); United States v. Kozeny, 541 F.3d 166, 170-71 (2d Cir. 2008), citing to the contrary United States v. Bischel, 61 F.3d 1429 (9th Cir. 1995).

[1349] United States v. Atiyeh, 402 F.3d 354, 362-66 (3d Cir. 2005)(holding that the statute of limitations may not be suspended under section 3292 when the request for foreign assistance is submitted after the evidence has in fact been received); contra, United States v. Miller, 830 F.2d 1073, 1076 (9th Cir. 1987); United States v. DeGeorge, 380 F.3d 1203, 1213 (9th Cir. 2004).

[1350] United States v. DeGeorge, 380 F.3d 1203, 1214 (9th Cir. 2004).

[1351] See generally, CRS Report 98-958, Extradition To and From the United States: Overview of the Law and Recent Treaties, by Charles Doyle.

[1352] 18 U.S.C. 3181 note (list the countries with whom we have extradition treaties).

crimes.[1353] Subsequently negotiated agreements either require extradition regardless of where the offense occurs,[1354] permit extradition regardless of where the offense occurs,[1355] or require extradition where the extraterritorial laws of the two nations are compatible.[1356]

More recent extradition treaties address other traditional features of the nation's earlier agreements that complicate extradition, most notable the nationality exception, the political offense exception, and the practice of limiting extradition to a list of specifically designated offenses.

Federal crimes committed within other countries are more likely to be the work of foreign nationals than is otherwise the case. Yet, the "most common type of treaty provision provides that neither of the contracting parties shall be bound to deliver up its own citizens or subjects."[1357] Most treaties negotiated of late, however, contain either an article declaring that extradition may not be denied on the basis of nationality[1358] or one declaring that if extradition is denied on the basis of nationality the case must be referred to local authorities for prosecution.[1359]

[1353] Abbell, EXTRADITION TO AND FROM THE UNITED STATES, §§3-2(5), 6-2(5) (2004 & 2007 Supp.).

[1354] E.g., Extradition Treaty, U.S.-Jordan, Art.2(4), S.Treaty Doc. 104-3 ("An offense described in this Article shall be an extraditable offense regardless of where the act or acts constituting the offense were committed"); Extradition Treaty, U.S.-Austria, Art.2(6), S.Treaty Doc. 105-50; Extradition Treaty, U.S.-Lux., Art.2(1), S.Treaty Doc. 105-10.

[1355] Extradition Treaty, U.S.-Hung., Art.2(4), S.Treaty Doc. 104-5 ("If the offense has been committed outside the territory of the Requesting State, extradition shall be granted if the laws of the Requested State provide for the punishment of an offense committed outside of its territory in similar circumstances. If the laws of the Requested State do not so provide, the executive authority of the Requested State may, in its discretion grant extradition"); Extradition Treaty, U.S.-Bah., Art.2(4), S.Treaty Doc. 102-17.

[1356] Extradition Treaty, U.S.-Fr., Art.2(4), S.Treaty Doc. 105-13 ("Extradition shall be granted for an extraditable offense committed outside the territory of the Requesting State, when the laws of the Requested State authorize the prosecution or provide the punishment for that offense in similar circumstances").

[1357] Bassiouni, INTERNATIONAL EXTRADITION: UNITED STATES LAW AND PRACTICE 683 (4th ed. 2002).

[1358] E.g., Extradition Treaty, U.S.-Peru, Art. III, S.Treaty Doc. 107-6 ("Extradition shall not be refused on the ground that the person sought is a national of the Requested State"); Extradition Treaty, U.S.-Belize, Art. 3, S.Treaty Doc. 10638; Extradition Treaty, U.S.-Para., Art. III, S.Treaty Doc. 106-4.

[1359] Extradition Treaty, U.S.-Kor., Art. 3, S.Treaty Doc. 106-2 ("1. Neither Contracting State shall be bound to extradite its own nationals, but the Requested State shall have the power to extradite such person if, in its discretion, it be deemed proper to do so. 2. If extradition is refused solely on

"The political offense exception is now a standard clause in almost all extradition treaties of the world."[1360] Originally designed to protect unsuccessful insurgents in flight,[1361] it is often construed to include both the purely political offense such as treason and sedition and related political offenses such as an act of violence committed during the course of, and in furtherance of, a political upheaval.[1362] The exception is somewhat at odds with contemporary desires to prevent, prosecute, and punish acts of terrorism. Consequently, treaties forged over the last several years frequently include some form of limitation on the exception, often accompanied by a discretionary right to refuse politically or otherwise discriminatorily motivated extradition requests.[1363]

---

the basis of the nationality of the person sought, the Requested State shall, at the request of the Requesting State, submit the case to its authorities for prosecution. 3. Nationality shall be determined at the time of the commission of the offense for which extradition is requested"); Extradition Treaty, U.S.-Pol., Art. 4, S.Treaty Doc. 105-14; Extradition Treaty, U.S.-Fr., Art. 3, S.Treaty Doc. 105-13.

[1360] Bassiouni, INTERNATIONAL EXTRADITION: UNITED STATES LAW AND PRACTICE 595 (4th ed. 2002).

[1361] Quinn v. Robinson, 783 F.2d 776, 792-93 (9th Cir. 1986)("The political offense exception is premised on a number of justifications. First, its historical development suggests that it is grounded on the belief that individuals have a right to resort to political activism to foster political change. This justification is consistent with the modern consensus that political crimes have greater legitimacy than common crimes. Second, the exception reflects a concern that individuals – particularly unsuccessful rebels – should not be returned to countries where they may be subjected to unfair trials and punishments because of their political opinions. Third, the exception comports with the notion that governments – and certainly their non-political branches – should not intervene in the internal political struggles of other nations").

[1362] Bassiouni, INTERNATIONAL EXTRADITION: UNITED STATES LAW AND PRACTICE 594-673 (4th ed. 2002).

[1363] E.g., Extradition Treaty, U.S.-S.Afr., Art. 4, S.Treaty Doc. 106-24 ("1. Extradition shall not be granted if the offense for which extradition is requested is a political offence. 2. For the purpose of this Treaty, the following offenses shall not be considered political offenses: (a) a murder or other violent crime against a Head of State or Deputy Head of State of the Requesting or Requested State, or against a member of such person's family; (b) an offence for which both the Requesting and Requested States have the obligation pursuant to a multilateral international agreement to extradite the person sought or to submit the case to their respective competent authorities for decision as to prosecution; (c) murder; (d) an offense involving kidnaping, abduction, or any form of unlawful detention, including the taking of a hostage; and (e) attempting or conspiring to commit, aiding, abetting, inducing, counseling or procuring the commission of, or being an accessory before or after the fact of such offences. 3. Notwithstanding the terms of sub-article 2, extradition shall not be granted if the executive authority of the Requested State determines that there are substantial grounds for believing that the request has been made for the purpose of prosecuting or punishing a person on account of that person's gender, race, religion, nationality, or political opinion"); Extradition Treaty, U.S.-Pol., Art. 5, S.Treaty Doc. 105-14 (motivation clause is limited to politically motivated); Extradition Treaty, U.S.-Sri Lanka, Art. 4, S.Treaty Doc. 106-34 (only Heads of State clause, clauses identifying particular international obligations, and a

Current U.S. extradition treaties signed prior to the 1980's list specific crimes to which the treaty is limited.[1364] In the nation's first extradition treaty the list was limited to murder and forgery;[1365] towards the end of the twentieth century the standard lists had grown to close to or more than thirty crimes.[1366] Treaties agreed to more recently opt for a generic description.[1367]

As an alternative to extradition, particularly if the suspect is not a citizen of the country of refuge, foreign authorities may be willing to expel or deport him under circumstances that allow the United States to take him into custody.[1368] In the absence of a specific treaty provision, the fact that the defendant was abducted overseas and brought to the United States for trial rather than pursuant to a request under the applicable extradition treaty does not deprive the federal court of jurisdiction to try him.[1369]

---

conspiracy-attempt-accessory clause)(motivation clause is limited to politically motivated requests).

[1364] Abbell, EXTRADITION TO AND FROM THE UNITED STATES, §3-2(2)(2004 & 2007 Supp.).

[1365] 8 Stat. 116, 129 (1794).

[1366] Extradition Treaty, U.S.-U.K., 28 U.S.T. 227, 235(1977)(29 crimes); Extradition Treaty, U.S.-Nor., 31 U.S.T. 5619, 5634 (1980)(33 crimes); Extradition Treaty, U.S.-F.R.G., 32 U.S.T. 1485, 1515 (1980)(33 crimes).

[1367] E.g., Extradition Treaty, U.S.-Austria, Art. 2(1), S.Treaty Doc. 105-50 ("Extradition shall be granted for offenses which are subject under the laws in both Contracting Parties by deprivation of liberty for a period of more than one year or by a more severe penalty"); Extradition Treaty, U.S.-Malay., Art. 2(1), S.Treaty Doc. 104-26; Extradition Treaty, U.S.-Zimb., Art. 2(1), S.Treaty Doc. 105-33.

[1368] United States v. Mejia, 448 F.3d 436, 439 (D.C.Cir. 2006)(Panamaian authorities arrested the defendants and turned them over to U.S. Drug Enforcement Administration (DEA) officers in Panama who flew them to the U.S.); United States v. Arbane, 446 F.3d 1223, 1225 (11th Cir. 2006)(Ecuadorian officials deported the defendant to Iran on a plane scheduled to stop in the U.S. where the defendant was arrested); United States v. Matta-Ballesteros, 71 F.3d 754, 761 (9th Cir. 1995)(Honduran military and U.S. Marshals seized the defendant in Honduras and the Marshals flew him to the U.S. by way of the Dominican Republic); United States v. Chapa-Garza, 62 F.3d 118, 120 (5th Cir. 1995)(Mexican authorities deported the defendant to the United States); United States v. Pomeroy, 822 F.2d 718, 720 (8th Cir. 1987) (Canadian authorities deported the defendant to the United States); United States v. Valot, 625 F.2d 308, 309 (9th Cir. 1980)(Thai immigration authorities handed the defendant over to DEA agents in the Bangkok airport who flew him to the United States "over his protest").

[1369] United States v. Alvarez-Machain, 504 U.S. 655, 669-70 (1992)(portions of the footnote 16 of the Court's opinion in brackets)("Mexico has protested the abduction of respondent through diplomatic notes, and the decision of whether respondent should be returned to Mexico, as a matter outside of the Treaty, is a matter for the Executive Branch. [The Mexican Government has also requested from the United States the extradition of two individuals it suspects of having abducted respondent in Mexico on charges of kidnaping. . . .] . . .The fact of respondent's forcible abduction does not therefore prohibit his trial in a court in the United States for violations of the

Venue

Federal crimes committed within the United States must be tried where they occur.[1370] Venue over extraterritorial crimes is a matter of statute, 18 U.S.C. 3238. Section 3238 permits the trial of extraterritorial crimes either (1) in the district into which the offender is "first brought" or in which he is arrested for the offense; or (2) prior to that time, by indictment or information in the district of the offender's last known residence, or if none is known, in the District of Columbia.[1371] The phrase "first brought" as used in section 3238 means "first brought while in custody."[1372] As the language of the section suggests, venue for all joint offenders is proper wherever venue for one of their number is proper.[1373]

Testimony of Overseas Witnesses

A federal court may subpoena a United States resident or national found abroad to appear before it or the grand jury.[1374] Federal courts ordinarily have no

---

criminal laws of the United States"); see also, United States v. Mejia, 448 F.3d 436, 442-43 (D.C.Cir. 2006); United States v. Arbane, 446 F.3d 1223, 1225 (11th Cir. 2006); United States v. Best, 304 F.3d 308, 311-16 (3d Cir. 2002); Kasi v. Angelone, 300 F.3d 487, 493-98 (4th Cir. 2002); United States v. Torres Gonzalez, 240 F.3d 14, 16 (1st Cir. 2001).

[1370] U.S. Const. Art. III, §2, cl.3; Amend.VI.

[1371] "The trial of all offenses begun or committed upon the high seas, or elsewhere out of the jurisdiction of any particular State or district, shall be in the district in which the offender, or any one of two or more joint offenders, is arrested or is first brought; but if such offender or offenders are not so arrested or brought into any district, an indictment or information may be filed in the district of the last known residence of the offender or of any one of two or more joint offenders, or if no such residence is known the indictment or information may be filed in the District of Columbia," 18 U.S.C. 3238. United States v. Hisin-Yung, 97 F.Supp.2d 24, 28 (D.C.Cir. 2000)("The two clauses provide alternative proper venues. Therefore, if the latter provision is relied on, and defendant is indicted before he is brought into the United States, he may be tried in the district in which he was indicted regardless of whether it is the district in which he is first brought into the United States"); see also, United States v. Gurr, 471 F.3d 144, 155 (D.C. Cir. 2007); United States v. Hilger, 867 F.2d 566, 568 (9th Cir. 1989); United States v. Fraser, 709 F.2d 1556, 1558 (6th Cir. 1983); United States v. McRary, 616 F.2d 181, 185 (5th Cir. 1980).

[1372] United States v. Feng, 277 F.3d 1151, 1155 (9th Cir. 2002)("The word 'brought' under the statute means first brought into a jurisdiction from outside the United States jurisdiction while in custody"); United States v. Catino, 735 F.2d 718, 724 (2d Cir. 1984).

[1373] 18 U.S.C. 3238 (". . . or any one of two or more joint offenders. . .". United States v. Stickle, 454 F.3d 1265, 1272273 (11th Cir. 2006); United States v. Yousef, 327 F.3d. 56, 115 (2d Cir. 2003).

[1374] 28 U.S.C. 1783 ("A court of the United States may order the issuance of a subpoena requiring the appearance as a witness before it, or before a person or body designated by it, of a national or

authority to subpoena foreign nationals located in a foreign country.[1375] Mutual legal assistance treaties and similar agreements generally contain provisions to facilitate a transfer of custody for foreign witnesses who are imprisoned overseas[1376] and in other instances to elicit assistance to encourage foreign nationals to come to this country and testify voluntarily.[1377]

---

resident of the United States who is in a foreign country, or requiring the production of a specified document or other thing by him, if the court finds that particular testimony or the production of the document or other thing by him is necessary in the interest of justice, and, in other than a criminal action or proceeding, if the court finds, in addition, that it is not possible to obtain his testimony in admissible form without his personal appearance or to obtain the production of the document or other thing in any other manner"); Blackmer v. United States, 284 U.S. 421, 436-38 (1932).

[1375] United States v. Abu Ali, 528 F.3d 210, 239 (4th Cir. 2008); United States v. Yates, 345 F.3d 1280, 1283 (11th Cir. 2003); United States v. Olafson, 213 F.3d 435, 441 (9th Cir. 2000); United States v. Groos, 616 F.Supp.2d 777, 791 (N.D.Ill. 2008); United States v. Ozsusamlar, 428 F.Supp.2d 161, 177 (S.D.N.Y. 2006); cf., United States v. Liner, 435 F.3d 920, 924 (8th Cir. 2006). Cases where the witness is in federal custody overseas may prove an exception to the rule, but they may also come with their own special complications, see e.g., United States v. Moussaoui, 382 F.3d 453 (4th Cir. 2004)(foreign nationals held in military custody overseas whom the government, in the interest of national security, declined to make available for depositions or to appear as witnesses in a criminal trial).

[1376] E.g., Treaty on Mutual Legal Assistance in Criminal Matters, U.S.-Leich., Art. 11, S.Treaty Doc. 107-16 ("1. A person in the custody of the Requested State whose presence outside of the Requested State is sought for purposes of assistance under this Treaty shall be transferred form the Requested State for that purpose if the person consents and if the Central Authorities of both States agree. . . 3. For purposes of this Article: a) the receiving State shall have the authority and the obligation to keep the person transferred in custody unless otherwise authorized by the sending State; b) the receiving State shall return the person transferred to the custody of the sending State as soon as circumstances permit or as otherwise agreed by both Central Authorities; c) the receiving state shall not require the sending State to initiate extradition proceedings for the return of the person transferred; d) the person transferred shall receive credit for service of the sentence imposed in the sending State for time served in the custody of the receiving State; and e) where the receiving State is a third State the Requesting State shall be responsible for all arrangements necessary to meet the requirements of this paragraph"); see also, Treaty on Mutual Legal Assistance in Criminal Matters, U.S.-Ukr., Art. 11, S.Treaty Doc. 106-16; Treaty on Mutual Legal Assistance in Criminal Matters, U.S.-Fr., Art. 18, S.Treaty Doc. 10617; Treaty on Mutual Legal Assistance in Criminal Matters, U.S.-Greece, Art. 11, S.Treaty Doc. 106-18.

[1377] E.g., Treaty on Mutual Legal Assistance in Criminal Matters, U.S.-Belize, Art. 10, S.Treaty Doc. 106-19 ("1. When the Requesting State requests the appearance of a person in that State, the Requested State shall invite the person to appear before the appropriate authority in the Requesting State. The Requesting State shall indicate the extent to which the expenses will be paid. The Central Authority of the Requested State shall promptly inform the Central Authority of the Requesting State of the response of the person. 2. The Central Authority of the Requesting state shall inform the Central Authority of the requested State whether a decision has been made by the competent authorities of the Requesting State that a person appearing in the Requesting State pursuant to this article shall not be subject to service of process, or be detained or subject to any restriction of personal liberty, by reason of any acts or convictions which preceded his departure from the Requested State"); see also, Treaty on Mutual Legal Assistance in Criminal Matters, U.S.-Liech., Art. 10, S.Treaty Doc. 107-16 (person may not be served or detained except as stated in the request); Treaty on Mutual Legal Assistance in Criminal Matters, U.S.-Venez.,

Unable to secure the presence of overseas witnesses, federal courts may authorize depositions to be taken abroad, under "exceptional circumstances and in the interests of justice"[1378] under even more limited circumstances, they may admit such depositions into evidence in a criminal trial.

Originally, only a defendant might request that depositions be taken under Rule 15 of the Federal Rules of Criminal Procedure, [1379] but they have been available to prosecutors since the 1970s.[1380] The Rule offers depositions as an alternative to long term incarceration of material witnesses.[1381] Otherwise, depositions may be ordered only under exceptional circumstances. Some courts have said that to "establish exceptional circumstances the moving party must show the witness's unavailability and the materiality of the witness's testimony."[1382] Others would add to these that "the testimony is necessary to prevent a failure of justice" or additional considerations.[1383] In any event, once a deposition has been taken the impediments to its use at trial, especially by the prosecution, are much more formidable.

Arts. X, S.Treaty Doc. 105-38. When a witness is found in a country with whom the United Statesd has no such treaty, officials have used U.S. immigration parole authority in an effort to accomplish the same results, see e.g., Wang v. Reno, 81 F.3d 808, 811-12 (9th Cir. 1996).

[1378] F.R.Crim.P. 15(a)(1)("A party may move that a prospective witness be deposed in order to preserve testimony for trial. The court may grant the motion because of exceptional circumstances and in the interest of justice. If the court orders the deposition to be taken, it may also require the deponent to produce at the deposition any designated material that is not privileged, including any book, paper, document, record, recording, or data").

[1379] F.R.Crim.P. 15(a), 18 U.S.C.App. (1964 ed.). For a history of the evolution of Rule 15 see, 2 WRIGHT, FEDERAL PRACTICE AND PROCEDURE §251 (Crim. 3d 2000).

[1380] F.R.Crim.P. 15(a), 18 U.S.C.App. (1976 ed.); see also 18 U.S.C. 3503 (1970 ed.).

[1381] "A witness who is detained under 18 U.S.C. § 3144 may request to be deposed by filing a written motion and giving notice to the parties. The court may then order that the deposition be taken and may discharge the witness after the witness has signed under oath the deposition transcript," F.R.Crim.P. 15(a)(2).

[1382] United States v. Liner, 435 F.3d 920, 924 (8th Cir. 2006); see also, United States v. Kelley, 36 F.3d 1118, 1125 (D.C. Cir. 1994)(identifying the two as "critical factors"); United States v. Jefferson, 594 F.Supp.2d 655, 664 (E.D.Va. 2009).

[1383] United States v. Cohen, 260 F.3d 68, 78 (2d Cir. 2001); see also, United States v. Ruiz-Castro, 92 F.3d 1519, 1533 (10th Cir. 1996)(identifying the three factors as among those a court should consider before authorizing depositions); United States v. Thomas, 62 F.3d 1332, 1341 (11th Cir. 1995)(listing consideration of unavailability, materiality, and "countervailing factors [that] would make the deposition unjust to the nonmoving party"); United States v. Aggarwal, 17 F.3d 737, 742 (5th Cir. 1994)(denial of the motion may be based entirely upon the fact it is untimely); United States v. Jefferson, 594 F.Supp.2d at 664-65 (failure of justice and all the circumstances).

"Compliance with Rule 15 is a necessary but not sufficient condition for use of a deposition at trial."[1384] Admissibility at trial requires compliance with Rule 15, the Federal Rules of Evidence, and the Constitution's confrontation clause. As general matter, depositions are to be taken in the same manner as depositions in civil cases.[1385] Moreover, the Rule requires that the defendant be afforded an opportunity to attend depositions taken at the government's request.[1386] The requirement reflects the demands of the Constitution's confrontation clause: "In all criminal prosecutions, the accused shall enjoy the right . . . to be confronted with the witnesses against him," U.S. Const. Amend. VI. The right embodies not only the prerogative of a literal face to face confrontation, but also the right to cross examine and to have the witness's testimonial demeanor exposed to the jury.[1387]

[1384] United States v. McKeeve, 131 F.3d 1, 8 (1st Cir. 1997).

[1385] "(e) Unless these rules or a court order provides otherwise, a deposition must be taken and filed in the same manner as a deposition in a civil action, except that (1) A defendant may not be deposed without that defendant's consent. (2) The scope and manner of the deposition examination and cross-examination must be the same as would be allowed during trial. (3) The government must provide to the defendant or the defendant's attorney, for use at the deposition, any statement of the deponent in the government's possession to which the defendant would be entitled at trial.

"(f) A party may use all or part of a deposition as provided by the Federal Rules of Evidence.

"(g) A party objecting to deposition testimony or evidence must state the grounds for the objection during the deposition, F.R.Crim.P. 15(e),(f),(g)(captions omitted).

[1386] "(1) The officer who has custody of the defendant must produce the defendant at the deposition and keep the defendant in the witness's presence during the examination, unless the defendant: (A) waives in writing the right to be present; or (B) persists in disruptive conduct justifying exclusion after being warned by the court that disruptive conduct will result in the defendant's exclusion. (2) A defendant who is not in custody has the right upon request to be present at the deposition, subject to any conditions imposed by the court. If the government tenders the defendant's expenses as provided in Rule 15(d) but the defendant still fails to appear, the defendant – absent good cause – waives both the right to appear and any objection to the taking and use of the deposition based on that right," F.R.Crim.P. 15(c)(captions omitted).

"If the deposition was requested by the government, the court may – or if the defendant is unable to bear the deposition expenses, the court must – order the government to pay: (1) any reasonable travel and subsistence expenses of the defendant and the defendant's attorney to attend the deposition; and (2) the costs of the deposition transcript,"F.R.Crim.P. 15(d)(captions omitted).

[1387] Barber v. Page, 390 U.S. 719, 725 (1968)("The right to confrontation is basically a trial right. It includes both the opportunity to cross-examine and the occasion for the jury to weigh the demeanor of the witness").

In the case of depositions taken overseas, the courts have observed that the right to confrontation is not absolute.[1388] When a deposition is taken abroad, the courts prefer that the defendant be present,[1389] that his counsel be allowed to cross-examine the witness,[1390] that the deposition be taken under oath,[1391] that a verbatim transcript be taken, and that the deposition be captured on videotape;[1392] but they have permitted depositions to be admitted into evidence at

---

[1388] United States v. McKeeve, 131 U.S. 1, 8 (1st Cir. 1997); United States v. Medjuck, 156 F.3d 916, 920 (9th Cir. 1998); United States v. Abu Ali, 528 F.3d 210, 240 (4th Cir. 2008).

[1389] United States v. McKeeve, 131 U.S. 1, 8 (1st Cir. 1997)("the confrontation clause requires, at a minimum, that the government undertake diligent efforts to facilitate the defendant's presence. We caution, however, that although such efforts must be undertaken in good faith, they need not be heroic); United States v. Kelly, 892 F.2d 255, 262 (3d Cir. 1989); United States v. Salim, 855 F.2d 944, 950 (2d Cir. 1988).

[1390] United States v. Johnpoll, 739 F.2d 702, 710 (2d Cir. 1984)("The confrontation clause does not preclude admission of prior testimony of an unavailable witness, provided his unavailability is shown and the defendant had an opportunity to cross-examine. In the present case, Johnpoll had the full opportunity, at government expense, with his attorney to confront and cross-examine the Swiss witness, which he waived when he and his attorney decided not to attend the taking of the depositions").

[1391] United States v. Sines, 761 F.2d 1434, 1441 (9th Cir. 1985)("The Supreme Court has identified the major purposes of the confrontation clause as: (1) ensuring that witnesses will testify under oath; (2) forcing witnesses to undergo cross-examination; and (3) permitting the jury to observe the demeanor of witnesses. All three of these purposes were fulfilled when Steneman's videotaped deposition was taken [in Thailand] with Sine's attorney present").

[1392] United States v. Medjuck, 156 F.3d 916, 920 (9th Cir. 1998)("When the government is unable to secure a witness's presence at trial, Rule 15 is not violated by admission of videotaped testimony so long as the government makes diligent efforts to secure the defendant's physical presence at the deposition, and failing this, employs procedures that are adequate to allow the defendant to take an active role in the deposition proceedings. . . The government was unable to secure Medjuck's presence at the Canadian depositions because there was no mechanism in place to allow United States officials to transfer Medjuck to Canadian authorities. . . and secure his return to the United States in a timely fashion after the depositions. Finally, the government set up an elaborate system to allow Medjuck to witness the depositions live by video feed and to participate with his attorneys by private telephone connection during the depositions taken in Canada. . . .[A]n exception to the confrontation requirements] has been recognized for admission of deposition testimony where a witness is unavailable to testify at trial . . . First, the deposition testimony must fall within an established exception to the hearsay rule. Second the deposition must be taken in compliance with law. Finally, the defendant must have had an opportunity to cross-examine the deposed witness "); United States v. Kelly, 892 F.2d 255, 260-62 (3d Cir. 1980); United States v. Walker, 1 F.3d 423, 429 (6th Cir. 1993); United States v. Mueller, 74 F.3d 1152, 1156-157 (11th Cir. 1996); see also, United States v. Salim, 855 F.2d 944, 950 (2d Cir. 1988)("In the context of the taking of a foreign deposition, we believe that so long as the prosecution makes diligent efforts . . . to attempt to secure the defendant's presence, preferably in person, but if necessary via some form of live broadcast, the refusal of the host government to permit the defendant to be present should not preclude the district court from ordering that the witness' testimony be preserved anyway. However, the district court should satisfy itself that defense counsel will be given an opportunity to cross-examine the witness in order to fulfill the

subsequent criminal trials in this country, notwithstanding the fact that one or more of these optimal conditions are not present.[1393] In some of those nations whose laws might not otherwise require or even permit depositions under conditions considered preferable under U.S. law, a treaty provision addresses the issue.[1394]

The Federal Rules of Evidence govern the admissibility of evidence in federal criminal trials. A deposition taken overseas that has survived Rule 15 and confrontation clause scrutiny is likely to be found admissible. The hearsay rule, Rule 802 which reflects the law's preference for evidence that is exposed to the adversarial process, poses the most obvious obstacle.[1395] The Rules, however, provide an explicit exception for depositions,[1396] one that has been applied to depositions taken overseas under the authority of Rule 15.[1397]

---

mandate of Rule 15(b) to ensure a likelihood that the deposition will not violate the confrontation clause").

[1393] United States v. Sturman, 951 F.2d 1466, 1480-481(6th Cir. 1992)("Swiss law forbids verbatim transcription so the summary method of establishing the record was the most effective legal method. All defense questions, with just one exception, were submitted to the witnesses so that objections and determinations on admissibility could be litigated later. Although the witnesses were not given an oath, defense conceded that each witness was told the penalties for giving false testimony. . . Depositions taken in foreign countries cannot at all times completely emulate the United States methods of obtaining testimony. Here all steps were taken to ensure the defendants' rights while respecting the legal rules established in a different country").

[1394] E.g., Treaty on Mutual Legal Assistance on Criminal Matters, U.S.-Fr., Art. 9(2), S.Treaty Doc. 106-17 ("The procedures specified in this paragraph and outlined in the request shall be carried out insofar as they are not contrary to the fundamental principles of a judicial proceeding in the Requested State. The Requested State, if the Requesting State requests, shall: (a) take the testimony of witnesses or experts under oath . . .; (b) allow a confrontation between a defendant, together with counsel, and a witness or expert whose testimony or evidence is taken for use against the defendant in a criminal prosecution in the Requesting State; (c) ask questions submitted by the Requesting State, including questions proposed by authorities of the Requesting State present at the execution of the request; (d) record or allow to be recorded the testimony, questioning, or confrontation; and (e) produce or allow to be produced a verbatim transcript of the proceeding in which the testimony, questioning, or confrontation occurs").

[1395] "Hearsay is not admissible except as provided by these rules and by other rules prescribed by the Supreme Court pursuant to statutory authority or by Act of Congress," F.R.Evid. Rule 802. "'Hearsay' is a statement, other than one made by the declarant while testifying at the trial or hearing, offered in evidence to prove the truth of the matter asserted," F.R.Evid. Rule 801(c).

[1396] "The following are not excluded by the hearsay rule if the declarant is unavailable as a witness: (1) Testimony given as a witness . . . in a deposition taken in compliance with law in the course of the same or another proceeding, if the party against whom the testimony is now offered. . . had an opportunity and similar motive to develop the testimony by direct, cross, or redirect examination," F.R.Evid. Rule 804(b)(2).

[1397] United States v. Medjuck, 156 F.3d 916, 921 (9th Cir. 1998); United States v. McKeeve, 131 F.3d 1, 10 (1st Cir. 1997); United States v. Kelly, 892 F.2d 255, 261-62 (3d Cir. 1990).

Yet the question of admissibility of overseas depositions rests ultimately upon whether the confrontation clause demands can be satisfied. The cases thus far have relied upon the Supreme Court's decisions either in Ohio v. Roberts[1398] or in Maryland v. Craig.[1399] Faced with the question of whether trial witnesses might testify remotely via a two-way video conference, Craig held that he confrontation clause's requirement of physical face-to-face confrontation between witness and defendant at trial can be excused under limited circumstances in light of "considerations of public policy and necessities of the case."[1400] Roberts dealt with the question of whether the admission of hearsay evidence violated the confrontation clause, and declared that as long as the hearsay evidence came within a "firmly rooted hearsay exception" its admission into evidence in a criminal trial constituted no breach of the clause.[1401]

More recent decisions might be thought to call into question any continued reliance on Roberts and Craig. At a minimum, the Supreme Court's Crawford v. Washington opinion repudiates the suggestion that Roberts permits anything less than actual confrontation in the case of "testimonial" hearsay, e.g., a formal statement to a government official, such as an affidavit or other pretrial statement.[1402] At least one appellate panel has concluded that the prosecution's need for critical evidence does not alone supply the kind of public policy considerations necessary to qualify for a Craig exception;[1403] but another has held that national security interests may suffice.[1404]

Since the pre-Crawford cases required a good faith effort to assure the defendant's attendance at overseas depositions, it might be argued that Crawford requires no adjustment in the area's jurisprudence. Moreover, the Eleventh Circuit en banc Craig analysis implied that it thought the use of overseas

---

[1398] United States v. McKeeve, 131 F.3d 1, 9 (1st Cir. 1997); United States v. Drogoul, 1 F.3d 1546, 1552 (11th Cir. 1993); United States v. Kelly, 892 F.2d 255, 261 (3d Cir. 1989); United States v. Salim, 855 F.2d 944, 954-55 (2d Cir. 1988).

[1399] United States v. Medjuck, 156 F.3d 916, 920-21 (9th Cir. 1998).

[1400] 497 U.S. 836, 848 (1990).

[1401] 448 U.S. 56, 66 (1980).

[1402] 541 U.S. 36, 68 (2004) ("Where nontestimonial hearsay is at issue, it is wholly consistent with the Framers' design to afford the states flexibility in their development of hearsay law – as does Roberts, and as would an approach that exempted such statements from confrontation clause scrutiny altogether. Where testimonial evidence is at issue, however, the Sixth Amendment demands what the common law required: unavailability and a prior opportunity for cross-examination").

[1403] United States v. Yates, 438 F.3d 1307, 1316 (11th Cir. 2006).

[1404] United States v. Abu Ali, 528 F.3d 210, 240-42 (4th Cir. 2008).

depositions at trial more compatible with the confrontation clause than the use of video trial testimony.[1405] In addition, the Fourth Circuit rejected a confrontation clause challenge where the circumstances satisfied the dual demands for a Craig exception: (1) denial of a face to face confrontation made necessary by important policy considerations, and (2) assurance of reliability in the form of an "oath, cross-examination, and observation of the witness' demeanor."[1406]

Admissibility of Foreign Documents

There is a statutory procedure designed to ease the evidentiary admission of foreign business records in federal courts, 18 U.S.C. 3505.[1407] The section covers "foreign record[s] of regularly conducted activity" in virtually any form, i.e., any "memorandum, report, record, or data compilation, in any form, of acts, events, conditions, opinions, or diagnoses, maintained in a foreign country," 18 U.S.C. 3505(c)(1). It exempts qualified business records from the operation of the hearsay rule in federal criminal proceedings[1408] and permits their authentication upon foreign certification.[1409] Finally, it establishes a procedure under which the

---

[1405] United States v. Yates, 438 F.3d 1307, 1316 (11th Cir. 2006) (emphasis added) ("The government's interest in presenting the fact-finding with crucial evidence is, of course, an important public policy. We hold , however, that, under the circumstances of this case (which include the availability of a Rule 15 deposition) , the prosecutor's need for the video conference testimony to make a case and to expeditiously resolve it are not the type of public policies that are important enough to outweigh the defendants' rights to confront their accusers face-to-face").

[1406] United States v. Abu Ali, 528 F.3d at 240-42. The Fourth Circuit distinguished Yates on the grounds that there the lower court had not considered alternative procedures under which face to face confrontation might have been possible and that there the crimes of conviction were different in kind and degree ("Whatever the merits in Yates, the defendants there were charged with mail fraud, conspiracy to commit money laundering, and drug-related offenses, crimes different in both kind and degree from those implicating the national security interests here [(conspiracy commit terrorist attacks on the United States)]," id. at 242 n.12.

[1407] "Under §3505, a foreign certification serves to authenticate the foreign records, and thus dispenses with the necessity of calling a live witness to establish authentication," United States v. Hagege, 437 F.3d 943, 957 (9th Cir. 2006).

[1408] "In a criminal proceeding in a court of the United States, a foreign record of regularly conducted activity, or a copy of such record, shall not be excluded as evidence by the hearsay rule if a foreign certification attests that – (A) such record was made, at or near the time of the occurrence of the matters set forth, by (or from information transmitted by) a person with knowledge of those matters; (B) such record was kept in the course of a regularly conducted business activity; (C) the business activity made such a record as a regular practice; and (D) if such record is not the original, such record is a duplicate of the original [–] unless the source of information or the method or circumstances of preparation indicate [a] lack of trustworthiness," 18 U.S.C. 3505(a)(1).

[1409] "A foreign certification under this section shall authenticate such record or duplicate," 18 U.S.C. 3505(a)(2). "Foreign certification" is "a written declaration made and signed in a foreign country by the custodian of a foreign record of regularly conducted activity or another qualified

reliability of the documents can be challenged in conjunction with other pre-trial motions.[1410] While the prosecution's failure to provide timely notice of its intent to rely upon section 3505 does not necessarily bar admission,[1411] its failure to supply a foreign certification of authenticity precludes admission under the section.[1412]

Early appellate decisions upheld section 3505 in the face of confrontation clause challenges, as in the case of depositions drawing support from Ohio v. Roberts.[1413] As noted above, Crawford cast doubt upon the continued vitality of the Roberts rule (hearsay poses no confrontation problems as long as it falls within a "firmly rooted hearsay exception") when it held that only actual confrontation will suffice in the case of "testimonial" hearsay.[1414] Although it left for another day a more complete definition of testimonial hearsay, Crawford did note in passing that "[m]ost of the hearsay exceptions covered statements that by their nature were not testimonial – for example business records."[1415] At least one later appellate panel has rejected a confrontation clause challenge to section 3505 on the basis of this distinction.[1416]

---

person that, if falsely made, would subject the maker to criminal penalty under the laws of that country," 18 U.S.C. 3505(c)(2).

[1410] "At the arraignment or as soon after the arraignment as practicable, a party intending to offer in evidence under this section a foreign record of regularly conducted activity shall provide written notice of that intention to each other party. A motion opposing admission in evidence of such record shall be made by the opposing party and determined by the court before trial. Failure by a party to file such motion before trial shall constitute a waiver of objection to such record or duplicate, but the court for cause shown may grant relief from the waiver," 18 U.S.C. 3505(b).

[1411] United States v. Newell, 239 F.3d 917, 921 (7th Cir. 2001); United States v. Garcia Abrego, 141 F.3d 142, 176-78 (5th Cir. 1998). The court expressed "no opinion as to whether a showing of prejudice resulting from untimely notice of an intent to offer foreign records could eliminate §3505 as a potential pathway for admissibility of foreign business records," 141 F.3d at 178 n. 26.

[1412] United States v. Doyle, 130 F.3d 523, 546 (2d Cir. 1997).

[1413] United States v. Garcia Abrego, 141 F.3d 142, 178-79 (5th Cir. 1998); United States v. Ross, 33 F.3d 1507, 1517 (11th Cir. 1994); United States v. Sturman, 951 F.2d 1466, 1490 (6th Cir. 1991); United States v. Miller, 830 F.2d 1073, 1078 (9th Cir. 1987).

[1414] 541 U.S. 36, 68 (2004) ("Where nontestimonial hearsay is at issue, it is wholly consistent with the Framers' design to afford the states flexibility in their development of hearsay law – as does Roberts, and as would an approach that exempted such statements from confrontation clause scrutiny altogether. Where testimonial evidence is at issue, however, the Sixth Amendment demands what the common law required: unavailability and a prior opportunity for cross-examination").

[1415] 541 U.S. at 56.

[1416] United States v. Hagege, 437 F.3d 943, 957-58 (9th Cir. 2006); accord United States v. Qualls, 553 F.Supp.2d 241, 244-45 (E.D.N.Y. 2008).

Conclusion

The Constitution grants Congress broad powers to enact laws of extraterritorial scope and imposes few limitations on the exercise of that power. The states enjoy only residual authority, but they too may and have enacted criminal laws which apply beyond the territorial confines of the United States. Prosecutions are relatively few, however, perhaps because of the practical, legal, and diplomatic obstacles that may attend such an endeavor.

Attachments

Federal Criminal Laws Which Enjoy Express Extraterritorial Application

Special Maritime & Territorial Jurisdiction

8 U.S.C. 1375a(d)(3) (informed consent violations by international marriage brokers)

15 U.S.C. 1175 (manufacture or possession of gambling devices)

15 U.S.C. 1243 (manufacture or possession of switchblade knives)

15 U.S.C. 1245 (manufacture or possession of ballistic knives)

16 U.S.C. 3372(a)(3) (possession of illegally taken fish or wildlife)

18 U.S.C. 81 (arson)

18 U.S.C. 113 (assault)

18 U.S.C. 114 (maiming)

18 U.S.C. 117 (domestic assault by an habitual offender)

18 U.S.C. 546 (smuggling goods into a foreign country from an American vessel)

18 U.S.C. 661 (theft)

18 U.S.C. 662 (receipt of stolen property)

18 U.S.C. 831 (threats, theft, or unlawful possession of nuclear material or attempting or conspiring to do so)

18 U.S.C. 1025 (false pretenses)

18 U.S.C. 1081 - 1083 (gambling ships)

18 U.S.C. 1111 (murder)

18 U.S.C. 1112 (manslaughter)

18 U.S.C. 1113 (attempted murder or manslaughter)

18 U.S.C. 1115 (misconduct or neglect by ship officers)

18 U.S.C. 1201 (kidnaping)

18 U.S.C. 1363 (malicious mischief)

18 U.S.C. 1460 (sale or possession with intent to sell obscene material)

18 U.S.C. 1466A (obscene visual representation of sexual abuse of children)

18 U.S.C. 1587 (captain of a slave vessel with slaves aboard)

18 U.S.C. 1591(sex trafficking of children)

18 U.S.C. 1656 (piratical conversion of vessel by captain, officer or crew member)

18 U.S.C. 1658 (plundering a ship in distress)

18 U.S.C. 1659 (attack upon a vessel with intent to plunder)

18 U.S.C. 1654 (Americans arming or serving on privateers outside the United States to be used against the United States or Americans)

18 U.S.C. 1801 (video voyeurism)

18 U.S.C. 1957 (prohibited monetary transactions)

18 U.S.C. 2111 (robbery)

18 U.S.C. 2191 (cruelty to seamen)

18 U.S.C. 2192 (incite to revolt or mutiny)

18 U.S.C. 2193 (revolt or mutiny by seamen)

18 U.S.C. 2194 (shanghaiing sailors)

18 U.S.C. 2195 (abandonment of sailors overseas)

18 U.S.C. 2196 (drunkenness of seamen)

18 U.S.C. 2197 (misuse of documents associated vessels)

18 U.S.C. 2198 (seduction of a female passenger)

18 U.S.C. 2199 (stowaways)

18 U.S.C. 2241 (aggravated sexual abuse)

18 U.S.C. 2242 (sexual abuse)

18 U.S.C. 2243 (sexual abuse of a minor or ward)

18 U.S.C. 2244 (abusive sexual contact)

18 U.S.C. 2252(a) (sale or possession of material involving sexual exploitation of children)

18 U.S.C. 2252A(a) (sale or possession of child pornography)

18 U.S.C. 2261A (stalking)

18 U.S.C. 2271-2279 (destruction of ships)

18 U.S.C. 2283 (transportation of explosives, biological, chemical, radioactive or nuclear materials for terrorist purposes on the high seas or aboard a U.S. vessel or in U.S. waters)

18 U.S.C. 2284 (transportation of a terrorist on the high seas or aboard a U.S. vessel or in U.S. waters)

18 U.S.C. 2318 (transporting counterfeit phonorecord labels, copies of computer programs or documentation, or copies of motion pictures or other audio visual works)

18 U.S.C. 2332b (acts of terrorism transcending national boundaries)

18 U.S.C. 2388 (war-time activities affecting armed forces)

18 U.S.C. 2422(b) (causing a minor to engage in prostitution or other sexual acts)

18 U.S.C. 2425 (transmission of information about a minor)

18 U.S.C. 3261(offenses committed by members of the United States armed forces or individuals accompanying or employed by the United States armed forces overseas)

46 U.S.C. App. 1903 (maritime drug law enforcement)

48 U.S.C. 1912 (offenses committed on United States defense sites in the Marshall Islands or Federated States of Micronesia)

48 U.S.C.1934 (offenses committed on United States defense sites in Palau)

Special Aircraft Jurisdiction

18 U.S.C. 32 (destruction of aircraft)

18 U.S.C. 831 (threats, theft, or unlawful possession of nuclear material or attempting or conspiring to do so)

18 U.S.C. 1201 (kidnaping)

18 U.S.C. 2318 (transporting counterfeit phonorecord labels, copies of computer programs or documentation, or copies of motion pictures or other audio visual works)

49 U.S.C. 46502(a) (air piracy or attempted air piracy)

49 U.S.C. 46504 (interference with flight crew or attendants within the special aircraft jurisdiction of the United States)

49 U.S.C. 46506 (assaults, maiming, theft, receipt of stolen property, murder, manslaughter, attempted murder or manslaughter, robbery, or sexual abuse)

Treaty-Related

18 U.S.C. 32(b)
Offenses:
- violence aboard a foreign civil aircraft (likely to endanger the safety of the aircraft) while in flight;
- destruction of or incapacitating or endangering damage to foreign civil aircraft;
- placing a bomb aboard a foreign civil aircraft; or
- attempting or conspiring to do so

Jurisdictional factors:
- a United States national was on board;
- the offender was a United States national; or
- the offender is afterwards found in the United States

18 U.S.C. 37

Offenses:

- violence causing or likely to cause serious bodily injury or death at an international airport;
- destruction of or serious damage to aircraft or facilities at an international airport; or
- attempting or conspiring to do so

Jurisdictional factors:

- a victim was a United States national;
- the offender was a United States national; or
- the offender is afterwards found in the United States

18 U.S.C. 112

Offenses:

- assaulting an internationally protected person;
- threatening an internationally protected person; or
- attempting to threaten an internationally protected person

Jurisdictional factors:

- the victim was a United States national;
- the offender was a United States national; or
- the offender is afterwards found in the United States

18 U.S.C. 175

Offenses:

- develop, produce, stockpile, transfer, acquire, retain, or possess biological weapons or delivery systems, misuse of biological weapons;
- assisting a foreign power to do so; or
- attempting, threatening or conspiring to do so
- Jurisdictional factor:
- "there is extraterritorial Federal jurisdiction over an offense under this section committed by or against a national of the United States," 18 U.S.C. 175(a)

18 U.S.C. 229

Offenses:

- using chemical weapons outside the United States; or
- attempting, or conspiring to do so

Jurisdictional factors:

- the victim or offender was a United States national; or
- the offense was committed against federal property

18 U.S.C. 831

Offenses:

- threats, theft, or unlawful possession of nuclear material; or
- attempting or conspiring to do so

Jurisdictional factors:

- a United States national or an American legal entity was the victim of the offense;
- the offender was a United States national or an American legal entity; or
- the offender is afterwards found in the United States;
- the offense involved a transfer to or from the United States; or
- the offense was a threat directed against the United States

18 U.S.C. 878

Offenses:

- threatening to assault, kill or kidnap an internationally protected person

Jurisdictional factors:

- the victim was a United States national;
- the offender was a United States national; or
- the offender is afterwards found in the United States

18 U.S.C. 1091

Offense: genocide

- killing members of a national, ethnic, racial or religious group
- assaulting members of a national, ethnic, racial or religious group
- imposing reproductive and other group destructive measures on a national, ethnic, racial or religious group
- forcibly transferring children of a national, ethnic, racial or religious group

Jurisdictional factors:

- the offender was a United States national
- the offender is a stateless person habitually residing in the United States
- the offender is present in the United States
- the offense occurred in part in the United States

18 U.S.C. 1116

Offense: killing an internationally protected person

Jurisdictional factors:

- the victim was a United States national;
- the offender was a United States national; or
- the offender is afterwards found in the United States

18 U.S.C. 1117

Offense: conspiracy to kill an internationally protected person

Jurisdictional factors:

- the victim was a United States national;

- the offender was a United States national; or
- the offender is afterwards found in the United States

18 U.S.C. 1201
Offense:
- kidnaping an internationally protected person; or
- attempting or conspiring to do so

Jurisdictional factors:
- the victim was a United States national;
- the offender was a United States national; or
- the offender is afterwards found in the United States

18 U.S.C. 1203
Offense:
- -hostage taking; or
- attempting or conspiring to do so

Jurisdictional factors:
- the victim was a United States national;
- the offender was a United States national; or
- the offender is afterwards found in the United States

18 U.S.C. 2280
Offenses:
- violence committed against maritime navigation; or
- attempting or conspiracy to commit violence against maritime navigation

Jurisdictional factors:
- the victim was a United States national;
- the offender was a United States national;
- the offender is afterwards found in the United States; or
- the offense was intended to compel action or abstention by the United States

18 U.S.C. 2281
Offenses:
- violence committed against a maritime platform; or
- attempting or conspiracy to commit violence against a maritime platform

Jurisdictional factors:
- the victim was a United States national;
- the offender was a United States national;
- the offender is afterwards found in the United States; or
- the offense was intended to compel action or abstention by the United States

18 U.S.C. 2332a

Offenses:

- using a weapon of mass destruction outside the United States; or
- threatening, attempting, or conspiring to do so

Jurisdictional factors:

- the victim was a United States national;
- the offender was a United States national; or
- the offense was committed against federal property

18 U.S.C. 2332f (effective upon the terrorist bombing convention entering into force for the U.S.)

Offenses:

- bombing public places, government facilities, or public utilities outside the United States; or
- threatening, attempting, or conspiring to do so

Jurisdictional factors:

- the victim was a United States national;
- the offender was a United States national;
- the offense was committed against federal property;
- the offender is present in the United States;
- the offense was committed on United States registered vessel or aircraft; or
- the offense was intended to compel action or abstention by the United States

18 U.S.C. 2339C

Offenses:

- financing terrorism outside the U.S.; or
- attempting or conspiring to do so

Jurisdictional factors:

- predicate act of terrorism was directed against
    - United States property,
    - United States nationals or their property, or
    - property of entities organized under United States law;
- offense was committed on United States registered vessel or aircraft operated by the United States.;
- the offense was intended to compel action or abstention by the United States;
- the offender was a United States national; or
- (effective upon the terrorism financing convention entering into force for the U.S.) the offender is present in the United States

18 U.S.C. 2340A

Offenses:

- torture under color of law outside the United States; or
- attempted torture

Jurisdictional factors:

- the offender was a United States national; or
- the offender is present in the United States

18 U.S.C. 2441

Offense:

- war crimes

Jurisdictional factors:

- an American or member of the American armed forces was the victim of the offense; or
- the offender was an American or member of the American armed forces

49 U.S.C. 46502(b)

Offenses:

- air piracy outside the special aircraft jurisdiction of the United States; or
- attempted air piracy outside the special aircraft jurisdiction of the United States

Jurisdictional factors:

- a United States national was aboard;
- the offender was a United States national; or
- the offender is afterwards found in the United States

Others

18 U.S.C. 175c (variola virus (small pox))

Jurisdictional factors:

- the offender or victim was a United States national;
- the offense occurred in or affected interstate or foreign commerce
- the offense was committed against U.S. property; or
- the offender aided or abetted the commission of an offense under the section for which there was extraterritorial jurisdiction

Attempt/conspiracy

- includes attempts and conspiracies

18 U.S.C. 351

Offenses:

- killing, kidnaping, attempting or conspiring to kill or kidnap, or assaulting a Member of Congress, a Supreme Court Justice, or senior executive branch official

- Jurisdictional factors:
- "[t]here is extraterritorial jurisdiction over an offense prohibited by this section," 18 U.S.C. 351(i)

18 U.S.C. 877 (mailing threatening communications to the United States from foreign countries)

18 U.S.C. 956 (conspiracy and overt act within the United States to commit murder, kidnaping, maiming or the destruction of certain property overseas)

18 U.S.C. 1029
Offenses:
- fraud related to access devices; or
- attempting or conspiring to commit the offense

Jurisdictional factors:
- involves a device issued, managed or controlled by an entity within the jurisdiction of the United States and
- item used in the offense or proceeds are transported or transmitted to or through the United States or deposited here, 18 U.S.C. 1029(h)

18 U.S.C. 1119 (killing of American by an American in a foreign country)

18 U.S.C. 1204 (parental kidnaping by retaining a child outside the United States)

18 U.S.C. 1512
Offenses:
- tampering with a federal witness or informant; or
- attempting to tamper with a federal witness or informant

Jurisdictional factors:
- "[t]here is extraterritorial Federal jurisdiction over an offense under this section," 18 U.S.C. 1512(g)

18 U.S.C. 1513
Offenses:
- -retaliating against a federal witness or informant; or
- attempting to retaliate against a federal witness or informant

Jurisdictional factors:
- "[t]here is extraterritorial Federal jurisdiction over an offense under this section," 18 U.S.C. 1513(d)

18 U.S.C. 1585 (service aboard a slave vessel by an American or American resident)

18 U.S.C. 1586 (service aboard a vessel transporting slaves from one foreign country to another by an American or American resident)

18 U.S.C. 1587 (captain of a slave vessel hovering off the coast of the United States)

18 U.S.C. 1651 (piracy upon the high seas where the offender is afterwards brought into or found in the United States)

18 U.S.C. 1652 (Americans acting as privateers against the United States or Americans on the high seas)

18 U.S.C. 1653 (acts of piracy upon the high seas committed against the United States or Americans by aliens)

18 U.S.C. 1654 (Americans arming or serving on privateers outside the United States to be used against the United States or Americans)

18 U.S.C. 1751
Offenses:
- killing, kidnaping, attempting or conspiring to kill or kidnap, or assaulting the President, Vice President, or a senior White House official

Jurisdictional factors:
- "[t]here is extraterritorial jurisdiction over an offense prohibited by this section," 18 U.S.C. 1751(k)

18 U.S.C. 1831-1839
Offenses:
- economic espionage;
- theft of trade secrets

Jurisdictional factors:
- "[t]his chapter also applies to conduct occurring outside the United States if"
    - (1) the offender was a United States national or entity organized under United States law; or
    - (2) an act in furtherance was committed here, 18 U.S.C. 1837

18 U.S.C. 1956
Offense:

- money laundering

Jurisdictional factors:

- "[t]here is extraterritorial jurisdiction over the conduct prohibited by this section if
    - the conduct is by a United States citizen or, in the case of a non-United States citizen, the conduct occurs in part in the United States; and
    - the transaction or series of related transactions involves funds. . . of a value exceeding $10,000," 18 U.S.C. 1956(f)

18 U.S.C. 1957

Offense:

- prohibited monetary transactions

Jurisdictional factors:

- the offense under this section takes place outside the United States, but the defendant is a United States person [other than a federal employee or contractor who is the victim of terrorism]," 18 U.S.C. 1957(d)

18 U.S.C. 1992 (attacks on railroad and mass transit systems engaged in interstate or foreign commerce)

18 U.S.C. 2151 - 2157 (sabotage) (definitions afford protection for armed forces of the United States and "any associate nation" and for things transported "either within the limits of the United States or upon the high seas or elsewhere," 18 U.S.C. 2151)

18 U.S.C. 2260 (production of sexually explicit depictions of children outside the United States with the intent to import into the United States)

18 U.S.C. 2290

Offenses:

- destruction of vessels or maritime facilities (18 U.S.C. 2291);
- attempting or conspiring to do so (18 U.S.C. 2291); or
- imparting or conveying false information (18 U.S.C. 2292)

Jurisdictional factors:

- victim or offender was a U.S. national;
- U.S. national was aboard victim vessel;
- victim vessel was a U.S. vessel

Attempt/conspiracy

- includes attempts and conspiracies

18 U.S.C. 2332 (killing, attempting or conspiring to kill, or assaulting Americans overseas) (prosecution upon Department of Justice certification of terrorist intent)

18 U.S.C. 2332b
Offenses:
- -terrorist acts transcending national boundaries; or
- attempting or conspiring to do so

Jurisdictional factors:
- use of U.S. mail or other facility of United States foreign commerce;
- affects foreign commerce of the United States;
- victim was federal officer or employee or United States government; or
- the offenses was committed within the special maritime or territorial jurisdiction of the United States

18 U.S.C. 2339B
Offenses:
- providing material support or resources to designated terrorist organizations by one "subject to the jurisdiction of the United States;" or
- attempting or conspiring to do so

Jurisdictional factors:
- "[t]here is extraterritorial jurisdiction over an offense under this section," 18 U.S.C. 2339B(d)

18 U.S.C. 2339D (receipt of military training from a foreign terrorist organization)
Jurisdictional factors:
- the offender was a United States national;
- the offender was habitual resident of the United States;
- the offender is present in the United States;
- the offense was committed in part in the United States;
- the offense occurred in or affected interstate or foreign commerce; or
- the offender aided or abetted a violation of the section over which extraterritorial jurisdiction exists

18 U.S.C. 2381 (treason) ("within the United States or elsewhere")

18 U.S.C. 2423 (U.S. citizen or resident alien traveling overseas with the intent to commit illicit sexual activity or traveling overseas and thereafter engaging in illicit sexual activity)

18 U.S.C. 2442 (recruitment or use of child soldiers)
Jurisdictional factors:
- the offender was a United States national

- the offender was a stateless person habitually residing in the United States
- the offender is present in the United States
- the offense occurred in part in the United States

18 U.S.C. 3271 (overseas trafficking in persons by those employed by or accompanying the United States)

21 U.S.C. 959
Offenses:
- manufacture, distribution or possession of illicit drugs for importation into the United States

Jurisdictional factors:
- "this section is intended to reach acts of manufacture or distribution committed outside the territorial
- jurisdiction of the United States. . . ." 21 U.S.C. 959(c)

21 U.S.C. 960A (narco-terrorism)
Jurisdictional factors:
- the offense was a U.S. drug or terrorism offense;
- the offender provided pecuniary value for terrorist offense to injure a U.S. national or damage U.S. property outside the United States;
- the offense was committed in part in the United States and the offender is a U.S. national; or
- the offense occurred in or affected interstate or foreign commerce

46 U.S.C. App. 1903
Offenses:
- manufacture, distribution or possession of controlled substances on various vessels outside United States maritime jurisdiction

Jurisdictional factors:
- the vessel is a "vessel without nationality"; or
- the vessel is of foreign registry or located within foreign territorial waters and the foreign nation has consented to application of the United States law

Federal Crimes Subject to Federal Prosecution When Committed Overseas

Homicide

7 U.S.C. 2146 (killing federal animal transportation inspectors)*

8 U.S.C. 1324 (death resulting from smuggling aliens into the U.S.)*

15 U.S.C. 1825(a)(2)(C) (killing those enforcing the Horse Protection Act)*

18 U.S.C. 32 (death resulting from destruction of aircraft or their facilities)
Jurisdictional factors:
- aircraft was in the special aircraft jurisdiction of the United States;
- the victim or offender was a United States national; or
- the offender is found in the United States

Attempt/Conspiracy
- attempt and conspiracy are included

18 U.S.C. 33 (death resulting from destruction of motor vehicles or their facilities used in United States foreign commerce)

18 U.S.C. 37 (death resulting from violence at international airports)
Jurisdictional factors:
- a victim was a United States national;
- the offender was a United States national; or
- the offender is afterwards found in the United States

18 U.S.C. 38 (death resulting from fraud involving aircraft or space vehicle parts)
Jurisdictional factors:
- the victim or offender was an entity organized under United States law;
- the victim or offender was a United States national; or
- an act in furtherance of the offense was committed in the United States)

18 U.S.C. 43
Offense (where death results):
- travel to disrupt an animal enterprise;
- causing damages of over $10,000 to an animal enterprise; or
- conspiring to cause damages of over $10,000 to an animal enterprise

Jurisdictional factors:
- the offense involved travel in the foreign commerce of the United States; or
- the offense involved use of the mails or other facility in the foreign commerce of the United States

18 U.S.C. 115(a)(1)(A) (murder, attempted murder or conspiracy to murder of a family member of a United States officer, employee or judge with intent to impede or retaliate for performance of federal duties)*

18 U.S.C. 115(a)(1)(B) (murder, attempted murder or conspiracy to murder of a former United States officer, employee or judge or any member of their families in retaliation for performance of federal duties)*

18 U.S.C. 175 (death resulting from biological weapons offenses)
Jurisdictional factors:
- a victim was a United States national; or
- the offender was a United States national

18 U.S.C. 175c (variola virus (small pox))
Jurisdictional factors:
- the offender or victim was a United States national;
- the offense occurred in or affected interstate or foreign commerce;
- the offense was committed against U.S. property; or
- the offender aided or abetted the commission of an offense under the section for which there was extraterritorial jurisdiction

18 U.S.C. 229 (death resulting from chemical weapons offenses)
Jurisdictional factors:
- a victim was a United States national;
- the offender was a United States national; or
- committed against United States property

18 U.S.C. 351 (killing a Member of Congress, cabinet officer, or Supreme Court justice)
Attempt/conspiracy
- attempt and conspiracy are included

18 U.S.C. 794 (death resulting from disclosing the identify of an American agent to foreign powers)

18 U.S.C. 831
Offenses:
- unlawful possession of nuclear material where the offender causes the death of another; or
- attempting or conspiring to do so

Jurisdictional factors:

- the offense is committed within the special aircraft or special maritime and territorial jurisdiction of the United States;
- a United States national or an American legal entity was the victim of the offense;
- the offender was a United States national or an American legal entity;
- the offender is afterwards found in the United States;
- the offense involved a transfer to or from the United States; or
- the offense was a threat directed against the United States

18 U.S.C. 844(d) (death resulting from the unlawful transportation of explosives in United States foreign commerce)
Attempt/conspiracy
- attempt and conspiracy are included

18 U.S.C. 844(f) (death resulting from bombing federal property)*
Attempt/conspiracy
- attempt and conspiracy are included

18 U.S.C. 844(i) (death resulting from bombing property used in or used in an activity which affects United States foreign commerce)
Attempt/conspiracy
- attempt and conspiracy are included

18 U.S.C. 930 (killing or attempting to kill another during the course of possessing, introducing, or attempting to possess or introduce a firearm or other dangerous weapon in a federal facility)*

18 U.S.C. 956 (conspiracy and overt act within the United States to commit murder, kidnaping, maiming or the destruction of certain property overseas)

18 U.S.C. 1091 (genocide)
Jurisdictional factors:
- -the offender was a United States national
- the offender is a stateless person habitually residing in the United States
- the offender is present in the United States
- the offense occurred in part in the United States

18 U.S.C. 1111 (murder within the special maritime jurisdiction of the United States)

18 U.S.C. 1112 (manslaughter within the special maritime jurisdiction of the United States)

18 U.S.C. 1113 (attempted murder or manslaughter within the special maritime jurisdiction of the United States)

18 U.S.C. 1114 (murder of a federal employee, including a member of the United States military, or anyone assisting a federal employee or member of the United States military during the performance of (or on account of the performance of) official duties*

18 U.S.C. 1116 (killing an internationally protected person)
Jurisdictional factors:
- the victim was a United States national;
- the offender was a United States national; or
- the offender is afterwards found in the United States

18 U.S.C. 1117 (conspiracy to kill an internationally protected person)
Jurisdictional factors:
- the victim was a United States national;
- the offender was a United States national; or
- the offender is afterwards found in the United States

18 U.S.C. 1119 (a United States national killing or attempting to kill a United States national outside the United States)

18 U.S.C. 1120 (murder by a person who has previously escaped from a federal prison)*

18 U.S.C. 1121(a) (killing another who is assisting or because of the other's assistance in a federal criminal investigation or killing (because of official status) a state law enforcement officer assisting in a federal criminal investigation)*

18 U.S.C. 1201 (kidnaping where death results)
Jurisdictional factors:
- the victim is removed from the United States;
- the offense occurs within the special aircraft or special maritime and territorial jurisdiction of the United States;
- the victim is a federal officer or employee; or
- the victim is an internationally protected person and
    - the victim was a United States national;

- the offender was a United States national; or
- the offender is afterwards found in the United States

Attempt/conspiracy
- attempt and conspiracy are included

18 U.S.C. 1203 (hostage taking where death results)
Jurisdictional factors:
- the victim was a United States national;
- the offender was a United States national; or
- the offender is afterwards found in the United States
- Attempt/conspiracy attempt and conspiracy are included

18 U.S.C. 1347 (defrauding U.S. health care program where death results)*

18 U.S.C. 1365 (tampering with consumer products where death results (in the United States))*

18 U.S.C. 1503 (killing another to obstruct federal judicial proceedings)*
Attempt/conspiracy
- attempt is included

18 U.S.C. 1512 (tampering with a federal witness or informant where death results)
Jurisdictional factors:
- "[t]here is extraterritorial Federal jurisdiction over an offense under this section," 18 U.S.C.1512(g)

Attempt/conspiracy
- attempt is included

18 U.S.C. 1513 (retaliating against a federal witness or informant)
Jurisdictional factors:
- "[t]here is extraterritorial Federal jurisdiction over an offense under this section," 18 U.S.C.1513(d))

Attempt/conspiracy
- attempt is included

18 U.S.C. 1652 (murder of an American by an American on the high seas in the name of a foreign state or person)

18 U.S.C. 1751 (killing the President, Vice President, or a senior White House official)
Jurisdictional factors:

- "[t]here is extraterritorial jurisdiction over an offense prohibited by this section," 18 U.S.C.1751(k)

Attempt/conspiracy

- attempt and conspiracy are included

18 U.S.C. 1952 (U.S.-foreign travel or use of the mails or of a facility of U.S. foreign commerce in furtherance of a violation of federal arson laws)

18 U.S.C. 1958 (commission of murder for hire in violation of U.S. law where death results)

Jurisdictional factor

- use U.S. foreign travel facilities, or
- use of mails or U.S. foreign commerce facilities

Attempt/conspiracy

- includes conspiracy

18 U.S.C. 1992 (attacks on railroad and mass transit systems engaged in interstate or foreign commerce)

Attempt/conspiracy

- includes attempts and conspiracy

18 U.S.C. 2118 (killing resulting from a robbery or burglary involving controlled substances)

Jurisdictional factors

- offense involved
- travel in U.S. foreign commerce, or
- use of a facility in U.S. foreign commerce

Attempt/Conspiracy

- attempt and conspiracy prohibitions are included

18 U.S.C. 2119 (death resulting from carjacking)

Jurisdictional factors

- car transported, shipped or received in U.S. foreign commerce in the course of the offense

18 U.S.C. 2241, 2245 (aggravated sexual abuse within the special maritime and territorial jurisdiction of the United States where death results)

18 U.S.C. 2242, 2245 (sexual abuse within the special maritime and territorial jurisdiction of the United States where death results)

18 U.S.C. 2243, 2245 (sexual abuse of a minor or ward within the special maritime and territorial jurisdiction of the United States where death results)

18 U.S.C. 2244, 2245 (abusive sexual contact within the special maritime and territorial jurisdiction of the United States where death results)

18 U.S.C. 2261A (death resulting from interstate stalking violation involving use of the mails or a facility in U.S. foreign commerce)
Jurisdictional factors
- travel in U.S. maritime jurisdiction; or
- travel in U.S. foreign commerce

18 U.S.C. 2280 (a killing resulting from violence against maritime navigation)
Jurisdictional factors
- aboard a ship of American registry;
- committed by an American national aboard a ship of foreign registry or outside the U.S.;
- victim was an American;
- committed in the territorial waters of another country and the offender is subsequently found in the U.S.; or
- committed in an effort to compel federal action or abstention

18 U.S.C. 2281 (resulting from violence against fixed maritime platforms)
Jurisdictional factors
- aboard a platform on the U.S. continental shelf;
- committed by an American national aboard a platform on the continental shelf of another nation
- victim was an American;
- committed aboard a platform on the continental shelf of another nation and the offender is subsequently found in the U.S.; or
- committed in an effort to compel federal action or abstention

18 U.S.C. 2283 (transportation of explosives, biological, chemical, radioactive or nuclear materials for terrorist purposes on the high seas or aboard a U.S. vessel or in U.S. waters)

18 U.S.C. 2290
Offenses:
- destruction of vessels or maritime facilities (18 U.S.C. 2291); or
- attempting or conspiring to do so (18 U.S.C. 2291)

Jurisdictional factors:
- victim or offender was a U.S. national;

- U.S. national was aboard victim vessel; or
- victim vessel was a U.S. vessel

Attempt/conspiracy
- includes attempts and conspiracies

18 U.S.C. 2332 (killing an American overseas)

Jurisdictional factors
- prosecution only on DoJ certification "to coerce, intimidate, or retaliate against a government or civilian population"

Attempt/conspiracy
- includes attempts and conspiracies

18 U.S.C. 2332a (resulting from use of weapons of mass destruction)

Jurisdictional factors
- victim or offender is American; or
- against federal property

Attempt/conspiracy
- includes attempts and conspiracies

18 U.S.C. 2332f (resulting from bombing of public places, government facilities, public transportation systems or infrastructure facilities)(effective when the terrorist bombing treaty enters into force for the U.S.)

Jurisdictional factors
- victim or offender is American;
- aboard aircraft operated by the U.S.;
- aboard vessel of aircraft of U.S. registry;
- offender is found in the U.S.;
- committed to coerce U.S. action; or
- against federal property

Attempt/conspiracy
- includes attempts and conspiracies

18 U.S.C. 2340A (resulting from torture committed outside the U.S. (physical or mental pain inflicted under color of law upon a prisoner))

Jurisdictional factors
- American offender; or
- offender subsequently found within the U.S.

Attempt/conspiracy
- includes attempts

18 U.S.C. 2441 (war crimes)

Jurisdictional factors
- victim or offender is an American; or

- victim or offender is a member of U.S. armed forces

18 U.S.C. 3261 (offenses committed by members of the United States armed forces or individuals accompanying or employed by the United States armed forces overseas)

21 U.S.C. 461(c) (murder of federal poultry inspectors during or because of official duties)*

21 U.S.C. 675 (murder of federal meat inspectors during or because of official duties)*

21 U.S.C. 848(e)(1)(B) (killing a federal or state law enforcement official in furtherance of a federal drug felony)*

21 U.S.C. 1041(c) (murder of an egg inspector during or because of official duties)*

42 U.S.C. 2000e-13 (murder, manslaughter or attempted murder or manslaughter of EEOC personnel)*

42 U.S.C. 2283 (killing federal nuclear inspectors during or because of official duties)*

49 U.S.C. 46502 (air piracy where death results)

49 U.S.C. 46506 (murder, manslaughter, or attempted murder or manslaughter within the special aircraft jurisdiction of the United States)

Kidnaping

18 U.S.C. 115(a)(1)(A) (kidnaping, attempted kidnaping or conspiracy to kidnap a family member of a United States officer, employee or judge with intent to impede or retaliate for performance of federal duties)*

18 U.S.C. 115(a)(1)(B) (kidnaping, attempted kidnaping or conspiracy to kidnap a former United States officer, employee or judge or any member of their families in retaliation for performance of federal duties)*

18 U.S.C. 351 (kidnaping a Member of Congress, a Supreme Court Justice, or senior executive branch official)

Jurisdictional factors:

- "[t]here is extraterritorial jurisdiction over an offense prohibited by this section," 18 U.S.C.351(i)

Attempt/conspiracy

- includes attempts and conspiracies

18 U.S.C. 956 (conspiracy and overt act within the United States to commit murder, kidnaping, maiming or the destruction of certain property overseas)

18 U.S.C. 1091 (genocide)

- forcibly transferring children of a national, ethnic, racial or religious group

Jurisdictional factors:

- -the offender was a United States national
- the offender is a stateless person habitually residing in the United States
- the offender is present in the United States
- the offense occurred in part in the United States

18 U.S.C. 1201 (kidnaping)

Jurisdictional factors:

- the victim is removed from the United States;
- the offense occurs within the special aircraft or special maritime and territorial jurisdiction of the United States;
- the victim is a federal officer or employee; or
- the victim is an internationally protected person and
- the victim was a United States national;
- the offender was a United States national; or
- the offender is afterwards found in the United States

18 U.S.C. 1203 (hostage taking)

Jurisdictional factors:

- the victim was a United States national;
- the offender was a United States national; or
- the offender is afterwards found in the United States

Attempt/conspiracy

- includes attempts and conspiracies

18 U.S.C. 1204 (international parental kidnaping detaining a child outside of the United States in violation of parental custody rights)

18 U.S.C. 3261 (offenses committed by members of the United States armed forces or individuals accompanying or employed by the United States armed forces overseas)

Assault

7 U.S.C. 60 (assault designed to influence administration of federal cotton standards program)*

7 U.S.C. 87b (assault designed to influence administration of federal grain standards program)*

7 U.S.C. 473c-1 (assaults on cotton samplers to influence administration of federal cotton standards program)*

7 U.S.C. 511i (assaults designed to influence administration of federal tobacco inspection program)*

7 U.S.C. 2146 (assault of United States animal transportation inspectors)*
Jurisdictional factors:

- use of U.S. mail or other facility of United States foreign commerce;
- affects foreign commerce of the United States;
- victim was federal officer or employee or United States government; or
- the offenses was committed within the special maritime or territorial jurisdiction of the United States

15 U.S.C. 1825(a)(2)(C) (assaults on those enforcing the Horse Protection Act))*

16 U.S.C. 773e (assaults on officials responsible for enforcing the Northern Pacific Halibut Act)*

16 U.S.C. 973c (assaults on officials responsible for enforcing the South Pacific tuna conversation provisions)*

16 U.S.C. 1417 (assaults on officials conducting searches or inspections with respect to the global moratorium on tuna harvesting practices)*

16 U.S.C. 1436 (assaults on officials conducting searches or inspections with respect to the marine sanctuaries)*

16 U.S.C. 1857, 1859 (assaults on officials conducting searches or inspections with respect to the federal fisheries management and conservation program)*

16 U.S.C. 2403, 2408 (assaults on federal officials conducting searches or inspections on vessels subject to the jurisdiction of the United States with respect Antarctic conservation)*

16 U.S.C. 2435 (assaults on federal officials conducting searches or inspections on vessels subject to the jurisdiction of the United States in enforcement of the Antarctic Marine Living Resources Convention)*

16 U.S.C. 3637 (assaults on federal officials conducting searches or inspections on vessels subject to the jurisdiction of the United States with respect Pacific salmon conservation)*

16 U.S.C. 5009 (assaults on federal officials conducting searches or inspections on vessels subject to the jurisdiction of the United States with respect North Pacific anadromous stock conservation)*

16 U.S.C. 5505 (assaults on federal officials conducting searches or inspections on vessels subject to the jurisdiction of the United States with respect high seas fishing compliance)*

16 U.S.C. 5606 (assaults on federal officials conducting searches or inspections on vessels subject to the jurisdiction of the United States with respect Northwest Atlantic Fisheries Convention compliance)*

18 U.S.C. 37 (violence at international airports)
Jurisdictional factors:
- a victim was a United States national;
- the offender was a United States national; or
- the offender is afterwards found in the United States

Attempt/conspiracy
- includes attempts and conspiracies

18 U.S.C. 111 (assault on a federal officer or employee)*

18 U.S.C. 112 (assaulting an internationally protected person)
Jurisdictional factors:

- the victim was a United States national;
- the offender was a United States national; or
- the offender is afterwards found in the United States

18 U.S.C. 113 (assault within the special maritime and territorial jurisdiction of the United States)

18 U.S.C. 114 (maiming within the special maritime and territorial jurisdiction of the United States)

18 U.S.C. 115(a)(1)(A) (assaults a family member of a United States officer, employee or judge with intent to impede or retaliate for performance of federal duties)*

18 U.S.C. 115(a)(1)(B) (assaults a former United States officer, employee or judge or any member of their families in retaliation for performance of federal duties)*

18 U.S.C. 351 (assaulting a Member of Congress, a Supreme Court Justice, or senior executive branch official)
Jurisdictional factor:
- "[t]here is extraterritorial jurisdiction over an offense prohibited by this section," 18 U.S.C. 351(i)

18 U.S.C. 831
Offenses:
- unlawful use of nuclear material where the offender causes the serious injury to another; or
- attempting or conspiring to do so

Jurisdictional factors:
- the offense is committed within the special aircraft or special maritime and territorial jurisdiction of the United States;
- a United States national or an American legal entity was the victim of the offense;
- the offender was a United States national or an American legal entity;
- the offender is afterwards found in the United States;
- the offense involved a transfer to or from the United States; or
- the offense was a threat directed against the United States

18 U.S.C. 844(f) (burning or bombing federal property where serious injury results)*

18 U.S.C. 844(i) (burning or bombing property used in or used in activities affecting United States foreign commerce where serious injury results)

18 U.S.C. 956 (conspiracy and overt act within the United States to commit murder, kidnaping, maiming or the destruction of certain property overseas)

18 U.S.C. 1091 (genocide)

- assaulting members of a national, ethnic, racial or religious group
- forcibly transferring children of a national, ethnic, racial or religious group

Jurisdictional factors:

- -the offender was a United States national
- the offender is a stateless person habitually residing in the United States
- the offender is present in the United States
- the offense occurred in part in the United States

18 U.S.C. 1365 (tampering with consumer products resulting in injury (in the United States))*

18 U.S.C. 1501 (assault on a server of federal process)*

18 U.S.C. 1502 (assaulting a federal extradition agent)*

18 U.S.C. 1503 (assaulting another to obstruct federal judicial proceedings)*

18 U.S.C. 1512 (tampering with a federal witness or informant through the use of physical force)

Jurisdictional factors:

- "[t]here is extraterritorial Federal jurisdiction over an offense under this section," 18 U.S.C.1512(g)

Attempt/conspiracy

- attempt is included

*18 U.S.C. 1513**

Offenses (causing physical injury):

- -retaliating against a federal witness or informant; or
- attempting to retaliate against a federal witness or informant

Jurisdictional factors:

- "[t]here is extraterritorial Federal jurisdiction over an offense under this section," 18 U.S.C.1513(d))

18 U.S.C. 1655 (assaulting the commander of a vessel is piracy)

18 U.S.C. 1751 (assaulting the President, Vice President, or a senior White House official; "[t]here is extraterritorial jurisdiction over an offense prohibited by this section," 18 U.S.C. 1751(k))

*18 U.S.C. 2114 * (assault upon one in possession of the property of the United States)*

18 U.S.C. 2191 (cruelty to seamen within the special maritime jurisdiction of the United States)

18 U.S.C. 2194 (shanghaiing sailors for employment within the foreign commerce of the United States)

18 U.S.C. 2241 (aggravated sexual abuse within the special maritime and territorial jurisdiction of the United States)

18 U.S.C. 2242 (sexual abuse within the special maritime and territorial jurisdiction of the United States)

18 U.S.C. 2243 (sexual abuse of a minor or ward within the special maritime and territorial jurisdiction of the United States)

18 U.S.C. 2244 (abusive sexual contact within the special maritime and territorial jurisdiction of the United States)

18 U.S.C. 2261 (traveling or causing a spouse to travel in foreign commerce of the United States for purposes of domestic violence)

18 U.S.C. 2261A (stalking within the special maritime and territorial jurisdiction of the United States)

18 U.S.C. 2262 (traveling or causing a spouse to travel in foreign commerce of the United States for purposes violating protective order)

18 U.S.C. 2280
Offenses:

- violence committed against maritime navigation; or
- attempting or conspiracy to commit violence against maritime navigation

Jurisdictional factors:

- the victim was a United States national;
- the offender was a United States national;
- the offender is afterwards found in the United States; or
- the offense was intended to compel action or abstention by the United States

18 U.S.C. 2281

Offenses:

- violence committed against a maritime platform; or
- attempting or conspiracy to commit violence against a maritime platform

Jurisdictional factors:

- the victim was a United States national;
- the offender was a United States national;
- the offender is afterwards found in the United States; or
- the offense was intended to compel action or abstention by the United States

18 U.S.C. 2332 (assaulting a United States national outside the United States) (prosecution upon Department of Justice certification of terrorist intent)

18 U.S.C. 2332a

Offenses:

- using a weapon of mass destruction outside the United States resulting physical injury; or
- attempting or conspiring to do so

Jurisdictional factors:

- the victim was a United States national;
- the offender was a United States national; or
- the offense was committed against federal property

18 U.S.C. 2332b

Offenses:

- -terrorist assaults transcending national boundaries; or
- attempt or conspiracy

Jurisdictional factors:

- use of U.S. mail or other facility of United States foreign commerce;
- affects foreign commerce of the United States;
- victim was federal officer or employee or United States government; or
- the offenses was committed within the special maritime or territorial jurisdiction of the United States

18 U.S.C. 2340A
Offenses:
- torture under color of law outside the United States; or
- attempted torture

Jurisdictional factors:
- the offender was a United States national; or
- the offender is present in the United States

18 U.S.C. 3261 (offenses committed by members of the United States armed forces or individuals accompanying or employed by the United States armed forces overseas)

21 U.S.C. 461(c) (assaulting federal poultry inspectors)*

21 U.S.C. 675 (assaulting federal meat inspectors)*

21 U.S.C. 1041(c) (assaulting federal egg inspector)*

30 U.S.C. 1461 (assaults on officials conducting searches or inspections with respect to the Deep Seabed Hard Mineral Resources Act)*

42 U.S.C. 2000e-13 (assaulting EEOC personnel)*

42 U.S.C. 2283 (assaulting federal nuclear inspectors)*

46 U.S.C. 11501 (seaman's assault upon officers within the special maritime jurisdiction of the United States)

46 U.S.C. App. 46504 (assaulting officers enforcing regulations of vessels in domestic commerce)

49 U.S.C. 46504 (assaulting a flight crew member within the special aircraft jurisdiction of the United States)

49 U.S.C. 46506 (assaults within the special aircraft jurisdiction of the United States)

Property Destruction

18 U.S.C. 32 (destruction of aircraft or their facilities)
Jurisdictional factors:
- aircraft was in the special aircraft jurisdiction of the United States;
- the victim or offender was a United States national; or
- the offender is found in the United States

Attempt/Conspiracy
- attempt and conspiracy are included

18 U.S.C. 33 (destruction of motor vehicles or their facilities used in United States foreign commerce)

18 U.S.C. 37 (violence at international airports)
Jurisdictional factors:
- a victim was a United States national;
- the offender was a United States national; or
- the offender is afterwards found in the United States

18 U.S.C. 43
Offense:
- travel to disrupt an animal enterprise;
- causing damages of over $10,000 to an animal enterprise; or
- conspiring to cause damages of over $10,000 to an animal enterprise

Jurisdictional factors:
- the offense involved travel in the foreign commerce of the United States; or
- the offense involved use of the mails or other facility in the foreign commerce of the United States

18 U.S.C. 81 (arson within the special maritime and territorial jurisdiction of the United States)

18 U.S.C. 229 (chemical weapons damage)
Jurisdictional factors:
- a victim was a United States national;
- the offender was a United States national; or
- committed against United States property

18 U.S.C. 831 (use nuclear material of damage or destroy)
Jurisdictional factors:
- committed within the special aircraft or special maritime and territorial jurisdiction of the United States

- a United States national or an American legal entity was the victim of the offense;
- the offender was a United States national or an American legal entity;
- the offender is afterwards found in the United States; or
- the offense involved a transfer to or from the United States

18 U.S.C. 844(f) (burning or bombing federal property)*
Attempt/conspiracy
- attempt and conspiracy are included

18 U.S.C. 844(i) (burning or bombing property used in or used in an activity which affects United States foreign commerce)
Attempt/conspiracy
- attempt and conspiracy are included

18 U.S.C. 956 (conspiracy and overt act within the United States to commit murder, kidnaping, maiming or the destruction of certain property overseas)

18 U.S.C. 1030 (computer abuse involving damage to federal or U.S. financial systems or systems used in the foreign commerce or communications of the United States)

18 U.S.C. 1361 (destruction of federal property)*

18 U.S.C. 1362 (destruction of federal communications lines, stations or related property)*

18 U.S.C. 1363 (destruction of property within the special maritime and territorial jurisdiction of the United States)

18 U.S.C. 1992 (attacks on railroad and mass transit systems engaged in interstate or foreign commerce)

18 U.S.C. 2071 (destruction of federal records)*

18 U.S.C. 2153 (war-time destruction of defense materials of the United States or its allies)*

18 U.S.C. 2155 (destruction of federal national defense materials)*

18 U.S.C. 2272 (destruction of a vessel within the maritime jurisdiction of the United States by its owner)

18 U.S.C. 2273 (destruction of a vessel within the maritime jurisdiction of the United States by others)

18 U.S.C. 2275 (burning or tampering with a vessel within the maritime jurisdiction of the United States)

18 U.S.C. 2280 (destruction of maritime navigational facilities)
Jurisdictional factors:
- the offender was a United States national;
- the offender is afterwards found in the United States; or
- the offense was intended to compel action or abstention by the United States

18 U.S.C. 2281 (damage to a maritime platform)
Jurisdictional factors:
- the offender was a United States national;
- the offender is afterwards found in the United States; or
- the offense was intended to compel action or abstention by the United States

18 U.S.C. 2290
Offenses:
- destruction of vessels or maritime facilities (18 U.S.C. 2291); or
- attempting or conspiring to do so (18 U.S.C. 2291)

Jurisdictional factors:
- victim or offender was a U.S. national;
- U.S. national was aboard victim vessel;
- victim vessel was a U.S. vessel

18 U.S.C. 2332a (using a weapon of mass destruction)
Jurisdictional factors:
- the victim was a United States national;
- the offender was a United States national; or
- the offense was committed against federal property

18 U.S.C. 2332f (effective upon the terrorist bombing convention entering into force for the U.S.) (bombing public places, government facilities, or public utilities outside the United States)

Jurisdictional factors:

- the victim was a United States national;
- the offender was a United States national;
- the offense was committed against federal property;
- the offender is present in the United States;
- the offense was committed on United States registered vessel or aircraft; or
- the offense was intended to compel action or abstention by the United States

18 U.S.C. 3261 (offenses committed by members of the United States armed forces or individuals accompanying or employed by the United States armed forces overseas)

Threats

18 U.S.C. 32 (threats to destroy foreign civil aircraft, or aircraft in the special aircraft jurisdiction of the United States, or aircraft or aircraft facilities in the special maritime and territorial jurisdiction of the United States)

18 U.S.C. 112 (threatening internationally protected person)

Jurisdictional factors:

- the victim was a United States national;
- the offender was a United States national; or
- the offender is afterwards found in the United States

18 U.S.C. 115(a)(1)(A) (threats to assault, murder or kidnap a family member of a United States officer, employee or judge with intent to impede or retaliate for performance of federal duties)*

18 U.S.C. 115(a)(1)(B) (threats to assault, murder or kidnap a former United States officer, employee or judge or any member of their families in retaliation for performance of federal duties)*

18 U.S.C. 175 (threatening to develop, produce, stockpile, transfer, acquire, retain, or possess biological weapons or delivery systems, misuse of biological weapons; or threatening to assisting a foreign power to do so;)

- "there is extraterritorial Federal jurisdiction over an offense under this section committed by or against a national of the United States," 18 U.S.C.175(a)

18 U.S.C. 229 (threatening to use chemical weapons)

Jurisdictional factors:

- the victim or offender was a United States national; or
- the offense was committed against federal property

18 U.S.C. 831 (threaten to use nuclear material of injury or destroy)

Jurisdictional factors:

- committed within the special aircraft or special maritime and territorial jurisdiction of the United States;
- a United States national or an American legal entity was the victim of the offense;
- the offender was a United States national or an American legal entity; or
- the offender is afterwards found in the United States;
- the offense involved a transfer to or from the United States; or
- the offense was a threat directed against the United States

18 U.S.C. 871 (threatening the President)*

18 U.S.C. 875 (transmission of a threat in the foreign commerce of the United States)

18 U.S.C. 877 (mailing a threat to kidnap or injure from a foreign country to the United States)

18 U.S.C. 878 (threatening to kill, kidnap or assault an internationally protected person)

Jurisdictional factors:

- a victim was a United States national;
- the offender was a United States national; or
- the offender is afterwards found in the United States

18 U.S.C. 879 (threatening former Presidents)*

18 U.S.C. 1203 (threaten to kill or injure a hostage outside the United States)
Jurisdictional factors:
- the victim was a United States national;
- the offender was a United States national;
- the offender is afterwards found in the United States; or
- the offense was intended to compel action or abstention by the United States

18 U.S.C. 1503 (obstruction of federal judicial proceedings by threat)*

18 U.S.C. 1505 (obstruction of administrative or Congressional proceedings by threat)*

18 U.S.C. 1512 (threatening a federal witness or informant)
Jurisdictional factors:
- "[t]here is extraterritorial Federal jurisdiction over an offense under this section," 18 U.S.C. 1512(g)

18 U.S.C. 1513 (threatening to retaliate against a federal witness or informant)
Jurisdictional factors:
- "[t]here is extraterritorial Federal jurisdiction over an offense under this section," 18 U.S.C. 1513(d))

18 U.S.C. 1992 (threatening a terrorist attack on mass transit)
Jurisdictional factor
- the victim was mass transit in or affecting U.S. foreign commerce, or
- the offender travels or communicates across a state line

18 U.S.C. 2280 (threats of violence against maritime navigation)
Jurisdictional factors:
- the victim was a United States national;
- the offender was a United States national;
- the offender is afterwards found in the United States; or
- the offense was intended to compel action or abstention by the United States

18 U.S.C. 2281 (threatens injury or destruction aboard a fixed maritime platform)
Jurisdictional factors:
- the victim was a United States national;
- the offender was a United States national;
- the offender is afterwards found in the United States; or

- the offense was intended to compel action or abstention by the United States

18 U.S.C. 2290
Offenses:
- destruction of vessels or maritime facilities (18 U.S.C. 2291); or
- attempting or conspiring to do so (18 U.S.C. 2291)

Jurisdictional factors:
- victim or offender was a U.S. national;
- U.S. national was aboard victim vessel;
- victim vessel was a U.S. vessel

18 U.S.C. 2332a (threatening to use a weapon of mass destruction)
Jurisdictional factors:
- the victim was a United States national;
- the offender was a United States national; or
- the offense was committed against federal property

18 U.S.C. 2332f (effective upon the terrorist bombing convention entering into force for the U.S.) (threatening to bomb public places, government facilities, or public utilities outside the United States)
Jurisdictional factors:
- the victim was a United States national;
- the offender was a United States national;
- the offense was committed against federal property;
- the offender is present in the United States;
- the offense was committed on United States registered vessel or aircraft; or
- the offense was intended to compel action or abstention by the United States

49 U.S.C. 46507 (threats or scares concerning air piracy or bombing aircraft in the special aircraft jurisdiction of the United States)

False Statements

8 U.S.C. 1160(b)(7)(A) (falsification of an application for immigration status)*

15 U.S.C. 158 (false or fraudulent statements by China Trade Act corporate personnel)*

15 U.S.C. 645 (false statements associated with the Small Business Administration)*

15 U.S.C. 714m (false statements associated with the Commodity Credit Corporation)*

16 U.S.C. 831t (false statements associated with TVA)*

*18 U.S.C. 152 * (false statements in bankruptcy)*

18 U.S.C. 287 (false or fraudulent claims against the United States)*

18 U.S.C. 288 (false claims for postal losses)*

18 U.S.C. 289 (false claims for pensions)*

18 U.S.C. 541 (entry of goods falsely classified)

18 U.S.C. 542 (entry of goods by means of false statements)

18 U.S.C. 550 (false claim for refund of duties)

18 U.S.C. 1001 (false statement on a matter within the jurisdiction of a federal agency)*

18 U.S.C. 1002 (possession of false papers to defraud the United States)*

18 U.S.C. 1003 (fraudulent claims against the United States)*

18 U.S.C. 1007 (false statements in an FDIC transaction)*

18 U.S.C. 1011 (false statements in federal land bank mortgage transactions)*

18 U.S.C. 1014 (false statements in loan or credit applications in which the United States has an interest)*

18 U.S.C. 1015 (false statements concerning naturalization, citizenship or alien registry)

18 U.S.C. 1019 (false certification by consular officer)

18 U.S.C. 1020 (false statements concerning highway projects)*

18 U.S.C. 1022 (false certification concerning material for the military)

18 U.S.C. 1027 (false statements to facilitate a theft concerning ERISA)*

18 U.S.C. 1039 (obtaining confidential communications information by fraud)

18 U.S.C. 1542 (false statement in application for a passport)

18 U.S.C. 1546 (fraud in connection with visas, permits and other documents)

18 U.S.C. 1621 (perjury)*

18 U.S.C. 1622 (subornation of perjury)*

22 U.S.C. 1980 (false statement to obtain compensation for loss of commercial fishing vessel or gear)*

22 U.S.C. 4221 (perjury or false swearing before American diplomatic personnel)

22 U.S.C. 4222 (presentation of forged documents to United States foreign service personnel)

42 U.S.C. 408 (false statement in old age claims)*

42 U.S.C. 1320a-7b (false statements concerning Medicare)*

Theft

7 U.S.C. 2024(b) (food stamp fraud)*

15 U.S.C. 645 (embezzlement or fraud associated with the Small Business Administration)*

15 U.S.C. 714m (embezzlement or fraud associated with the Commodity Credit Corporation)*

16 U.S.C. 831t (theft associated with TVA)*

18 U.S.C. 371 (conspiracy to defraud the United States)

18 U.S.C. 641 (theft of federal property)*

18 U.S.C. 645 (theft by federal court officers)*

18 U.S.C. 648 (theft of federal property by custodians)*

18 U.S.C. 656 (embezzlement from a federally insured bank)*

18 U.S.C. 657 (embezzlement from a federally insured credit union)*

18 U.S.C. 658 (theft of property mortgaged or pledged to federal farm credit agencies)*

18 U.S.C. 661 (theft within the special maritime and territorial jurisdiction of the United States)

18 U.S.C. 662 (receipt of stolen property within the special maritime and territorial jurisdiction of the United States)

18 U.S.C. 831 (theft of nuclear materials)
Jurisdictional factors:

- within the special aircraft or special maritime and territorial jurisdiction of the United States;
- the victim was a United States national or an American legal entity;
- the offender was a United States national or an American legal entity;
- the offender is afterwards found in the United States; or
- the offense involved a transfer to or from the United States

18 U.S.C. 1025 (theft by false pretenses or fraud within the special maritime and territorial jurisdiction of the United States)

18 U.S.C. 793-798 (espionage)*

18 U.S.C. 1010 (fraud to secure loan or credit advance from HUD)*

18 U.S.C. 1013 (fraud in connection with farm loan bonds or credit bank debentures)*

18 U.S.C. 1023 (fraud in connection with deliveries for military services)*

18 U.S.C. 1024 (receipt of stolen military property)*

18 U.S.C. 1026 (fraudulently securing the cancellation of farm debt to the United States)*

18 U.S.C. 1030 (fraud in connection with computers)*

18 U.S.C. 1031 (major fraud against the United States)*

18 U.S.C. 1506 (theft or alteration of court records)*

18 U.S.C. 1707 (theft of postal service property)*

18 U.S.C. 1711 (theft of postal funds)*

18 U.S.C. 2071 (destruction of United States records)*

18 U.S.C. 2112 (robbery of the personal property of the United States)*

18 U.S.C. 2115 (robbery of a post office)*

18 U.S.C. 3261 (offenses committed by members of the United States armed forces or individuals accompanying or employed by the United States armed forces overseas)

20 U.S.C. 1097 (fraud in connection with financial aid to students)*

22 U.S.C. 4217 (embezzlement by American diplomatic personnel)*

25 U.S.C. 450d (theft involving the Indian Self-Determination and Education Assistance Act)*

38 U.S.C. 787 (fraud concerning veterans' life insurance)*

42 U.S.C. 1307 (social security fraud)*

42 U.S.C. 1383a (fraud in connection with supplemental security income for the blind, aged and disabled)*

42 U.S.C. 1713 (fraud in connection in connection with claims for injuries overseas associated with contracts for the United States)*

42 U.S.C. 1760(g) (theft in connection with the school lunch program)*

42 U.S.C. 1761(o) (fraud in connection with summer food programs)*

42 U.S.C. 3220 (fraud and theft concerning public works and economic development)*

42 U.S.C. 3795 (fraud or theft of funds associated with the Office of Justice Programs)*

45 U.S.C. 359 (fraud in connection with railroad unemployment insurance)*

46 U.S.C. App. 1276 (fraud in connection with federal ship mortgage insurance)*

Counterfeiting

18 U.S.C. 470-474 (counterfeiting United States obligations outside the United States)

18 U.S.C. 484 (connecting parts of different notes of the United States)*

18 U.S.C. 486 (uttering United States coins of gold, silver or other metal)*

18 U.S.C. 487 (making or possessing counterfeit dies for United States coins)*

18 U.S.C. 490 (counterfeiting minor United States coins)*

18 U.S.C. 491 (counterfeiting tokens or paper used as money of the United States)*

18 U.S.C. 493 (counterfeiting bonds and obligations of certain federal lending agencies)*

18 U.S.C. 494 (forging contractors bonds, bids or public records in order to defraud the United States)*

18 U.S.C. 495 (forging contracts, deeds or powers of attorney in order to defraud the United States)*

18 U.S.C. 496 (counterfeiting United States customs entry certificates)*

18 U.S.C. 497 (counterfeiting United States letters patent)*

18 U.S.C. 498 (counterfeiting United States military or naval discharge certificates)*

18 U.S.C. 499 (counterfeiting United States military, naval or official passes)*

*18 U.S.C. 500 *(counterfeiting United States postal money orders)*

18 U.S.C. 501 (counterfeiting United States postal stamps)*

18 U.S.C. 503 (counterfeiting postmarking stamps)*

18 U.S.C. 505 (counterfeiting federal judicial documents)*

18 U.S.C. 506 (counterfeiting federal agency seals)*

18 U.S.C. 507 (forging or counterfeiting ships papers)*

18 U.S.C. 508 (forging or counterfeiting government transportation requests)*

18 U.S.C. 509 (possession of plates to counterfeiting government transportation requests)*

18 U.S.C. 510 (forging endorsements on Treasury checks)*

18 U.S.C. 513 (counterfeiting state securities)*

18 U.S.C. 514 (transmitting, transporting, or sending a fictitious U.S. financial instrument in the foreign commerce of the United States)*

Piggyback Statutes

18 U.S.C. 2 (principals)

18 U.S.C. 3 (accessories after the fact)

18 U.S.C. 4 (misprision)

18 U.S.C. 371 (conspiracy)

18 U.S.C. 924(c), (j) (using or carrying a firearm during the course of a federal crime of violence or drug trafficking crime)

18 U.S.C. 1952 (Travel Act)

18 U.S.C. 1956-1957 (money laundering)

18 U.S.C. 1959 (violence in aid of racketeering)

18 U.S.C. 1961-1965 (RICO)

21 U.S.C. 846 (conspiracy or attempt to violate the Controlled Substances Act)

21 U.S.C. 963 (conspiracy or attempt to violate the Controlled Substances Import and Export Act)

Model Penal Code

§1.03 Territorial Applicability

(1) Except as otherwise provided in this Section, a person may be convicted under the law of this State of an offense committed by his own conduct or the conduct of another for which he is legally accountable if:

(a) either the conduct that is an element of the offense or the result that is such an element occurs within this State; or

(b) conduct occurring outside the State is sufficient under the law of this State to constitute an attempt to commit an offense within the State; or

(c) conduct occurring outside the State is sufficient under the law of this State to constitute a conspiracy to commit an offense within the state and an overt act in furtherance of such conspiracy occurs within the state; or

(d) conduct occurring within the State establishes complicity in the commission of, or an attempt, solicitation or conspiracy to commit , an offense in another jurisdiction that also is an offense under the law of this State; or

(e) the offense consists of the omission to perform a legal duty imposed by the law of this State with respect to domicile, residence or a relationship to a person, thing or transaction in the State; or

(f) the offense is based on a statute of this State that expressly prohibits conduct outside the State, when the conduct bears a reasonable relation to a legitimate interest of this State and the actor knows or should know that his conduct is likely to affect that interest.

(2) Subsection (1)(a) does not apply when either causing a specified result or a purpose to cause or danger of causing such a result is an element of an offense and the result occurs or is designed or likely to occur only in another jurisdiction where the conduct charged would not constitute an offense, unless a legislative purpose plainly appears to declare the conduct criminal regardless of the place of the result.

(3) Subsection (1)(a) does not apply when causing a particular result is an element of an offense and the result is caused by conduct occurring outside the State that would not constitute an offense if the result had occurred there, unless the actor purposely or knowingly caused the result within the State.

(4) When the offense is homicide, either the death of the victim or the bodily impact causing death constitutes a result within the meaning of Subsection (a)(1), and if the body of a homicide victim is found within the State, it is presumed that such result occurred within the State.

(5) This State includes the land and water and the air space above such land and water with respect to which the State has legislative jurisdiction.

Restatement of the Law Third: Foreign Relations Law of the United States

§401. Categories of Jurisdiction

Under international law, a state is subject to limitations on

(a) jurisdiction to prescribe, i.e., to make its law applicable to the activities, relations, or status of persons, or the interests of persons in things, whether by legislation, by executive act or order, by administrative rule or regulation, or by determination of a court;

(b) jurisdiction to adjudicate, i.e., to subject persons or things to the process of its courts or administrative tribunals, whether in civil or in criminal proceedings, whether or not the state is a party to the proceedings;

(c) jurisdiction to enforce, i.e., to induce or compel compliance or to punish noncompliance with its laws or regulations, whether through the courts or by use of executive, administrative, police, or other nonjudicial action.

§402. Bases of Jurisdiction to Prescribe

Subject to §403, a state has jurisdiction to prescribe law with respect to

(1)

(a) conduct that, wholly or in substantial part, takes place within its territory;

(b) the status of persons, or interests in things, present within its territory;

(c) conduct outside its territory that has or is intended to have substantial effect within its territory;

(2) the activities, interests, status, or relations of its nationals outside as well as within its territory; and

(3) certain conduct outside its territory by persons not its nationals that is directed against the security of the state or against a limited class of other state interests.

§403. Limitations on Jurisdiction to Prescribe

(1) Even when one of the bases for jurisdiction under §402 is present, a state may not exercise jurisdiction to prescribe law with respect to a person or activity having connections with another state when the exercise of such jurisdiction is unreasonable.

(2) Whether exercise of jurisdiction over a person or activity is unreasonable is determined by evaluating all relevant factors, including, where appropriate:

(a) the link of the activity to the territory of the regulating state, i.e., the extent to which the activity takes place within the territory, or has substantial, direct, and foreseeable effect upon or in the territory;

(b) the connections, such as nationality, residence, or economic activity, between the regulating state and the person principally responsible for the

activity to be regulated, or between that state and those whom the regulation is designed to protect;

(c) the character of the activity to be regulated, the importance of regulation to the regulating state, the extent to which other states regulate such activities, and the degree to which the desirability of such regulation is generally accepted;

(d) the existence of justified expectations that might be protected or hurt by the regulation;

(e) the importance of the regulation to the international political, legal, or economic system;

(f) the extent to which the regulation is consistent with the traditions of the international system;

(g) the extent to which another state may have an interest in regulating the activity; and

(h) the likelihood of conflict with regulation by another state.

(3) When it would not be unreasonable for each of two states to exercise jurisdiction over a person or activity, but the prescriptions by the two states are in conflict, each state has an obligation to evaluate its own as well as the other state's interest in exercising jurisdiction, in light of all the relevant factors, Subsection (2); a state should defer to the other state if that state's interest is clearly greater.

§404. Universal Jurisdiction to Define and Punish Certain Offenses

A state has jurisdiction to define and prescribe punishment for certain Offenses recognized by the community of nations as of universal concern, such as piracy, slave trade, attacks on or hijacking of aircraft, genocide, war crimes, and perhaps certain acts of terrorism, even where none of the jurisdiction indicated in §402 is present.

§421. Jurisdiction to Adjudicate

(1) A state may exercise jurisdiction through its courts to adjudicate with respect to a person or thing if the relationship of the state to the person or thing is such as to make the exercise of jurisdiction reasonable.

(2) In general, a state's exercise of jurisdiction to adjudicate with respect to a person or thing is reasonable if, at the time jurisdiction is asserted:

(a) the person or thing is present in the territory of the state, other than transitorily;

(b) the person, if a natural person, is domiciled in the state;

(c) the person, if a natural person, is resident in the state;

(d) the person, if a natural person, is a national of the state;

(e) the person, if a corporation or comparable juridical person, is organized pursuant to the law of the state;

(f) a ship, aircraft, or other vehicle to which the adjudication relates is registered under the laws of the state;

(g) the person, whether natural or juridical, has consented to the exercise of jurisdiction;

(h) the person, whether natural or juridical, regularly carries on business in the state;
(i) the person, whether natural or juridical, had carried on activity in the state, but only in respect to such activity;
(j) the person, whether natural or juridical, had carried on outside the state an activity having a substantial, direct, and foreseeable effect within the state, but only in respect to such activity;
or
(k) the thing that is the subject of adjudication is owned, possessed, or used in the state, but only in respect to a claim reasonably connected with that thing.

(3) A defense of lack of jurisdiction is generally waived by any appearance by or on behalf of a person or thing (whether as plaintiff, defendant, or third party), if the appearance is for a purpose that does not include a challenge to the exercise of jurisdiction.

§431. Jurisdiction to Enforce

(1) A state may employ judicial or nonjudicial measures to induce or compel compliance or punish noncompliance with its laws or regulations, provided it has jurisdiction to prescribe in accordance with §§402 and 403.
(2) Enforcement measures must be reasonably related to the laws or regulations to which they are directed; punishment for noncompliance must be preceded by an appropriate determination of violation and must be proportional to the gravity of the violation.
(3) A state may employ enforcement measures against a person located outside the territory
(a) if the person is given notice of the claims or charges against him that is reasonable in the circumstances;
(b) if the person is given an opportunity to be heard, ordinarily in advance of enforcement, whether in person or by counsel or other representative; and
(c) when enforcement is through the courts, if the state has jurisdiction to adjudicate.

<u>18 U.S.C. 7. Special Maritime and Territorial Jurisdiction of the United States (text)</u>

The term “special maritime and territorial jurisdiction of the United States”, as used in this title, includes:
(1) The high seas, any other waters within the admiralty and maritime jurisdiction of the United States and out of the jurisdiction of any particular State, and any vessel belonging in whole or in part to the United States or any citizen thereof, or to any corporation created by or under the laws of the United States, or of any State, Territory, District, or possession thereof, when such vessel is within the admiralty and maritime

jurisdiction of the United States and out of the jurisdiction of any particular State.
(2) Any vessel registered, licensed, or enrolled under the laws of the United States, and being on a voyage upon the waters of any of the Great Lakes, or any of the waters connecting them, or upon the Saint Lawrence River where the same constitutes the International Boundary Line.
(3) Any lands reserved or acquired for the use of the United States, and under the exclusive or concurrent jurisdiction thereof, or any place purchased or otherwise acquired by the United States by consent of the legislature of the State in which the same shall be, for the erection of a fort, magazine, arsenal, dockyard, or other needful building.
(4) Any island, rock, or key containing deposits of guano, which may, at the discretion of the President, be considered as appertaining to the United States.
(5) Any aircraft belonging in whole or in part to the United States, or any citizen thereof, or to any corporation created by or under the laws of the United States, or any State, Territory, District, or possession thereof, while such aircraft is in flight over the high seas, or over any other waters within the admiralty and maritime jurisdiction of the United States and out of the jurisdiction of any particular State.
(6) Any vehicle used or designed for flight or navigation in space and on the registry of the United States pursuant to the Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies and the Convention on Registration of Objects Launched into Outer Space, while that vehicle is in flight, which is from the moment when all external doors are closed on Earth following embarkation until the moment when one such door is opened on Earth for disembarkation or in the case of a forced landing, until the competent authorities take over the responsibility for the vehicle and for persons and property aboard.
(7) Any place outside the jurisdiction of any nation with respect to an offense by or against a national of the United States.
(8) To the extent permitted by international law, any foreign vessel during a voyage having a scheduled departure from or arrival in the United States with respect to an offense committed by or against a national of the United States.
(9) With respect to Offenses committed by or against a national of the United States as that term is used in section 101 of the Immigration and Nationality Act—

> (A) the premises of United States diplomatic, consular, military or other United States Government missions or entities in foreign States, including the buildings, parts of buildings, and land appurtenant or ancillary thereto or used for purposes of those missions or entities, irrespective of ownership; and
> (B) residences in foreign States and the land appurtenant or ancillary thereto, irrespective of ownership, used for purposes of

those missions or entities or used by United States personnel assigned to those missions or entities.

Nothing in this paragraph shall be deemed to supersede any treaty or international agreement with which this paragraph conflicts. This paragraph does not apply with respect to an offense committed by a person described in section 3261(a) of this title.

18 U.S.C. 3261. Military Extraterritorial Jurisdiction (text)

(a) Whoever engages in conduct outside the United States that would constitute an offense punishable by imprisonment for more than 1 year if the conduct had been engaged in within the special maritime and territorial jurisdiction of the United States –

(1) while employed by or accompanying the Armed Forces outside the United States; or

(2) while a member of the Armed Forces subject to chapter 47 of title 10 (the Uniform Code of Military Justice), shall be punished as provided for that offense.

(b) No prosecution may be commenced against a person under this section if a foreign government, in accordance with jurisdiction recognized by the United States, has prosecuted or is prosecuting such person for the conduct constituting such offense, except upon the approval of the Attorney General or the Deputy Attorney General (or a person acting in either such capacity), which function of approval may not be delegated.

(c) Nothing in this chapter may be construed to deprive a court-martial, military commission, provost court, or other military tribunal of concurrent jurisdiction with respect to offenders or offenses that by statute or by the law of war may be tried by a court-martial, military commission, provost court, or other military tribunal.

(d) No prosecution may be commenced against a member of the Armed Forces subject to chapter 47 of title 10 (the Uniform Code of Military Justice) under this section unless –

(1) such member ceases to be subject to such chapter; or

(2) an indictment or information charges that the member committed the offense with one or more other defendants, at least one of whom is not subject to such chapter.

Bibliography

Books and Articles

Abbell, EXTRADITION TO AND FROM THE UNITED STATES (2004 & 2007 Supp.)

_____, OBTAINING EVIDENCE ABROAD IN CRIMINAL CASES (2004 & 2008 Supp.)

Abramovsky, Extraterritorial Jurisdiction: The United States Unwarranted Attempt to Alter International Law in United States v. Yunis, 15 YALE JOURNAL OF INTERNATIONAL LAW 121 (1990)

Abramovsky & Edelstein, Time for Final Action on 18 U.S.C. 3292, 21 MICHIGAN JOURNAL OF INTERNATIONAL LAW 941 (2000)

American Law Institute, RESTATEMENT OF THE LAW THIRD: THE FOREIGN RELATIONS LAW OF THE UNITED STATES (1987)

Bassiouni, INTERNATIONAL EXTRADITION: UNITED STATES LAW AND PRACTICE (4th ed. 2002)

Bentley, Toward an International Fourth Amendment: Rethinking Searches and Seizures Abroad After Verdugo-Urquidez, 27 VANDERBILT JOURNAL OF TRANSNATIONAL LAW 329 (1994)

Blakesley, A Conceptual Framework for Extradition and Jurisdiction Over Extraterritorial Crimes, 1984 UTAH LAW REVIEW 685

Blakesley & Stigall, The Myopia of U.S. v. Martinelli: Extraterritorial Jurisdiction in the 21st Century, 39 GEORGE WASHINGTON INTERNATIONAL LAW REVIEW 1 (2007)

Birkett, Cracks in the Foundation of Extraterritorial Law Enforcement—A Challenge to Basic Judicial Doctrines, 15 SOUTHERN ILLINOIS UNIVERSITY LAW JOURNAL 895 (1991)

Born, Reappraisal of the Extraterritorial Reach of United States Law, 24 LAW & POLICY IN INTERNATIONAL BUSINESS 1 (1992)

Bradley, Universal Jurisdiction and United States Law, 2001 UNIVERSITY OF CHICAGO LEGAL FORUM 323

Brilmayer, The Extraterritorial Application of American Law: A Methodological and Constitutional Appraisal, 50 LAW & CONTEMPORARY PROBLEMS 11 (1987)

Brilmayer & Norchi, Federal Extraterritoriality and Fifth Amendment Due Process, 105 HARVARD LAW REVIEW 1217 (1992)

Cabranes, Our Imperial Criminal Procedure: Problems in the Extraterritorial Application of U.S. Constitutional Law, 118 YALE LAW JOURNAL 1660 (2009)

Carey, Should American Courts Listen to What Foreign Courts Hear? The Confrontation and Hearsay Problems of Prior Testimony Taken Abroad in Criminal Proceedings, 29 AMERICAN JOURNAL OF CRIMINAL LAW 29 (2001)

Colangelo, Constitutional Limits on Extraterritorial Jurisdiction: Terrorism and the Intersection of National and International Law, 48 HARVARD INTERNATIONAL LAW JOURNAL 121 (2007)

Condon, Extraterritorial Interrogation: The Porous Border Between Torture and U.S. Criminal Trials, 60 RUTGERS LAW REVIEW 647 (2008)

Gans, Reasonableness as a Limit to Extraterritorial Jurisdiction, 62 WASHINGTON UNIVERSITY LAW QUARTERLY 681 (1985)

George, Extraterritorial Application of Penal Legislation, 64 MICHIGAN LAW REVIEW 609 (1966)

Gerger, Beyond Balancing: International Law Restraints on the Reach of National Laws, 10 YALE JOURNAL OF INTERNATIONAL LAW 185 (1984)

Gibney, The Extraterritorial Application of United States Law: The Perversion of Democratic Governance, the Reversal of Institutional Roles, and the Imperative of Establishing Normative Principles, 19 BOSTON COLLEGE INTERNATIONAL & COMPARATIVE LAW REVIEW 297 (1996)

Gordon, United States Extraterritorial Subject Matter Jurisdiction in Securities Fraud Litigation, 10 FLORIDA JOURNAL OF INTERNATIONAL LAW 487 (1996)

Grandman, New Imperialism: The Extraterritorial Application of United States Law, 14 INTERNATIONAL LAWYER 257 (1980)

Griffin, Foreign Governmental Reactions to United States Assertions of Extraterritorial Jurisdiction, 6 GEORGE MASON LAW REVIEW 505 (1998)

Harvard Research in International Law, Jurisdiction With Respect to Crime, 72 AMERICAN JOURNAL OF INTERNATIONAL LAW (SUPP.) 485 (1935)

Joshua, Camesasca & Jung, Extradition and Mutual Legal Assistance Treaties: Cartel Enforcement's Global Reach, 75 ANTITRUST LAW JOURNAL 353 (2008)

Kane, Prosecuting International Terrorists in United States Courts: Gaining the Jurisdictional Threshold, 12 YALE JOURNAL INTERNATIONAL LAW 294 (1987)

Kontorovich, Beyond the Article I Horizon: Congress's Enumerated Powers and Universal Jurisdiction Over Drug Crimes, 93 MINNESOTA LAW REVIEW 1191 (2009)

_____, The "Define and Punish" Clause and the Limits of Universal Jurisdiction, 103 NORTHWESTERN UNIVERSITY LAW REVIEW 149 (2009)

Paust, Non-Extraterritoriality of "Special Territorial Jurisdiction" of the United States: Forgotten History and the Errors of Erdos, 24 YALE JOURNAL OF INTERNATIONAL LAW 305 (1999)

Perkins, The Territorial Principle in Criminal Law, 22 HASTINGS LAW JOURNAL 1155 (1971)

Petersen, The Extraterritorial Effect of Federal Criminal Statutes: Offenses Directed at Members of Congress, 6 HASTINGS INTERNATIONAL & COMPARATIVE LAW REVIEW 773 (1983)

Podgor, Globalization and the Federal Prosecution of White Collar Crime, 34 AMERICAN CRIMINAL LAW REVIEW 325 (1997)

___, International Computer Fraud: A Paradigm for Limiting National Jurisdiction, 35 UNIVERSITY OF CALIFORNIA DAVIS LAW REVIEW 267 (2002)

Randall, Universal Jurisdiction Under International Law, 66 TEXAS LAW REVIEW 785 (1988)

Richardson, Due Process for the Global Crime Age: A Proposal, 41 CORNELL INTERNATIONAL LAW JOURNAL 347 (2008)

Smith, In re Forfeiture Proceedings and Extraterritorial Jurisdiction, 45 INTERNATIONAL & COMPARATIVE LAW QUARTERLY 902 (1996)

Snow, The Investigation and Prosecution of White Collar Crime: International Challenges and the Legal Tools Available to Address Them, 11 WILLIAM & MARY BILL OF RIGHTS JOURNAL 20-9 (2002)

Tuerkheimer, Globalization of United States Law Enforcement: Does the Constitution Come Along? 39 HOUSTON LAW REVIEW 307 (2002)

Turley, When in Rome: Multinational Misconduct and the Presumption Against Extraterritoriality, 84 NORTHWESTERN UNIVERSITY LAW REVIEW 598 (1990)

United States Congress, Legislative Initiatives to Curb Domestic and International Terrorism; Hearings Before the Subcomm. on Security and Terrorism of the Senate Comm. on the Judiciary, 98th Cong., 2d Sess. (1984)

___, Bills to Authorize Prosecution of Terrorists and Others Who Attack United States Government Employees and Citizens Abroad: Hearing Before the Subcomm. on Security and Terrorism of the Senate Comm. on the Judiciary, 99th Cong., 1st Sess. (1985)

___, Extraterritorial Jurisdiction Over Terrorists Acts Abroad: Hearings Before Subcomm. on Crime of House Comm. on Judiciary, 101st Cong., 1st Sess. (1989)
van der Vyver, Prosecuting Offenses Against the Law of Nations in the United States, 20 EMORY INTERNATIONAL LAW REVIEW 473 (2006)

Warner, Challenges to International Law Enforcement Cooperation for the United States in the Middle East and North Africa: Extradition and Its Alternatives, 50 VILLANOVA LAW REVIEW 479 (2005)

Watson, Offenders Abroad: The Case for Nationality-Based Criminal Jurisdiction, 17 YALE JOURNAL OF INTERNATIONAL LAW 41 (1992)

___, The Passive Personality Principle, 28 TEXAS INTERNATIONAL LAW JOURNAL 1 (1993)

Weisburd, Due Process Limits on Federal Extraterritorial Legislation? 35 COLUMBIA JOURNAL OF TRANSNATIONAL LAW 379 (1997)

Yost & Anderson, The Military Extraterritorial Jurisdiction Act of 2000: Closing the Gap, 33 CONNECTICUT LAW REVIEW 446 (2001)

Zabel, Extraterritoriality, 26 HARVARD INTERNATIONAL LAW JOURNAL 569 (1985)

Notes and Comments

Constructing the State Extraterritorially: Jurisdictional Discourse, the National Interests, and Transnational Norms, 103 HARVARD LAW REVIEW 1273 (1990)

Defining and Punishing Abroad: Constitutional Limits on the Extraterritorial Reach of the Offenses Clause, 48 DUKE LAW JOURNAL 1305 (1999)

Extraterritorial Jurisdiction Under International Law: The Yunis Decision as a Model for the Prosecution of Terrorists in United States Courts, 22 LAW & POLICY IN INTERNATIONAL BUSINESS 409 (1991)

The Five Bases of Extraterritorial Jurisdiction and the Failure of the Presumption Against Extraterritoriality, 33 HASTINGS INTERNATIONAL & COMPARATIVE LAW REVIEW 177 (1997)

The Fourth Amendment and Remote Searches: Balancing the Protection of "The People" With the Remote Investigation of Internet Crimes, 19 NOTRE DAME JOURNAL OF LAW, ETHICS & PUBLIC POLICY 355 (2005)

From a Pakistani Station House to the Federal Court House: A Confession's Uncertain Journey in the U.S.-Led War on Terror, 12 CARDOZO JOURNAL OF INTERNATIONAL AND COMPARATIVE LAW 297 (2004)

Interpreting 18 U.S.C.§2331 Under United States and International Law, 27 HARVARD JOURNAL ON LEGISLATION 579 (1990)

Love's Labour's Lost: Michael Lewis Clark's Constitutional Challenge of 18 U.S.C. 2423(C), 43 AMERICAN CRIMINAL LAW REVIEW 1241 (2006)

Predictability and Comity: Toward Common Principles of Extraterritorial Jurisdiction, 98 HARVARD LAW REVIEW 1310 (1985)

Protecting National Interests: The Legal Status of Extraterritorial Law Enforcement by the Military, 41 DUKE LAW JOURNAL 867 (1992)

The Protective Principle of Extraterritorial Jurisdiction: A Brief History and an Application of the Principle to Espionage as an Illustration of Current United States Practice, 6 BOSTON UNIVERSITY INTERNATIONAL LAW JOURNAL 337 (1988)

To Apply or Not to Apply: Extraterritorial Application of Federal RICO Laws, 33 FLORIDA JOURNAL OF INTERNATIONAL LAW 131 (1993)

United States v. Jura: Fifth Amendment Due Process and Stateless Vessels on the High Seas, 73 BOSTON UNIVERSITY LAW REVIEW 477 (1993)

United States v. Passaro: Exercising Extraterritorial Jurisdiction Over Non-Defense Department Government Contractors Committing Crimes Overseas Under the Special Maritime and Territorial Jurisdiction of the United States, 58 CATHOLIC UNIVERSITY LAW REVIEW 1143 (2009)
United States v. Yunis: The D.C. Circuit's Dubious Approval of United States Long-arm Jurisdiction Over Extraterritorial Crime, 87 NORTHWESTERN UNIVERSITY LAW REVIEW 697 (1993).

18 U.S.C. Chapter 37: Espionage and Censorship (18 U.S.C. §§ 791-799)

Unauthorized Disclosure of Classified Information

Criminal Prohibitions on the Publication of Classified Defense Information, R41404 (December 6, 2010).

JENNIFER K. ELSEA, CONGRESSIONAL RESEARCH SERV., CRIMINAL PROHIBITIONS ON THE PUBLICATION OF CLASSIFIED DEFENSE INFORMATION (2010), *available at* http://www.intelligencelaw.com/library/secondary/crs/pdf/R41404_12-6-2010.pdf.

Jennifer K. Elsea
Legislative Attorney

December 6, 2010
Order Code R41404

Summary

The recent online publication of classified defense documents and diplomatic cables by the organization WikiLeaks and subsequent reporting by the New York Times and other news media have focused attention on whether such publication violates U.S. criminal law. The Attorney General has reportedly stated that the Justice Department and Department of Defense are investigating the circumstances to determine whether any prosecutions will be undertaken in connection with the disclosure.

This report identifies some criminal statutes that may apply, but notes that these have been used almost exclusively to prosecute individuals with access to classified information (and a corresponding obligation to protect it) who make it available to foreign agents, or to foreign agents who obtain classified information unlawfully while present in the United States. Leaks of classified information to the press have only rarely been punished as crimes, and we are aware of no case in which a publisher of information obtained through unauthorized disclosure by a government employee has been prosecuted for publishing it. There may be First Amendment implications that would make such a prosecution difficult, not to mention political ramifications based on concerns about government censorship.

To the extent that the investigation implicates any foreign nationals whose conduct occurred entirely overseas, any resulting prosecution may carry foreign policy implications related to the exercise of extraterritorial jurisdiction and whether suspected persons may be extradited to the United States under applicable treaty provisions.

This report will discuss the statutory prohibitions that may be implicated, including the Espionage Act; the extraterritorial application of such statutes; and the First Amendment implications related to such prosecutions against domestic or foreign media organizations and associated individuals. The report will also provide a summary of pending legislation relevant to the issue, including S. 4004.

Introduction

The recent online publication of classified defense documents and diplomatic cables by the organization WikiLeaks and subsequent reporting by the New York Times, the Guardian (UK), and Der Spiegel (Germany) have focused attention on whether such publication violates U.S. criminal law. The Attorney General has reportedly stated that the Justice Department and Department of Defense are investigating the circumstances to determine whether any prosecutions will be undertaken in connection with the disclosure,[1417] but has not released sufficient factual findings to permit a full legal analysis. Accordingly, the following discussion will provide a general overview of the relevant law as it may apply to pertinent allegations reported in the media, assuming them to be true. The discussion should not be interpreted to confirm the truth of any allegations or establish that a particular statute has been violated.

Background

WikiLeaks.org describes itself as a "public service designed to protect whistle-blowers, journalists and activists who have sensitive materials to communicate to the public."[1418] Arguing that "[p]rincipled leaking has changed the course of history for the better," it states that its purpose is to promote transparency in government and fight corporate fraud by publishing information governments or corporations would prefer to keep secret, obtained from sources in person, by means of postal drops, and by using "cutting-edge cryptographic technologies" to receive material electronically.[1419] The organization promises contributors that their anonymity will be protected.

[1417] Mahmoud Kassem, Attorney General Holder Says U.S. Probing Leaks of Afghanistan Documents, BLOOMBERG, July 28, 2010, available at http://www.bloomberg.com/news/2010-07-28/attorney-general-holder-says-u-s-probing-leaks¬of-afghanistan-documents.html.

[1418] http://www.wikileaks.org/wiki/WikiLeaks:About.

[1419] Id.

According to press reports, WikiLeaks obtained more than 91,000 secret U.S. military reports related to the war in Afghanistan and posted the majority of them, unredacted, on its website in late July, 2010, after first alerting the New York Times and two foreign newspapers, the Guardian (London) and Der Spiegel (Germany), about the pending disclosure.[1420] Military officials have reportedly said they suspect an Army private, Bradley Manning, of having leaked the documents to WikiLeaks.[1421] Private Manning, a U.S. citizen, was already in military custody under suspicion of having provided WikiLeaks with video footage of an airstrike that resulted in the deaths of civilians.[1422] U.S. officials have condemned the leaks, predicting that the information disclosed could lead to the loss of lives of U.S. soldiers in Afghanistan and Afghan citizens who have provided them assistance.[1423] Defense Secretary Robert M. Gates informed Members of Congress that a preliminary review of the disclosed information by the Defense Department found that no sensitive information related to intelligence sources or methods was made public, but reiterated that the release of Afghan informants' names could have "potentially dramatic and grievously harmful consequences."[1424] WikiLeaks subsequently released some 400,000 documents related to the war in Iraq,[1425] this time with names of informants apparently redacted.[1426]

[1420] The New York Times published a series of articles under the headline "The War Logs," which is available online at http://www.nytimes.com/interactive/world/war-logs.html. The Times describes the leaked material as an archive covering six years of incident reports and intelligence documents—"usually spare summaries but sometimes detailed narratives"—that "illustrate[s] in mosaic detail why" the military effort in Afghanistan has not weakened the Taliban. C. J. Chivers et al., The Afghan Struggle: A Secret Archive, N.Y. TIMES, July 26, 2010, at 1. The German periodical Der Spiegel published a series of articles under the topic "Afghanistan Protocol," which is available (in English) online at http://www.spiegel.de/international/world/0,1518,708314,00.html. The Guardian (UK) published a series entitled "Afghanistan: The War Logs," which is available online at http://www.guardian.co.uk/world/the-war-logs.

[1421] Military airstrike video leak suspect in solitary confinement, CNN.com, Aug. 1, 2010, available at http://www.cnn.com/2010/POLITICS/07/31/wikileaks.manning/index.html.

[1422] Id.

[1423] Admiral Michael Mullen, Chairman of the Joint Chiefs of Staff, on Meet the Press, Aug. 1, 2010, transcript available at http://www.msnbc.msn.com/id/38487969/ns/meet_the_press-transcripts/.

[1424] See Elisabeth Bumiller, Gates Found Cost of Leaks Was Limited, NY TIMES, Oct. 17, 2010 (quoting letter to Senator Levin from Secretary Gates).

[1425] See The Iraq Archive: The Strands of a War, NY TIMES, at http://www.nytimes.com/2010/10/23/world/middleeast/ 23intro.html?_r=1.

[1426] See Anna Mulrine, Wikileaks Iraq Documents not as Damaging as Pentagon Feared—Yet, CHRISTIAN SCIENCE MONITOR, Oct. 25, 2010. The New York Times has stated it redacted names prior to publishing the leaked materials. See The Iraq Archive, supra footnote 9.

In late November, 2010, WikiLeaks began publishing what the New York Times calls a "mammoth cache of a quarter-million confidential American diplomatic cables," dated for the most part within the last three years.[1427] Wikileaks.org posted 220 cables on November 28, 2010, as a first installment, some of which documents were redacted to protect diplomatic sources. The most recent documents in the collection are reportedly dated February 2010.[1428]

The United States government was aware of the impending disclosure, although not apparently directly informed by the web-based anti-secrecy organization (or given access to the documents to be released), although WikiLeaks Editor in Chief Julian Assange offered in a letter sent to the U.S. ambassador to the U.K., Louis Susman, to consider any U.S. requests to protect specific information that the government believes could, if published, put any individuals at significant risk of harm.[1429] The State Department Legal Adviser responded in a letter to Mr. Assange's attorney that the publication of classified materials violates U.S. law, that the United States will not negotiate with WikiLeaks with respect to the publication of illegally obtained classified documents, and that WikiLeaks should cease these activities and return all documents, as well as delete any classified U.S. government material in its possession from its databases.[1430] Mr. Assange responded by accusing the United States of adopting a confrontational stance and indicating an intent to continue publishing the materials, subject to the checks WikiLeaks and its media partners planned to implement to reduce any risk to individuals.[1431]

After learning the classified cables were to be published, the Defense Department notified the U.S. Senate and House Armed Services Committees in general terms about what to expect.[1432] Assistant Secretary for Legislative Affairs Elizabeth King explained that "State Department cables by their nature contain everyday

---

[1427] State's Secrets, NY TIMES (online edition), Nov. 29, 2010, http://www.nytimes.com/interactive/world/statessecrets.html.

[1428] Scott Shane and Andrew W. Lehren, Cables Obtained by WikiLeaks Shine Light Into Secret Diplomatic Channels, NY TIMES.

[1429] Letter to Ambassador Susman, Nov. 26, 2010, available at http://documents.nytimes.com/letters-between-wikileaks-and-gov.

[1430] Letter from State Department Legal Adviser Harold Hongju Koh to Jennifer Robinson, Nov. 27, 2010, available at http://documents.nytimes.com/letters-between-wikileaks-and-gov.

[1431] Letter to Ambassador Susman, Nov. 28, 2010, available at http://documents.nytimes.com/letters-between-wikileaks¬and-gov.

[1432] Tony Capaccio, Pentagon Alerts House, Senate Panels to New Classified WikiLeaks Release, BLOOMBERG, Nov. 24, 2010, http://www.bloomberg.com/news/2010-11-24/pentagon-warns-house-senate-defense-panels-of-more-wikileaks-documents.html.

analysis and candid assessments that any government engages in as part of effective foreign relations," and predicted that the publication of the classified cables, which she described as intended to "wreak havoc and destabilize global security," could potentially jeopardize lives.[1433] State Department spokesman Philip J. Crowley told Bloomberg that the State Department is "assessing the possible impact on our on-going diplomatic activity and notifying both Congress and other governments what may occur."[1434] The White House issued a statement condemning the activities of WikiLeaks[1435] and ordered all agencies to conduct reviews of their information security policies and programs.[1436]

The publication of the leaked documents by WikiLeaks and the subsequent reporting of information contained therein raise questions with respect to the possibility of bringing criminal charges for the dissemination of materials by media organizations following an unauthorized disclosure, in particular when done by non-U.S. nationals overseas. This report will discuss the statutory prohibitions that may be implicated; the extraterritorial application of such statutes; and the First Amendment implications related to such prosecutions against domestic or foreign media organizations and associated individuals.

[1433] Id.

[1434] Id.

[1435] White House, Statement of the Press Secretary, Nov. 28, 2010, at http://www.whitehouse.gov/the-press-office/2010/ 11/28/statement-press-secretary. The statement reads in full: We anticipate the release of what are claimed to be several hundred thousand classified State department cables on Sunday night that detail private diplomatic discussions with foreign governments. By its very nature, field reporting to Washington is candid and often incomplete information. It is not an expression of policy, nor does it always shape final policy decisions. Nevertheless, these cables could compromise private discussions with foreign governments and opposition leaders, and when the substance of private conversations is printed on the front pages of newspapers across the world, it can deeply impact not only US foreign policy interests, but those of our allies and friends around the world. To be clear—such disclosures put at risk our diplomats, intelligence professionals, and people around the world who come to the United States for assistance in promoting democracy and open government. These documents also may include named individuals who in many cases live and work under oppressive regimes and who are trying to create more open and free societies. President Obama supports responsible, accountable, and open government at home and around the world, but this reckless and dangerous action runs counter to that goal. By releasing stolen and classified documents, Wikileaks has put at risk not only the cause of human rights but also the lives and work of these individuals. We condemn in the strongest terms the unauthorized disclosure of classified documents and sensitive national security information.

[1436] Memorandum from Jacob J. Lew, Director, Office of Management and Budget to Heads of Executive Departments and Agencies (Nov. 28, 2010) , at http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-06.pdf. For other White House responses to the WikiLeaks disclosures, see FACT SHEET: U.S. Government Mitigation Efforts in Light of the Recent Unlawful Disclosure of Classified Information (Dec. 1, 2010), at http://www.whitehouse.gov/search/site/classified%20information.

Statutory Protection of Classified Information

While there is no one statute that criminalizes the unauthorized disclosure of any classified information, a patchwork of statutes exists to protect information depending upon its nature, the identity of the discloser and of those to whom it was disclosed, and the means by which it was obtained. It seems likely that most of the information disclosed by WikiLeaks that was obtained from Department of Defense databases falls under the general rubric of information related to the national defense. The diplomatic cables obtained from State Department channels may also contain information relating to the national defense and thus be covered under the Espionage Act, but otherwise its disclosure by persons who are not government employees does not appear to be directly proscribed. It is possible that some of the government information disclosed in any of the three releases does not fall under the express protection of any statute, despite its classified status.

The Espionage Act

National defense information in general is protected by the Espionage Act,[1437] 18 U.S.C. §§ 793– 798, while other types of relevant information are covered elsewhere. Some provisions apply only to government employees or others who have authorized access to sensitive government information,[1438] but the following provisions apply to all persons. 18 U.S.C. § 793 prohibits the gathering, transmitting, or receipt of defense information with the intent or reason to believe the information will be used against the United States or to the benefit of a foreign nation. Violators are subject to a fine or up to 10 years imprisonment, or both,[1439] as are those who conspire to violate the statute.[1440] Persons who possess

---

[1437] Act of October 6, 1917, ch. 106, § 10(i), 40 Stat. 422.

[1438] E.g., 18 U.S.C. §§ 952 (prohibiting disclosure of diplomatic codes and correspondence), 1924 (unauthorized removal and retention of classified documents or material); 50 U.S.C. § 783 (unauthorized disclosure of classified information to an agent of a foreign government, unauthorized receipt by foreign government official) This report does not address such prohibitions, nor prohibitions that apply to military personnel under the Uniform Code of Military Justice.

[1439] 18 U.S.C. § 793(a)-(c) provides: (a) Whoever, for the purpose of obtaining information respecting the national defense with intent or reason to believe that the information is to be used to the injury of the United States, or to the advantage of any foreign nation, goes upon, enters, flies over, or otherwise obtains information concerning any vessel, aircraft, work of defense, [etc.], or any prohibited place so designated by the President by proclamation in time of war or in case of national emergency in which anything for the use of the Army, Navy, or Air Force is being prepared or constructed or stored, information as to which prohibited place the President has determined would be prejudicial to the national defense; or (b) Whoever, for the purpose aforesaid, and with like intent or reason to believe, copies, takes, makes, or obtains, or attempts to copy, take, make, or obtain any sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, document, writing, or note of anything connected with the national defense; or (c) Whoever, for the purpose aforesaid, receives or obtains or agrees or attempts to

defense information that they have reason to know could be used to harm the national security, whether the access is authorized or unauthorized, and who disclose that information to any person not entitled to receive it, or who fail to surrender the information to an officer of the United States, are subject to the same penalty.[1441] Although it is not necessary that the information be classified by a government agency, the courts seem to give deference to the executive determination of what constitutes "defense information."[1442] Information that is made available by the government to the public is not covered under the prohibition, however, because public availability of such information negates the bad-faith intent requirement.[1443] On the other hand, classified documents remain within the ambit of the statute even if information contained therein is made public by an unauthorized leak.[1444]

18 U.S.C. § 794 (aiding foreign governments or communicating information to an enemy in time of war) covers "classic spying" cases,[1445] providing for

---

receive or obtain from any person, or from any source whatever, any [protected thing] connected with the national defense, knowing or having reason to believe ... that it has been or will be obtained, taken, made, or disposed of by any person contrary to the provisions of this chapter [18 U.S.C. §§ 792 et seq.]....

[1440] 18 U.S.C. § 793(g) provides: If two or more persons conspire to violate any of the foregoing provisions of this section, and one or more of such persons do any act to effect the object of the conspiracy, each of the parties to such conspiracy shall be subject to the punishment provided for the offense which is the object of such conspiracy.

[1441] 18 U.S.C. § 793(e) provides: Whoever having unauthorized possession of, access to, or control over any document [or other protected thing], or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits ... to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it; ... Shall be fined under this title or imprisoned not more than ten years, or both.

[1442] The government must demonstrate that disclosure of the information is at least "potentially damaging" to the United States or advantageous to a foreign government. See United States v. Morison, 844 F.2d 1057, 1072 (4th Cir.), cert. denied, 488 U.S. (1988)(upholding conviction under 18 U.S.C. § 793 for delivery of classified photographs to publisher). Whether the information is "related to the national defense" under this meaning is a question of fact for the jury to decide. Id. at 1073.

[1443] Gorin v. United States, 312, U.S. 9, 27-28 (1941) ("Where there is no occasion for secrecy, as with reports relating to national defense, published by authority of Congress or the military departments, there can, of course, in all likelihood be no reasonable intent to give an advantage to a foreign government.").

[1444] United States v. Squillacote, 221 F.3d 542, 578 (4th Cir. 2000).

[1445] Morison, 844 F.2d at 1064-65 (explaining that critical element distinguishing § 794 from § 793 is the requirement that disclosure be made to an agent of a foreign government rather than anyone not entitled to receive it).

imprisonment for any term of years or life, or under certain circumstances, the death penalty.[1446] The provision penalizes anyone who transmits defense information to a foreign government (or foreign political or military party) with the intent or reason to believe it will be used against the United States. It also prohibits attempts to elicit information related to the public defense "which might be useful to the enemy."[1447] The death penalty is available only upon a finding that the offense resulted in the death of a covert agent or directly concerns nuclear weapons or other particularly sensitive types of information. The death penalty is also available under § 794 for violators who gather, transmit or publish information related to military plans or operations and the like during time of war, with the intent that the information reach the enemy.[1448] These penalties are available to punish any person who participates in a conspiracy to violate the statute. Offenders are also subject to forfeiture of any ill-gotten gains and property used to facilitate the offense.[1449]

The unauthorized creation, publication, sale or transfer of photographs or sketches of vital defense installations or equipment as designated by the

---

[1446] § 794. Gathering or delivering defense information to aid foreign government (a) Whoever, with intent or reason to believe that it is to be used to the injury of the United States or to the advantage of a foreign nation, communicates, delivers, or transmits ... to any foreign government, or to any faction or party or military or naval force within a foreign country, whether recognized or unrecognized by the United States, or to any representative, officer, agent, employee, subject, or citizen thereof, either directly or indirectly, any document [or other protected thing], or information relating to the national defense, shall be punished by death or by imprisonment for any term of years or for life, except that the sentence of death shall not be imposed unless the jury or ... the court, further finds that the offense resulted in the identification by a foreign power (as defined in section 101(a) of the Foreign Intelligence Surveillance Act of 1978 [50 U.C.S. § 1801(a)]) of an individual acting as an agent of the United States and consequently in the death of that individual, or directly concerned nuclear weaponry, military spacecraft or satellites, early warning systems, or other means of defense or retaliation against large-scale attack; war plans; communications intelligence or cryptographic information; or any other major weapons system or major element of defense strategy.

[1447] § 794(b) provides: (b) Whoever, in time of war, with intent that the same shall be communicated to the enemy, collects, records, publishes, or communicates, or attempts to elicit any information with respect to the movement, numbers, description, condition, or disposition of any of the Armed Forces, ships, aircraft, or war materials of the United States, or with respect to the plans or conduct, or supposed plans or conduct of any naval or military operations, or with respect to any works or measures undertaken for or connected with, or intended for the fortification or defense of any place, or any other information relating to the public defense, which might be useful to the enemy, shall be punished by death or by imprisonment for any term of years or for life....

[1448] During time of war, any individual who communicates intelligence or any other information to the enemy may be prosecuted by the military for aiding the enemy under Article 104 of the Uniform Code of Military Justice (UCMJ), and if convicted, punished by "death or such other punishment as a court-martial or military commission may direct." 10 U.S.C. § 904.

[1449] 18 U.S.C. § 794(d). Proceeds go to the Crime Victims Fund.

President is prohibited by 18 U.S.C. §§ 795 and 797.[1450] Violators are subject to fine or imprisonment for not more than one year, or both.

The knowing and willful disclosure of certain classified information is punishable under 18 U.S.C. § 798 by fine and/or imprisonment for not more than 10 years.[1451] To incur a penalty, the disclosure must be prejudicial to the safety or interests of the United States or work to the benefit of any foreign government and to the detriment of the United States. The provision applies only to information related to cryptographic systems or communications intelligence that is specially designated by a U.S. government agency for "limited or restricted dissemination or distribution."[1452]

Other Statutes

[1450] § 795. Photographing and sketching defense installations (a) Whenever, in the interests of national defense, the President defines certain vital military and naval installations or equipment as requiring protection against the general dissemination of information relative thereto, it shall be unlawful to make any photograph, sketch, picture, drawing, map, or graphical representation of such vital military and naval installations or equipment without first obtaining permission of the commanding officer of the military or naval post, camp, or station, or naval vessels, military and naval aircraft, and any separate military or naval command concerned, or higher authority, and promptly submitting the product obtained to such commanding officer or higher authority for censorship or such other action as he may deem necessary.... § 797. Publication and sale of photographs of defense installations On and after thirty days from the date upon which the President defines any vital military or naval installation or equipment as being within the category contemplated under section 795 of this title [18], whoever reproduces, publishes, sells, or gives away any photograph, sketch, picture, drawing, map, or graphical representation of the vital military or naval installations or equipment so defined, without first obtaining permission of the commanding officer ... or higher authority, unless such photograph, sketch, picture, drawing, map, or graphical representation has clearly indicated thereon that it has been censored by the proper military or naval authority, shall be fined under this title or imprisoned not more than one year, or both.

[1451] § 798. Disclosure of classified information (a) Whoever knowingly and willfully communicates, furnishes, transmits, or otherwise makes available to an unauthorized person, or publishes, or uses in any manner prejudicial to the safety or interest of the United States or for the benefit of any foreign government to the detriment of the United States any classified information—-(1) concerning the nature, preparation, or use of any code, cipher, or cryptographic system of the United States or any foreign government; or (2) concerning the design, construction, use, maintenance, or repair of any device, apparatus, or appliance used or prepared or planned for use by the United States or any foreign government for cryptographic or communication intelligence purposes; or (3) concerning the communication intelligence activities of the United States or any foreign government; or (4) obtained by the processes of communication intelligence from the communications of any foreign government, knowing the same to have been obtained by such processes—-Shall be fined ... or imprisoned not more than ten years, or both.

[1452] 18 U.S.C. § 798(b).

18 U.S.C. § 1030(a)(1) punishes the willful retention, communication, or transmission, etc., of classified information retrieved by means of knowingly accessing a computer without (or in excess of) authorization, with reason to believe that such information "could be used to the injury of the United States, or to the advantage of any foreign nation." Receipt of information procured in violation of the statute is not addressed, but depending on the specific facts surrounding the unauthorized access, criminal culpability might be asserted against persons who did not themselves access a government computer as conspirators, aiders and abettors, or accessories after the fact.[1453] The provision imposes a fine or imprisonment for not more than 10 years, or both, in the case of a first offense or attempted violation. Repeat offenses or attempts can incur a prison sentence of up to 20 years.

18 U.S.C. § 641 punishes the theft or conversion of government property or records for one's own use or the use of another. While this section does not explicitly prohibit disclosure of classified information, it has been used to prosecute "leakers."[1454] Violators may be fined, imprisoned for not more than 10 years, or both, unless the value of the property does not exceed the sum of $100, in which case the maximum prison term is one year. The statute also covers knowing receipt or retention of stolen or converted property with the intent to convert it to the recipient's own use. It does not appear to have been used to prosecute any recipients of classified information even where the original discloser was charged under the statute.

50 U.S.C. § 421 provides for the protection of information concerning the identity of covert intelligence agents.[1455] It generally covers persons authorized to know

---

[1453] For more information about conspiracy law, see CRS Report R41223, Federal Conspiracy Law: A Brief Overview, by Charles Doyle.

[1454] See United States v. Morison, 844 F.2d 1057 (4th Cir. 1988)(photographs and reports were tangible property of the government); United States v. Fowler, 932 F.2d 306 (4th Cir. 1991)("information is a species of property and a thing of value" such that "conversion and conveyance of governmental information can violate § 641," citing United States v. Jeter, 775 F.2d 670, 680-82 (6th Cir. 1985)); United States v. Girard, 601 F.2d 69, 70-71 (2d Cir. 1979). The statute was used to prosecute a DEA official for leaking unclassified but restricted documents pertinent to an agency investigation. See Dan Eggen, If the Secret's Spilled, Calling Leaker to Account Isn't Easy, WASH. POST, Oct. 3, 2003, at A5 (reporting prosecution of Jonathan Randel under conversion statute for leaking government documents to journalist).

[1455] The Intelligence Identities and Protection Act of 1982, codified at 50 U.S.C. §§ 421-26. For more information, see CRS Report RS21636, Intelligence Identities Protection Act, by Elizabeth B. Bazan. The term "covert agent" is defined to include a non-U.S. citizen "whose past or present intelligence relationship to the United States is classified information and who is a present or former agent of, or a present or former informant or source of operational assistance to, an intelligence agency." 50 U.S.C. § 426(4)(c). "Intelligence agency" is defined to include a "foreign intelligence component of the Department of Defense"; informant means "any individual who furnishes information to an intelligence agency in the course of a confidential relationship." 50

the identity of such agents, but can also apply to a person who learns of the identity of a covert agent through a "pattern of activities intended to identify and expose covert agents" and discloses the identity to any individual not authorized access to classified information, with reason to believe that such activities would impair U.S. foreign intelligence efforts. This crime is subject to a fine or imprisonment for a term of not more than three years. To be convicted, a violator must have knowledge that the information identifies a covert agent whose identity the United States is taking affirmative measures to conceal. To date, there have been no reported cases interpreting the statute, but it did result in one conviction pursuant to a guilty plea.[1456]

There appears to be no statute that generally proscribes the acquisition or publication of diplomatic cables, although government employees who disclose such information without proper authority may be subject to prosecution. 18 U.S.C. § 952 punishes employees of the United States who, without authorization, willfully publish or furnish to another any official diplomatic code or material prepared in such a code, by imposing a fine, a prison sentence (up to 10 years), or both. The same punishment applies for materials "obtained while in the process of transmission between any foreign government and its diplomatic mission in the United States,"[1457] but not, apparently, materials obtained during transmission from U.S. diplomatic missions abroad to the State Department or vice versa (unless the material was or purports to have been prepared using an official diplomatic code – it is unclear whether messages that are encrypted for transmission are covered).

Analysis

In light of the foregoing, it seems that there is ample statutory authority for prosecuting individuals who elicit or disseminate most of the documents at issue, as long as the intent element can be satisfied and potential damage to national security can be demonstrated.[1458] There is some authority, however, for

---

U.S.C. § 426(5-6). The definitions suggest that the act is intended to protect the identities of persons who provide intelligence information directly to a military counterintelligence unit, but perhaps they can be read to cover those who provide information to military personnel carrying out other functions who provide situation reports intended to reach an intelligence component. In any event, the extraterritorial application of the statute is limited to U.S. citizens and permanent resident aliens. 50 U.S.C. § 424.

[1456] See Richard B. Schmitt, Rare Statute Figures in Rove Case, LA TIMES, July 15, 2005, at A15 (reporting 1985 conviction of Sharon Scranage, a clerk for the CIA in Ghana, for disclosing identities of covert agents).

[1457] 18 U.S.C. § 952.

[1458] It appears the intent element is satisfied by proof that the material was obtained or disclosed "with intent or reason to believe that the information is to be used [or could be used] to the injury of the United States, or to the advantage of any foreign nation." 18 U.S.C. §§ 793 and 794. This has

interpreting 18 U.S.C. § 793, which prohibits the communication, transmission, or delivery of protected information to anyone not entitled to possess it, to exclude the "publication" of material by the media.[1459] Publication is not expressly proscribed in 18 U.S.C. § 794(a), either, although it is possible that publishing covered information in the media could be construed as an "indirect" transmission of such information to a foreign party, as long as the intent that the information reach said party can be demonstrated.[1460] The death penalty is available under that subsection if the offense results in the identification and subsequent death of "an individual acting as an agent of the United States,"[1461] or the disclosure of information relating to certain other broadly defined defense matters. The word "publishes" does appear in 18 U.S.C. § 794(b), which applies to wartime disclosures of information related to the "public defense" that "might be useful to the enemy" and is in fact intended to be communicated to the enemy. The types of information covered seem to be limited to military plans and information about fortifications and the like, which may exclude data related to purely historical matters.

Moreover, the statutes described in the previous section have been used almost exclusively to prosecute individuals with access to classified information (and a corresponding obligation to protect it) who make it available to foreign agents, or to foreign agents who obtain classified information unlawfully while present in the United States. Leaks of classified information to the press have only rarely been punished as crimes, and we are aware of no case in which a publisher of information obtained through unauthorized disclosure by a government employee has been prosecuted for publishing it. There may be First Amendment

---

been interpreted to require the prosecution to demonstrate a "bad purpose." See United States v. Morison, 844 F.2d 1057, 1071 ("An act is done willfully if it is done voluntarily and intentionally and with the specific intent to do something that the law forbids. That is to say, with a bad purpose either to disobey or to disregard the law."). If any of the disclosed material involves communications intelligence as described in 18 U.S.C. § 798, the conduct must be undertaken knowingly and willfully to meet the intent threshold.

[1459] See New York Times Co. v. United States, 403 U.S. 713, 721-22 (1971) (Douglas, J., concurring) (rejecting government argument that term "communicate" should be read to include "publish," based on conspicuous absence of the term "publish" in that section of the Espionage Act and legislative history demonstrating Congress had rejected an effort to reach publication).

[1460] See Harold Edgar and Benno C. Schmidt, Jr., Curtiss-Wright Comes Home: Executive Power and National Security Secrecy, 21 HARV. C.R.-C.L. L. REV. 349, 395 (1986) (questioning whether Espionage Act can be construed to except publication).

[1461] The data released by WikiLeaks contains some names of Afghans who assisted Coalition Forces, leading to some concern that the Taliban might use the information to seek out those individuals for retaliation. See Eric Schmitt and David E. Sanger, Gates Cites Peril in Leak of Afghan War Logs, N.Y. TIMES, Aug. 2, 2010, at 4. The New York Times, The Guardian, and Der Spiegel published excerpts of the database, but did not publish the names of individual Afghans. Id. No deaths have yet been tied to the leaks. See Robert Burns, Pentagon Sees Deadly Risk in Wikileaks Disclosures, AP NEWSWIRE, Aug. 17, 2010. There appears to be no court precedent interpreting "agent of the United States" in the context of18 U.S.C. § 794(a).

implications that would make such a prosecution difficult, not to mention political ramifications based on concerns about government censorship. To the extent that the investigation implicates any foreign nationals whose conduct occurred entirely overseas, any resulting prosecution may carry foreign policy implications related to the exercise of extraterritorial jurisdiction and whether suspected persons may be extradited to the United States under applicable treaty provisions.

Jurisdictional Reach of Relevant Statutes

The Espionage Act gives no express indication that it is intended to apply extraterritorially, but courts have not been reluctant to apply it to overseas conduct of Americans, in particular because Congress in 1961 eliminated a provision restricting the act to apply only "within the admiralty and maritime jurisdiction of the United States and on the high seas, as well as within the United States."[1462] This does not answer the question whether the act is intended to apply to foreigners outside the United States. Because espionage is recognized as a form of treason,[1463] which generally applies only to persons who owe allegiance to the United States, it might be supposed that Congress did not regard it as a crime that could be committed by aliens with no connection to the United States. However, the only court that appears to have addressed the question concluded otherwise.[1464] A district court judge held in 1985 thata citizen of East Germany could be prosecuted under §§ 793(b), 794(a) and 794(c) for having (1) unlawfully sought and obtained information regarding the U.S. national defense, (2) delivered that information to his own government, and (3) conspired to do so with the intent that the information be used to the injury of the United States or to the advantage of the German Democratic Republic, all of which offenses were committed within East Germany or in Mexico. The court rejected the defendant's contention that construing the act to cover him would permit the prosecution of noncitizens "who might merely have reviewed defense documents supplied to them by their respective governments."[1465] The court considered the scenario unlikely, stating:

[1462] See United States v. Zehe, 601 F. Supp. 196, 198 (D.C. Mass. 1985)(citing former 18 U.S.C. § 791 repealed by P.L. 87-369, 75 Stat. 795(1961)).

[1463] See 70 AM. JUR. 2D Sedition, Subversive Activities and Treason § 15 (2005). Courts have not been persuaded that the Treason Clause of the Constitution requires the safeguards associated with treason apply also to similar crimes such as espionage or levying war against the United States. See id., United States v. Rosenberg, 195 F.2d 583 (2d. Cir.), cert. denied, 344 U.S. 838 (1952)(espionage); United States v. Rodriguez, 803 F.2d 318 (7th Cir.), cert. denied, 480 U.S. 908 (1986) (levying war).

[1464] Zehe at 198 ("Espionage against the United States, because it is a crime that by definition threatens this country's security, can therefore be punished by Congress even if committed by a noncitizen outside the United States.").

[1465] Id. at 199.

Under the statutorily defined crimes of espionage in §§ 793 and 794, noncitizens would be subject to prosecution only if they actively sought out and obtained or delivered defense information to a foreign government or conspired to do so.[1466]

Under this construction, it is possible that noncitizens involved in publishing materials disclosed to them by another would be subject to prosecution only if it can be demonstrated that they took an active role in obtaining the information. The case was not appealed. The defendant, Dr. Alfred Zehe, pleaded guilty in February, 1985 and was sentenced to eight years in prison, but was traded as part of a "spy swap" with East Germany in June of that year.[1467]

Application of the Espionage Act to persons who do not hold a position of trust with the government, outside of the classic espionage scenario (in which an agent of a foreign government delivers damaging information to such hostile government), has been controversial. The only known case of that type involved two pro-Israel lobbyists in Washington, Steven J. Rosen and Keith Weissman, associated with the American Israel Public Affairs Committee (AIPAC), who were indicted in 2005 for conspiracy to disclose national security secrets to unauthorized individuals, including Israeli officials, other AIPAC personnel, and a reporter for the Washington Post.[1468] Their part in the conspiracy amounted to receiving information from government employees with knowledge that the employees were not authorized to disclose it.[1469] The prosecution was criticized for effectively "criminalizing the exchange of information,"[1470] based in part on the government's theory that the defendants were guilty of solicitation of classified information because they inquired into matters they knew their government informant was not permitted to discuss, something that many journalists consider to be an ordinary part of their job.[1471] Charges were

---

[1466] Id.

[1467] Henry Giniger and Milt Freudenheim, Free to Spy Another Day?, NY TIMES, Jun 16, 1985, at A.4.

[1468] See United States v. Rosen, 445 F. Supp. 2d 602 (E.D. Va. 2006); Jerry Markon, U.S. Drops Case Against Ex-Lobbyists, WASH. POST, May 2, 2009, at A1 (stating the case is the first prosecution under the Espionage Act against civilians not employed by the government).

[1469] See William E. Lee, Deep Background: Journalists, Sources, and the Perils of Leaking, 57 AM. U. L. REV. 1453, 1519 (2007) (opining that "the conspiracy charge especially threatens reporter-source transactions where the reporter promises not to disclose the identity of the source").

[1470] Time to Call It Quits, WASH. POST, March 11, 2009 (editorial urging Attorney General to drop charges).

[1471] See William E. Lee, Probing Secrets: The Press and Inchoate Liability for Newsgathering Crimes, 36 AM. J. CRIM. L. 129, 132-34 (2009). The solicitation theory relied on a 2008 Supreme Court case finding that solicitation of an illegal transaction is not speech deserving of First

eventually dropped, reportedly due to a judge's ruling regarding the government's burden of proving the requisite intent and concerns that classified information would have to be disclosed at trial.[1472]

Extradition Issues[1473]

Assuming that the Espionage Act does apply to foreign nationals for their conduct overseas, there may be several legal obstacles to the extradition of such a suspect to the United States to face charges under the statute, including the possibility that the crime constitutes a political offense for which extradition is unavailable. Extradition to or from the United States is almost exclusively a creature of treaty. The United States has extradition treaties with more than 100 countries, although there are many countries with which it does not.[1474] In addition to providing an explicit list of crimes for which extradition may be granted, most modern extradition treaties also identify various classes of offenses and situations for which extradition may or must be denied.

The "political offense" exception has been a common feature of extradition treaties for almost a century and a half, and the exception appears to be contained in every modern U.S. extradition treaty.[1475] A political offense may be

---

Amendment protection. United States v. Williams, 553 U.S. 285 (2008). See id. at 133 (citing Brief of the United States at 43-44, United States v. Rosen, 557 F.3d 192 (4th Cir. 2008) (No. 08-4358)). Williams had to do with solicitation of child pornography, but Justice Scalia posed as a rhetorical question whether Congress could criminalize solicitation of information thought to be covered by the Espionage Act: Is Congress prohibited from punishing those who attempt to acquire what they believe to be national-security documents, but which are actually fakes? To ask is to answer. Williams at 304.

[1472] See Markon, supra footnote 52 (quoting Dana J. Boente, the acting U.S. attorney in Alexandria, VA, where the trial was scheduled to take place). The judge found the scienter requirement of 18 U.S.C. § 793 to require that the defendants must have reason to believe the communication of the information at issue "could be used to the injury of the United States or to the advantage of any foreign nation." 445 F. Supp. 2d at 639. Moreover, the judge limited the definition of "information related to the national defense" to information that is "potentially damaging to the United States or ... useful to an enemy of the United States." Id. (citing United States v. Morison, 844 F.2d 1057, 1084 (4th Cir. 1988) (Wilkinson, J., concurring)).

[1473] This section is contributed by Michael John Garcia, Legislative Attorney.

[1474] A current list of countries with which the United States has an extradition treaty is found in CRS Report 98-958, Extradition To and From the United States: Overview of the Law and Recent Treaties, by Michael John Garcia and Charles Doyle, at Appendix A.

[1475] See, e.g., Australian Extradition Treaty, art. VII(1), entered into force May 8, 1976, 27 U.S.T. 957 ("Extradition shall not be granted ... when the offense in respect of which extradition is requested is of a political character, or the person whose extradition is requested proves that the extradition request has been made for the purpose of trying or punishing him for an offense of a political character."); Norwegian Extradition Treaty, entered into force Mar. 7, 1980, 31 U.S.T. 5619 (similar); United Kingdom Extradition Treaty, art. 4, entered into force Apr. 26, 2007, S. TREATY DOC. 108-23 ("Extradition shall not be granted if the offense for which extradition is

characterized as a pure political offense, or one that is directed singularly at a sovereign entity and does not have the features an ordinary crime (e.g., there is no violation of the private rights of individuals),[1476] or as a relative political offense, meaning an "otherwise common crime[] committed in connection with a political act ... or common crimes ... committed for political motives or in a political context."[1477]

The political offense exception may pose a significant obstacle to the extradition of a foreign national to the United States to face charges under the Espionage Act. Espionage, along with treason and sedition, has been recognized as a quintessential example of a purely political offense,[1478] although this recognition may arguably apply only to the "classic case" of espionage on behalf of a foreign government by one who owes allegiance to the aggrieved government.[1479] Even if the political offense exception applies to the unauthorized disclosure of national defense information, however, the United States could still seek the extradition of a suspect to face other criminal charges (though it would likely be unable to try the fugitive for an offense other than the one for which he was extradited),[1480]

---

requested is a political offense."); ."); Swedish Extradition Treaty, art. 5, entered into force Dec. 3, 1963, 14 U.S.T. 1845 ("Extradition shall not be granted....[i]f the offense is regarded by the requested State as a political offense or as an offense connected with a political offense.").

[1476] Quinn v. Robinson, 783 F.2d 776, 791 (9th Cir. 1986). See also M. CHERIF BASSIOUNI, INTERNATIONAL EXTRADITION: UNITED STATES LAW AND PRACTICE (BASSIOUNI) 604 (5th ed. 2007).604; Charles Cantrell, The Political Offense Exception to Extradition: A Comparison of the United States, Great Britain and the Republic of Ireland, 60 MARQ. L. REV. 777, 780 (1977).

[1477] Quinn, 783 F.2d at 791 (internal citations omitted).

[1478] See, e.g., Quinn, 783 F.2d at 791 (citing treason, sedition, and espionage as examples of purely political offenses); BASSIOUNI, supra footnote 60, at 604.

[1479] It might be argued that certain offenses punishable under the Espionage Act do not fall under the traditional conception of "espionage," and should therefore not be deemed to be pure political offenses per se. See generally PIETRO VERRI, DICTIONARY OF THE INTERNATIONAL LAW OF ARMED CONFLICT 47 (1992) (espionage is "commonly applied to the efforts made in territory under enemy control by a party to the conflict to collect all information on the enemy that may be useful to the conduct of the war in general and to that of hostilities in particular....The word espionage is also applied to the collection by States, in peacetime as well as in time of war, of political and military information regarding each other."); Lt. Col. Geoffrey B. Demarest, Espionage in International Law, 24 DENV. J. INT'L L. & POL'Y 321, 324 (1996) ("Throughout history, the terms 'espionage' and 'spying' have carried varying amounts of pejorative baggage. Therefore, any attempt at a precise definition is difficult."). Nonetheless, such an offense might still be deemed to be sufficiently related to political action or informed by political motivations so as to fall under the political offense exception.

[1480] Under the doctrine of specialty, sometimes called speciality, "a person who has been brought within the jurisdiction of the court by virtue of proceedings under an extradition treaty, can only be tried for one of the offences described in that treaty, and for the offence with which he is charged in the proceedings for his extradition, until a reasonable time and opportunity have been

although extradition might be refused if the charged conduct is deemed to have been committed in furtherance of an act of espionage (or other political offense).[1481]

Extradition is also generally limited to crimes identified in the relevant treaty. Early extradition treaties concluded by the United States typically listed specific crimes constituting extraditable offenses. More recent agreements often adopt a dual criminality approach, in which extradition is available when each party recognizes a particular form of misconduct as a punishable offense (subject to other limitations found elsewhere in the applicable extradition treaty).[1482] No U.S. extradition treaty currently in force lists espionage as an extraditable offense.[1483] Assuming for the sake of argument that certain espionage offenses are not per se political offenses for which extradition may not be granted, it would appear that the United States could only seek the extradition of a foreign national for an espionage offense if the applicable treaty authorized extradition in cases of dual criminality, and the requested state recognized espionage (or perhaps unauthorized receipt or disclosure of protected government information) as a criminal offense under its domestic laws.

Whether extradition is available for an offense occurring outside the United States may depend in part upon whether the applicable treaty covers extraterritorial offenses. As a general rule, crimes are defined by the laws of the place where they are committed.[1484] Nations have always been understood to have authority to outlaw and punish conduct occurring outside the confines of

---

given him after his release or trial upon such charge, to return to the country from whose asylum he had been forcibly taken under those proceedings." United States v. Alvarez-Machain, 504 U.S. 655, 661 (1992) (quoting United States v. Rauscher, 119 U.S. 407, 430 (1886)). This limitation is expressly included in many treaties.

[1481] 18 U.S.C. § 641

[1482] E.g., Extradition Agreement with the European Union, art. 4(1), entered into force Feb. 1, 2010, S. TREATY DOC. 109-14 (applying in place of any provision in an earlier extradition agreement between the United States and an EU Member State which only authorized extradition only an exclusive list of offenses, and instead providing that "An offense shall be an extraditable offense if it is punishable under the laws of the requesting and requested States by deprivation of liberty for a maximum period of more than one year or by a more severe penalty"); Protocol to Australian Extradition Treaty, entered into force Dec. 21, 1992, art. 1, S. TREATY DOC. 102-23 (replacing provision of earlier extradition agreement listing specific offenses where extradition was available with a provision requiring dual criminality).

[1483] It should be noted, however, that extradition treaties may cover certain offenses that can constitute elements of the crime of espionage (e.g., knowingly receiving or fraudulently obtaining property). See, e.g., Extradition Treaty with Belize, appendix listing extraditable offenses, entered into force March 27, 2001, S. TREATY DOC. 106-38,

[1484] See CRS Report 94-166, Extraterritorial Application of American Criminal Law, by Charles Doyle.

their own territory under some circumstances, but the United States now claims more sweeping extraterritorial application for some of its criminal laws than is recognized either in its more historic treaties or by many of today's governments.[1485] This may complicate any extradition efforts because many U.S. extradition treaties apply only to crimes "committed within the [territorial] jurisdiction" of the country seeking extradition.[1486] Some contemporary treaties call for extradition regardless of where the offense was committed, while perhaps an equal number permit or require denial of an extradition request that falls within an area where the countries hold conflicting views on extraterritorial jurisdiction.[1487]

The extradition of a foreign national to the United States to face criminal charges may be impeded by nationality provisions contained in extradition treaties with many countries, which recognize the right of a requested party to refuse to extradite its own nationals. U.S. extradition agreements generally are either silent with respect to nationality, in which case all persons are subject to extradition without regard to their nationality, or they contain a nationality clause that specifies that parties are not bound to deliver up their own nationals, in some cases leaving room for executive discretion.[1488] Some newer treaties declare that "extradition shall not be refused based on the nationality of the person sought," while others limit the nationality exemption to nonviolent crimes or bar nationality from serving as the basis to deny extradition when the fugitive is sought in connection with a listed offense.

The ability of the United States to obtain the extradition of a foreign national for a criminal offense may also be impacted by the existence of competing extradition requests made by other States. The criteria used by a requested State to determine the precedence given to competing extradition requests may be established either by its domestic laws or via its extradition treaties with the requesting countries.[1489] If the requested State opts to give priority to the

---

[1485] See CRS Report 98-958, Extradition To and From the United States: Overview of the Law and Recent Treaties, by Michael John Garcia and Charles Doyle. Even among countries holding fairly expansive views of the extraterritorial jurisdiction, there may be substantial differences between the perceptions of common law countries and those of civil law countries, Charles L. Blakesley, A Conceptual Framework for Extradition and Jurisdiction Over Extraterritorial Crimes, 1984 UTAH L. REV. 685 (1984).

[1486] IV Michael Abbell & Bruno A. Ristau, International Judicial Assistance: Criminal 64-7 (1990).

[1487] For examples of specific treaties, see CRS Report 98-958, Extradition To and From the United States: Overview of the Law and Recent Treaties.

[1488] BASSIOUNI, supra footnote 60, at 739.

[1489] Extradition Agreement with the European Union, art. 10, entered into force Feb. 1, 2010, S. TREATY DOC. 109-14 (describing factors to be considered by requested State when considering

extradition request of another country, it might still be possible for the United States to obtain the extradition of the fugitive at a later date. Whether a fugitive extradited to one State can thereafter be extradited to a third country may depend upon the applicable treaties between the relevant States. Some extradition agreements authorize the requesting State to re-extradite a person to a third country in certain circumstances. Generally, re-extradition is only permitted when the State from whom extradition was initially obtained consents to the re-extradition of the fugitive, or the fugitive voluntarily remains in the State where he was initially extradited for a specified period after having been released from custody.[1490]

Constitutional Issues

The publication of information pertaining to the national defense or foreign policy may serve the public interest by providing citizens with information necessary to shed light on the workings of government, but it seems widely accepted that the public release of at least some of such information poses a significant enough threat to the security of the nation that the public interest is better served by keeping it secret. The Constitution protects the public right to access government information and to express opinions regarding the functioning of the government, among other things, but it also charges the government with "providing for the common defense." Policymakers are faced with the task of balancing these interests.

The First Amendment to the U.S. Constitution provides: "Congress shall make no law ... abridging the freedom of speech, or of the press...."[1491] Despite this absolute language, the Supreme Court has held that "[t]he Government may ... regulate the content of constitutionally protected speech in order to promote a

---

competing extradition requests from the United States or other EU Member States); Bolivian Extradition Treaty, art. X, entered into force Nov. 21, 1996, S. TREATY DOC. 104-22.

[1490] See, e.g., Swedish Extradition Treaty, art. IX, entered into force Dec. 3, 1963, 14 U.S.T. 1845 ("A person extradited by virtue of this Convention may not be tried or punished by the requesting State for any offense committed prior to his extradition, other than that which gave rise to the request, nor may he be re-extradited by the requesting State to a third country which claims him, unless the surrendering State so agrees or unless the person extradited, having been set at liberty within the requesting State, remains voluntarily in the requesting State for more than 45 days from the date on which he was released. Upon such release, he shall be informed of the consequences to which his stay in the territory of the requesting State might subject him."); Turkish Extradition Treaty, art. 17, entered into force Jan. 1, 1987, 32 UST 2111 (similar). See also Council of Europe, Convention on Extradition, art. 15, done Dec. 13, 1957 (providing similar requirements for re-extradition among member States of the Council of Europe), available at http://conventions.coe.int/ Treaty/EN/Treaties/Html/024.htm.

[1491] For an analysis of exceptions to the First Amendment, see CRS Report 95-815, Freedom of Speech and Press: Exceptions to the First Amendment, by Kathleen Ann Ruane.

compelling interest if it chooses the least restrictive means to further the articulated interest."[1492]

Where speech is restricted based on its content, the Supreme Court generally applies "strict scrutiny," which means that it will uphold a content-based restriction only if it is necessary "to promote a compelling interest," and is "the least restrictive means to further the articulated interest."[1493] Protection of the national security from external threat is without doubt a compelling government interest.[1494] It has long been accepted that the government has a compelling need to suppress certain types of speech, particularly during time of war or heightened risk of hostilities.[1495] Speech likely to incite immediate violence, for example, may be suppressed.[1496] Speech that would give military advantage to a foreign enemy is also susceptible to government regulation.[1497]

Where First Amendment rights are implicated, it is the government's burden to show that its interest is sufficiently compelling to justify enforcement. Whether the government has a compelling need to punish disclosures of classified information turns on whether the disclosure has the potential of causing damage to the national defense or foreign relations of the United States.[1498] Actual damage need not be proved, but potential damage must be more than merely speculative and incidental.[1499] On the other hand, the Court has stated that "state

---

[1492] Sable Communications of California v. Federal Communications Commission, 492 U.S. 115, 126 (1989).

[1493] Id.

[1494] See Haig v. Agee, 453 U.S. 280 (1981) ("It is 'obvious and unarguable' that no governmental interest is more compelling than the security of the Nation.")(citing Aptheker v. Secretary of State, 378 U.S. 500, 509; accord Cole v. Young, 351 U.S. 536, 546 (1956)).

[1495] See Schenck v. United States, 249 U.S. 47 (1919) (formulating "clear and present danger" test).

[1496] Brandenburg v. Ohio, 395 U.S. 444 (1969).

[1497] Near v. Minnesota, 283 U.S. 697, 716 (1931) ("No one would question but that a government might prevent actual obstruction to its recruiting service or the publication of the sailing dates of transports or the number and location of troops.").

[1498] "National Security" is defined as national defense and foreign relations. See Exec. Order No. 13526, 75 Fed. Reg. 707 § 6.1(cc) (Jan. 5, 2010).

[1499] See, e.g., New York Times Co. v. United States, 403 U.S. 713, 725 (1971) (Brennan, J., concurring) (rejecting as insufficient government's assertions that publication of Pentagon Papers "could," "might," or "may" prejudice the national interest); Elrod v. Burns, 427 U.S. 347, 362 (1976) ("The interest advanced must be paramount, one of vital importance, and the burden is on the government to show the existence of such an interest.") (citing Buckley v. Valeo, 424 U.S. 1, 94(1976); Williams v. Rhodes, 393 U.S. 23, 31-33 (1968); NAACP v. Button, 371 U.S. 38, 45

action to punish the publication of truthful information seldom can satisfy constitutional standards."[1500] And it has described the constitutional purpose behind the guarantee of press freedom as the protection of "the free discussion of governmental affairs."[1501]

Although information properly classified in accordance with statute or executive order carries by definition, if disclosed to a person not authorized to receive it, the potential of causing at least identifiable harm to the national security of the United States,[1502] it does not necessarily follow that government classification by itself will be dispositive of the issue in the context of a criminal trial. However, courts have adopted as an element of the espionage statutes a requirement that the information at issue must be "closely held."[1503] Government classification will

---

(1963); Bates v. Little Rock, 361 U.S. 516, 524 (1960); NAACP v. Alabama, 357 U.S. 449, 464-466 (1958); Thomas v. Collins, 323 U.S. 516, 530 (1945)).

[1500] Bartnicki v. Vopper, 532 U.S. 514, 527 (2001) (citing Smith v. Daily Mail Publishing Co., 443 U.S. 97 (1979)).

[1501] Mills v. Alabama, 384 U.S. 214, 218 (1966). Because of the First Amendment purpose to protect the public's ability to discuss governmental affairs along with court decisions denying that it provides any special rights to journalists, e.g., Branzburg v. Hayes, 408 U.S. 665 (1972), it is not likely a plausible argument to posit that it does not apply to the foreign press. See United States v. 18 Packages of Magazines 238 F. Supp. 846, 847-848 (D.C. Cal. 1964) ("Even if it be conceded, arguendo, that the 'foreign press' is not a direct beneficiary of the Amendment, the concession gains nought for the Government in this case. The First Amendment does protect the public of this country. ... The First Amendment surely was designed to protect the rights of readers and distributors of publications no less than those of writers or printers. Indeed, the essence of the First Amendment right to freedom of the press is not so much the right to print as it is the right to read. The rights of readers are not to be curtailed because of the geographical origin of printed materials."). Likewise, the fact that WikiLeaks is not a typical newsgathering and publishing organization would likely make little difference under First Amendment analysis. The Supreme Court has not established clear boundaries between the protection of speech and that of the press, nor has it sought to develop criteria for identifying what constitutes "the press" that might qualify its members for privileges not available to anyone else. See generally CONGRESSIONAL RESEARCH SERVICE, THE CONSTITUTION OF THE UNITED STATES: ANALYSIS AND INTERPRETATION, SEN. DOC. NO. 108-17, at 1083-86 (2002), available at http://crs.gov/conan/default.aspx?mode=topic&doc= Amendment01.xml&t=2|3.

[1502] Exec. Order No. 13526, 75 Fed. Reg. 707 § 1.2 (Jan. 5, 2010) ("Classified National Security Information"). Sec. 1.3 defines three levels of classification: (1) "Top Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe. (2) "Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe. (3) "Confidential" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe.

[1503] United States v. Heine, 151 F.2d 813 (2d Cir.1945) (information must be "closely held" to be considered "related to the national defense" within the meaning of the espionage statutes).

likely serve as strong evidence to support that contention, even if the information seems relatively innocuous or does not contain much that is not already publicly known.[1504] Typically, courts have been unwilling to review decisions of the executive related to national security, or have made a strong presumption that the material at issue is potentially damaging.[1505] Still, judges have recognized that the government must make some showing that the release of specific national defense information has the potential of harming U.S. interests, lest the Espionage Act become a means to punish whistle-blowers who reveal information that poses more of a danger of embarrassing public officials than of endangering national security.[1506]

The Supreme Court seems satisfied that national security is a vital interest sufficient to justify some intrusion into activities that would otherwise be protected by the First Amendment—at least with respect to federal employees. Although the Court has not held that government classification of material is sufficient to show that its release is damaging to the national security,[1507] it has seemed to accept without much discussion the government's assertion that the material in question is damaging. It is unlikely that a defendant's bare assertion that information poses no danger to U.S. national security will be persuasive without some convincing evidence to that effect, or proof that the information is not closely guarded by the government.[1508]

A challenge to the Espionage Act has reached the Supreme Court for decision in only one instance. In Gorin v. United States,[1509] the Court upheld portions of the

---

[1504] See, e.g., United States v. Abu-Jihaad 600 F.Supp.2d 362, 385 -386 (D. Conn. 2009) (although completely inaccurate information might not be covered, information related to the scheduled movements of naval vessels was sufficient to bring materials within the ambit of national defense information).

[1505] See, e.g., Haig v. Agee, 453 U.S. 280, 291 (1981) ("Matters intimately related to foreign policy and national security are rarely proper subjects for judicial intervention.").

[1506] See, e.g., United States v. Morison, , 844 F.2d 1057, 1086 (4th Cir. 1988) (Phillips, J., concurring) ("... I assume we reaffirm today, that notwithstanding information may have been classified, the government must still be required to prove that it was in fact 'potentially damaging ... or useful,' i.e., that the fact of classification is merely probative, not conclusive, on that issue, though it must be conclusive on the question of authority to possess or receive the information. This must be so to avoid converting the Espionage Act into the simple Government Secrets Act which Congress has refused to enact.") (emphasis in original).

[1507] See, e.g., Scarbeck v. United States, 317 F.2d 546 (D.C. Cir. 1962) (holding government did not have to show documents were properly classified "as affecting the national defense" to convict employee under 50 U.S.C. § 783, which prohibits government employees from transmitting classified documents to foreign agents or entities).

[1508] See United States v. Dedeyan, 594 F.2d 36, 39 (4th Cir. 1978).

[1509] 312 U.S. 19 (1941).

act now codified as 18 U.S.C. §§ 793 and 794 against assertions of vagueness, but only because jury instructions properly established the elements of the crimes, including the scienter requirement (proof of "guilty knowledge") and a definition of "national defense" that includes potential damage in case of unauthorized release of protected information and materials. Gorin was a "classic case" of espionage, and did not involve a challenge based on the First Amendment right to free speech. The Court agreed with the government that the term "national defense" was not vague; it was satisfied that the term describes "a generic concept of broad connotations, referring to the military and naval establishments and the related activities of national preparedness."[1510] Whether information was "related to the national defense" was a question for the jury to decide,[1511] based on its determination that the information "may relate or pertain to the usefulness, efficiency or availability of any of the above places, instrumentalities or things for the defense of the United States of America. The connection must not be a strained one nor an arbitrary one. The relationship must be reasonable and direct."[1512] As long as the jury was properly instructed that only information likely to cause damage meets the definition of information "related to the national defense" for the purpose of the statute, the term was not unconstitutionally vague.

United States v. Morison[1513] is significant in that it represents the first case in which a person was convicted for selling classified documents to the media.[1514] Samuel Loring Morison, charged with providing classified satellite photographs to the British defense periodical Jane's Defence Weekly, argued that the espionage statutes did not apply to his conduct because he could not have had the requisite intent to commit espionage. The Fourth Circuit rejected his appeal, finding the intent to sell photographs that he clearly knew to be classified sufficient to satisfy the scienter requirement under 18 U.S.C. § 793(d) (disclosure by lawful possessor of defense information to one not entitled to receive it). The definition of "relating to the national defense" was not overbroad because the jury had been instructed that the government had the burden of showing that the

---

[1510] Id. at 28.

[1511] Id. at 32. The information defendant was charged with passing to the Soviet government had to do with U.S. intelligence on the activities of Japanese citizens in the United States.

[1512] Id. at 31.

[1513] 844 F.2d 1057 (4th Cir.), cert. denied, 488 U.S. 908 (1988).

[1514] Efforts to prosecute Daniel Ellsberg and Anthony Russo in connection with the disclosure of the Pentagon Papers were unsuccessful after the judge dismissed them for prosecutorial misconduct. More recently, a Defense Department employee pleaded guilty to charges under the Espionage Act for disclosing classified material to lobbyists and to journalists. United States v. Franklin, Cr. No. 05-225 (E.D. Va., 2005). For a description of these and other relevant cases, see Lee, supra footnote 53.

information was so related.[1515] His assertedly laudable motive in permitting publication of the photographs did not negate the element of intent.[1516]

The fact that the Morison prosecution involved a leak to the media with no obvious intent to transmit sensitive information to hostile intelligence services did not persuade the jury or the judges involved that he lacked culpability, but the Justice Department did come under some criticism on the basis that such prosecutions are so rare as to amount to a selective prosecution in his case, and that it raised concerns about the chilling effect such prosecutions could have on would-be whistle-blowers who could provide information embarrassing to the government but vital to public discourse.[1517] On leaving office, President Clinton pardoned Morison.[1518]

As far as the possible prosecution of the publisher of information leaked by a government employee is concerned, the most relevant case is likely to be the Pentagon Papers case.[1519] To be sure, the case involved an injunction against publication rather than a prosecution for having published information, but the rationale for protecting such disclosure may nevertheless inform any decision involving a conviction. In a per curiam opinion accompanied by nine concurring or dissenting opinions, the U.S. Supreme Court refused to grant the government's request for an injunction to prevent the New York Times and the Washington Post from printing a classified study of the U.S. involvement in Vietnam. The Court explained:

> *prior restraints are the most serious and least tolerable infringement on First Amendment rights.... A prior restraint, ... by*

[1515] But see Scarbeck v. United States, 317 F.2d 546 (D.C. Cir. 1962) (holding that government did not need to prove proper classification of documents to prove a violation).

[1516] 844 F.2d at 1073-74. Morison had stated that he sought the publication of the photos because they would demonstrate to the public the gravity of the threat posed by the Soviet Union, which he hoped would result in an increased defense budget. See P. Weiss, The Quiet Coup: U.S. v. Morison - A Victory for Secret Government, HARPER'S, September 1989.

[1517] See Jack Nelson, U.S. Government Secrecy and the Current Crackdown on Leaks 8, The Joan Shorenstein Center on the Press, Politics and Public Policy, Working Paper Series 2003-1 (2002), available at http://www.hks.harvard.edu/presspol/publications/papers/working_papers/2003_01_nelson.pdf.

[1518] Valerie Strauss, Navy Analyst Morison Receives a Pardon, WASH. POST, Jan. 21, 2001, at A17. Senator Daniel Patrick Moynihan wrote a letter in support of Morison's pardon and explaining his view that "An evenhanded prosecution of leakers could imperil an entire administration," and that "[i]f ever there were to be widespread action taken, it would significantly hamper the ability of the press to function." Letter, Sen. Daniel Patrick Moynihan to President Clinton, September 29, 1998, available at http://www.fas.org/sgp/news/2001/04/moynihan.html.

[1519] New York Times Co. v. United States, 403 U.S. 713 (1971) (per curiam).

> *definition, has an immediate and irreversible sanction. If it can be said that a threat of criminal or civil sanctions after publication "chills" speech, prior restraint "freezes" it at least for the time. The damage can be particularly great when the prior restraint falls upon the communication of news and commentary on current events.*[1520]

A majority of the justices suggested in separate dicta that the newspapers—along with the former government employee who leaked the documents to the press—could be prosecuted under the Espionage Act.[1521] Still, in later cases the Court stressed that any prosecution of a publisher for what has already been printed would have to overcome only slightly less insurmountable hurdles.[1522] Moreover, if national security interests were not sufficient to outweigh the First Amendment principles implicated in the prior restraint of pure speech related to the public interest, as in the Pentagon Papers case,[1523] it is difficult to discern an obvious rationale for finding that punishing that same speech after it has already been disseminated nevertheless tilts the balance in favor of the government's interest in protecting sensitive information.

The publication of truthful information that is lawfully acquired enjoys considerable First Amendment protection.[1524] The Court has not resolved the question "whether, in cases where information has been acquired unlawfully by a newspaper or by a source, government may ever punish not only the unlawful

---

[1520] Nebraska Press Association v. Stuart, 427 U.S. 539, 559 (1976) (striking down a court order restraining the publication or broadcast of accounts of confessions or admissions made by the defendant at a criminal trial).

[1521] 403 U.S. at 734-40 (White, J. with Stewart, J. concurring); id. at 745-47 (Marshall, J., concurring); id. at 752 (Burger, C.J., dissenting); id. at 752-59 (Harlan, J., joined by Burger, C.J. and Blackmun, J., dissenting). See David Topol, Note, United States v. Morison: A Threat to the First Amendment Right to Publish Security Information, 43 S.C. L. REV. 581, 586 (noting that three concurring justices suggested that the government could convict the newspapers under the Espionage Act even though it could not enjoin them from printing the documents, while the three dissenting justices thought the injunction should issue).

[1522] Smith v. Daily Mail Publishing Co., 443 U.S. 97, 102-03 (1979) ("Whether we view the statute as a prior restraint or as a penal sanction for publishing lawfully obtained, truthful in-formation is not dispositive because even the latter action requires the highest form of state interest to sustain its validity.") The case involved the prosecution of a newspaper for publishing the name of a juvenile defendant without court permission, in violation of state law.

[1523] For a list of the types of damage the government argued would ensue if its efforts to enjoin publication failed, see William H. Freivogel, Publishing National Security Secrets: The Case for "Benign Indeterminacy," 3 J. NAT'L SECURITY L. & POL'Y 95, 112-13 (2009).

[1524] See, e.g., Landmark Commc'ns. v. Virginia, 435 U.S. 829, 837 (1978).

acquisition, but the ensuing publication as well."[1525] (The Pentagon Papers Court did not consider whether the newspapers' receipt of the classified document was in itself unlawful, although it appeared to accept that the documents had been unlawfully taken from the government by their source).

The Court has established that "routine newsgathering" is presumptively lawful acquisition, the fruits of which may be published without fear of government retribution.[1526] However, what constitutes "routine newsgathering" has not been further elucidated. In the 2001 case Bartnicki v. Vopper, the Court cited the Pentagon Papers case to hold that media organizations cannot be punished (albeit in the context of civil damages) for divulging information on the basis that it had been obtained unlawfully by a third party.[1527] The holding suggests that recipients of unlawfully disclosed information cannot be considered to have obtained such material unlawfully based solely on their knowledge (or "reason to know") that the discloser acted unlawfully. Under such circumstances, disclosure of the information by the innocent recipient would be covered by the First Amendment, although a wrongful disclosure by a person in violation of an obligation of trust would receive no First Amendment protection, regardless of whether the information was obtained lawfully.[1528]

Bartnicki had to do with the disclosure of illegally intercepted communications in violation of federal and state wiretap laws, which prohibited disclosure of such information by anyone who knew or had reason to know that it was the product of an unlawful interception, but did not prohibit the receipt of such information. The Espionage Act, by contrast, does expressly prohibit the receipt of any national defense material with knowledge or reason to believe that it "is to be used to the injury of the United States, or to the advantage of any foreign nation" and that it was disclosed contrary to the provisions of the Espionage Act.[1529] This distinction could possibly affect whether a court would view the information as having been lawfully acquired; although the Bartnicki opinion seems to establish that knowledge that the information was unlawfully disclosed by the initial leaker cannot by itself make receipt or subsequent publication unlawful, it does not

---

[1525] Florida Star v. B.J.F. 491 U.S. 524, 535 (1989) . The Court also questioned whether the receipt of information can ever constitutionally be proscribed. Id. at 536.

[1526] Daily Mail, 443 U.S at 103. Here, routine newsgathering consisted of perusing publicly available court records.

[1527] 532 U.S. 514 (2001).

[1528] See Boehner v. McDermott, 484 F.3d 573 (D.C. Cir. 2007) (en banc) (Congressman, bound by Ethics Committee rules not to disclose certain information, had no First Amendment right to disclose to press contents of tape recording illegally made by third party).

[1529] 18 U.S.C. § 793(c).

directly address whether knowledge of the nature of the information received would bring about a different result.

Proposed Legislation

To date, one bill has been introduced to address disclosures of classified information of the type at issue in the WikiLeaks publications. The Securing Human Intelligence and Enforcing Lawful Dissemination Act' ("SHIELD Act"), S. 4004, introduced by Senator Ensign on December 2, 2010, would amend 18 U.S.C. § 798 to add coverage for disclosures of classified information related to human intelligence activities (the provision currently covers only certain information related to communications intelligence). The bill would add "transnational threat" to the entities whose benefit from unlawful disclosures would make such disclosure illegal. The statute as written prohibits disclosure of classified information for the benefit of any foreign government (or to the detriment of the United States, which would remain unchanged if the bill is enacted). A "transnational threat" for purposes of the bill means any "any transnational activity (including international terrorism, narcotics trafficking, the proliferation of weapons of mass destruction and the delivery systems for such weapons, and organized crime) that threatens the national security of the United States" or any person or group who engages in any of these activities. This change is likely intended to ensure that disclosures of any covered information that a violator "publishes, or uses in any manner … for the benefit" of Al Qaeda or any other terrorist group, international drug cartels, arms dealers who traffic in weapons of mass destruction, and other international criminals will be subject to prosecution, regardless of whether the group purports to govern any territory. As is currently the case, it is unclear whether this conduct must be undertaken "knowingly and willfully" to incur a punishment, or whether those qualifiers apply only to furnishing covered information to an unauthorized individual.

The bill would add two types of information to be covered by the prohibition: "information concerning the human intelligence activities of the United States or any foreign government"; and "information concerning the identity of a classified source or informant of an element of the intelligence community of the United States." "Human intelligence" is defined under the bill as "all procedures, sources, and methods employed in the collection of intelligence through human sources." "Classified information" would continue to be defined as "information which, at the time of a violation of this section, is, for reasons of national security, specifically designated by a United States Government Agency for limited or restricted dissemination or distribution." In other words, the information need not be classified information within the meaning of the executive order, so long as it has been specifically designated as subject to some form of restricted dissemination due to national security concerns. Because the concept of national security includes foreign affairs as well as national defense, the information covered may be broader than that already protected under the preceding sections of the Espionage Act. However, the limitation on the identity of informants and sources to those giving information to an element of the intelligence community

may be interpreted to exclude informants and sources who provide information to entities not listed in 50 U.S.C. § 401a(4), such as infantry units or consular offices.

Conclusion

The Espionage Act on its face applies to the receipt and unauthorized dissemination of national defense information, which has been interpreted broadly to cover closely held government materials related to U.S. military operations, facilities, and personnel. It has been interpreted to cover the activities of foreign nationals overseas, at least when they take an active part in seeking out information. Although cases involving disclosures of classified information to the press have been rare, it seems clear that courts have regarded such disclosures by government employees to be conduct that enjoys no First Amendment protection, regardless of the motives of the divulger or the value the release of such information might impart to public discourse.[1530] The Supreme Court has stated, however, that the question remains open whether the publication of unlawfully obtained information by the media can be punished consistent with the First Amendment. Thus, although unlawful acquisition of information might be subject to criminal prosecution with few First Amendment implications, the publication of that information remains protected. Whether the publication of national security information can be punished likely turns on the value of the information to the public weighed against the likelihood of identifiable harm to the national security, arguably a more difficult case for prosecutors to make.

[1530] The courts have permitted government agencies to enjoin their employees and former employees from publishing information they learned on the job, United States v. Marchetti, 466 F.2d 1309 (4th Cir.), cert. denied, 409 U.S. 1063 (1972), and permitted harsh sanctions against employees who publish even unclassified information in violation of an obligation to obtain pre-publication clearance, Snepp v. United States, 444 U.S. 507 (1980).

Protection of National Security Information Generally

The Protection of Classified Information: The Legal Framework, RS21900 (December 21, 2006).

JENNIFER K. ELSEA, CONGRESSIONAL RESEARCH SERV., THE PROTECTION OF CLASSIFIED INFORMATION: THE LEGAL FRAMEWORK (2006), *available at* http://www.intelligencelaw.com/library/secondary/crs/pdf/RS21900_12-21-2006.pdf.

Order Code RS21900
Updated December 21, 2006

Jennifer K. Elsea
Legislative Attorney
American Law Division

Summary

Recent incidents involving "leaks" of classified information have heightened interest in the legal framework that governs security classification, access to classified information, and penalties for improper disclosure. Classification authority has generally rested with the executive branch, although Congress has enacted legislation regarding the protection of certain sensitive information. While the Supreme Court has stated that the President has inherent constitutional authority to control access to sensitive information relating to the national defense or to foreign affairs, no court has found that Congress is without authority to legislate in this area. This report provides an overview of the relationship between executive and legislative authority over national security information, and summarizes the current laws and regulations that form the legal framework protecting classified information.

Background

Prior to the New Deal, classification decisions were left to military regulation.[1531] In 1940, President Franklin Roosevelt issued an executive order authorizing government officials to protect information pertaining to military and naval installations.[1532] Presidents since that time have continued to set the federal

---

[1531] See Harold Relyea, The Presidency and the People's Right to Know, in THE PRESIDENCY AND INFORMATION POLICY 1, 16-18 (1981).

[1532] Exec. Order No. 8,381 (1940).

government's classification standards by executive order, but with one critical difference: while President Roosevelt cited specific statutory authority for his action, later presidents have cited general statutory and constitutional authority.[1533]

The Supreme Court has never directly addressed the extent to which Congress may constrain the executive branch's power in this area. Citing the President's constitutional role as Commander-in-Chief,[1534] the Supreme Court has repeatedly stated in dicta that "[the President's] authority to classify and control access to information bearing on national security ... flows primarily from this Constitutional investment of power in the President and exists quite apart from any explicit congressional grant."[1535] This language has been interpreted by some to indicate that the President has virtually plenary authority to control classified information. On the other hand, the Supreme Court has suggested that "Congress could certainly [provide] that the Executive Branch adopt new [classification procedures] or [establish] its own procedures — subject only to whatever limitations the Executive Privilege may be held to impose on such congressional ordering."[1536] In fact, Congress established a separate regime in the Atomic Energy Act for the protection of nuclear-related "Restricted Data."[1537]

Congress has directed the President to establish procedures governing the access to classified material so that no person can gain such access without having

---

[1533] Compare Exec. Order No. 10,501 (1953) with, e.g. Exec. Order 13,292 (2003).

[1534] U.S. CONST., art. II, § 2.

[1535] Department of the Navy v. Egan, 484 U.S. 518, 527 (1988) (quoting Cafeteria Workers v. McElroy, 367 U.S. 886, 890 (1961). In addition, courts have also been wary to second-guess the executive branch in areas of national security. See, e.g., Haig v. Agee, 453 U.S. 280, 291 (1981) ("Matters intimately related to foreign policy and national security are rarely proper subjects for judicial intervention."). The Court has suggested, however, that it might intervene where Congress has provided contravening legislation. Egan at 530 ("Thus, unless Congress specifically has provided otherwise, courts traditionally have been reluctant to intrude upon the authority of the Executive in military and national security affairs.")(emphasis added).

[1536] EPA v. Mink, 410 U.S. 73, 83 (1973).

[1537] 42 U.S.C. § 2011 et seq. In addition, the Invention Secrecy Act (codified at 35 U.S.C. § 181 et seq.) authorizes the Commissioner of Patents to keep secret those patents on inventions in which the government has an ownership interest and the widespread knowledge of which would, in the opinion of the interested agency, harm national security. For a more detailed discussion of these and other regulatory regimes for the protection of sensitive government information, see CRS Report RL33502, Protection of National Security Information, by Jennifer K. Elsea; CRS Report RL33303: 'Sensitive But Unclassified' Information and Other Controls: Policy and Options for Scientific and Technical Information, by Genevieve J. Knezo.

undergone a background check.[1538] Congress also directed the President, in formulating the classification procedures, to adhere to certain minimum standards of due process with regard to access to classified information.[1539] These include the establishment of uniform procedures for, inter alia, background checks, denial of access to classified information, and notice of such denial.[1540] The statute also explicitly states that the agency heads are not required to comply with the due process requirement in denying or revoking an employee's security clearance where doing so could damage national security, although the statute directs agency heads to submit a report to the congressional intelligence committees in such a case.[1541]

With the authority to determine classification standards vested in the President, these standards tend to change whenever a new administration takes control of the White House.[1542] The differences between the standards of one administration and the next have often been dramatic. As one congressionally authorized commission put it in 1997:

> *The rules governing how best to protect the nation's secrets, while still insuring that the American public has access to information on the operations of its government, past and present, have shifted along with the political changes in Washington. Over the last fifty years, with the exception of the Kennedy Administration, a new executive order on classification was issued each time one of the political parties regained control of the Executive Branch. These*

[1538] Counterintelligence and Security Enhancement Act of 1994, Title VIII of P.L. 103-359 (codified at 50 U.S.C. § 435 et seq.). Congress has also required specific regulations regarding personnel \security procedures for employees of the National Security Agency, P.L. 88-290, 78 Stat. 168, codified at 50 U.S.C. §§ 831 -835. Congress has also prohibited the Department of Defense from granting or renewing security clearances for officers, employees, or contract personnel who had been convicted of a crime (and served at least one year prison time) and for certain other reasons, with a waiver possible only in "meritorious cases," P.L. 106-398 § 1, Div. A, Title X, § 1071(a), 114 Stat. 1654, 10 U.S.C. § 986.

[1539] 50 U.S.C. § 435(a).

[1540] Id.

[1541] Id. at § 435(b). The House Conference Report that accompanied this legislation in 1994 suggests that Congress understood that the line defining the boundaries of executive and legislative authority in this area is blurry at best. The conferees made explicit reference to the Egan case, expressing their desire that the legislation not be understood to affect the President's authority with regard to security clearances. See H.R. REP. 103-753, at 54.

[1542] See Report of the Commission on Protecting and Reducing Government Secrecy, S. DOC. NO. 105-2, at 11 (1997).

have often been at variance with one another ... at times even reversing outright the policies of the previous order.[1543]

Various congressional committees have investigated ways to bring some continuity to the classification system and to limit the President's broad powers to shield information from public examination.[1544] In 1966, Congress passed the Freedom of Information Act (FOIA), creating a presumption that government information will be open to the public unless it falls into one of FOIA's exceptions. One exception covers information that, under executive order, must be kept secret for national security or foreign policy reasons.[1545] In 2000, Congress enacted the Public Interest Declassification Act of 2000,[1546] which established the Public Interest Declassification Board to advise the President on matters regarding the declassification of certain information, but the Act expressly disclaims any intent to restrict agency heads from classifying or continuing the classification of information under their purview, nor does it create any rights or remedies that may be enforced in court.[1547]

Executive Order 12,958 (as amended)

The present standards for classifying and declassifying information were last amended in March, 2003.[1548] Under these current standards, the President, Vice President, agency heads, and any other officials designated by the President may classify information upon a determination that the unauthorized disclosure of such information could reasonably be expected to damage national security.[1549] Such information must be owned by, produced by, or under the control of the federal government, and must concern one of the following:

[1543] Id.

[1544] See, e.g., Availability of Information from Federal Departments and Agencies: Hearings Before the House Committee on Government Operations, 85th Cong. (1955).

[1545] 5 U.S.C. § 552(b)(1). The Supreme Court has honored Congress's deference to executive branch determinations in this area. EPA v. Mink, 410 U.S. 73 (1973). Congress, concerned that the executive branch may have declared some documents to be "national security information" that were not vital to national security, added a requirement that such information be "properly classified pursuant to an executive order." 5 U.S.C. § 552(b)(1)(B).

[1546] P.L. 106 — 567, title VII, Dec. 27, 2000, 114 Stat. 2856, 50 U.S.C. § 435 note.

[1547] Id. §§ 705 and 707.

[1548] Exec. Order No. 12,958, as amended by Exec. Order No. 13,292 (2003), 68 F.R. 15,315 (March 28, 2003).

[1549] Exec. Order No. 12,958 (as amended by Exec. Order No. 13,292 (2003)), § 1.1. The unauthorized disclosure of foreign government information is presumed to damage national security. Id. at § 1.1(b).

- military plans, weapons systems, or operations;
- foreign government information;
- intelligence activities, intelligence sources/methods, cryptology;
- scientific, technological, or economic matters relating to national security;
- federal programs for safeguarding nuclear materials or facilities;
- vulnerabilities or capabilities of national security systems; or
- weapons of mass destruction.[1550]

Information is classified at one of three levels based on the amount of danger that its unauthorized disclosure could reasonably be expected to cause to national security.[1551] Information is classified as "Top Secret" if its unauthorized disclosure could reasonably be expected to cause "exceptionally grave damage" to national security. The standard for "Secret" information is "serious damage" to national security, while for "confidential" information the standard is "damage" to national security. Significantly, for each level, the original classifying officer must identify or describe the specific danger potentially presented by the information's disclosure.[1552] The officer who originally classifies the information establishes a date for declassification based upon the expected duration of the information's sensitivity. If the office cannot set an earlier declassification date, then the information must be marked for declassification in 10 years' time or 25 years, depending on the sensitivity of the information.[1553] The deadline for declassification can be extended if the threat to national security still exists.[1554]

Classified information is required to be declassified "as soon as it no longer meets the standards for classification,"[1555] although there is a presumption that classified information continues to meet these standards. The original classifying agency has the authority to declassify information when the public interest in disclosure outweighs the need to protect that information.[1556] On December 31, 2006, and every year thereafter, all information that has been classified for 25

[1550] Id. at § 1.4. In addition, when classified information which is incorporated, paraphrased, restated, or generated in a new form, that new form must be classified at the same level as the original. Id. at §§ 2.1 - 2.2.

[1551] Id. at § 1.2.

[1552] Id. Classifying authorities are specifically prohibited from classifying information for reasons other than protecting national security, such as to conceal violations of law or avoid embarrassment. Id. at § 1.7(a).

[1553] Id. at § 1.5.

[1554] Id. at § 1.5(c).

[1555] Id. at § 3.1(a).

[1556] Id. at § 3.1(b).

years or longer and has been determined to have "permanent historical value" under Title 44 of the U.S. Code will be automatically declassified, although agency heads can exempt from this requirement classified information that continues to be sensitive in a variety of specific areas.[1557]

Agencies are required to review classification determinations upon a request for such a review that specifically identifies the materials so that the agency can locate them.[1558] This requirement does not apply to information that has undergone declassification review in the previous two years; information that is exempted from review under the National Security Act;[1559] or information classified by the incumbent President and staff, the Vice President and staff (in the performance of executive duties), commissions appointed by the President, or other entities within the executive office of the President that advise the President.[1560] Each agency that has classified information is required to establish a system for periodic declassification reviews.[1561] The National Archivist is required to establish a similar systemic review of classified information that has been transferred to the National Archives.[1562]

Access to classified information is generally limited to those who demonstrate their eligibility to the relevant agency head, sign a nondisclosure agreement, and have a need to know the information.[1563] The need-to-know requirement can be waived, however, for former Presidents and Vice Presidents, historical researchers, and former policy-making officials who were appointed by the President or Vice President.[1564] The information being accessed may not be removed from the controlling agency's premises without permission. Each agency is required to establish systems for controlling the distribution of classified information.[1565]

[1557] Id. at § 3.3.

[1558] Id. at § 3.5.

[1559] 50 U.S.C. §§ 403-5c, 403-5e, 431.

[1560] Exec. Order No. 12,958 (as amended by Exec. Order No. 13,292 (2003)), § 3.5.

[1561] Id. at § 3.4.

[1562] Id.

[1563] Id. at § 4.1.

[1564] Id. at § 4.4.

[1565] Id. at § 4.2.

The Information Security Oversight Office (ISOO) — an office within the National Archives — is charged with overseeing compliance with the classification standards and promulgating directives to that end.[1566] ISOO is headed by a Director, who is appointed by the Archivist of the United States, and who has the authority to order declassification of information that, in the Director's view, is classified in violation of the aforementioned classification standards.[1567] In addition, there is an Interagency Security Classifications Appeals Panel ("the Panel"), headed by the ISOO Director and made up of representatives of the heads of various agencies, including the Departments of Defense, Justice, and State, as well as the Central Intelligence Agency, and the National Archives.[1568] The Panel is empowered to decide appeals of classifications challenges[1569] and to review automatic and mandatory declassifications. If the ISOO Director finds a violation of Executive Order 12,958 (as amended) or its implementing directives, then the Director must notify the appropriate classifying agency so that corrective steps can be taken. Officers and employees of the United States (including contractors, licensees, etc.) who commit a violation are subject to sanctions that can range from reprimand to termination.[1570]

Criminal Penalties

Generally, federal law prescribes a prison sentence of no more than a year and/or a $1,000 fine for officers and employees of the federal government who knowingly remove classified material without the authority to do so and with the intention of keeping that material at an unauthorized location.[1571] Stiffer penalties — fines of up to $10,000 and imprisonment for up to 10 years — attach when a federal employee transmits classified information to anyone that the employee has reason to believe is an agent of a foreign government.[1572] A fine and a 10-year prison term also await anyone, government employee or not, who publishes, makes available to an unauthorized person, or otherwise uses to the United States' detriment classified information regarding the codes, cryptography, and

---

[1566] Id. at § 5.2.

[1567] Id. at § 3.1(c).

[1568] Id. at § 5.3.

[1569] Id. at § 5.3(b)(1) - (3) For example, an authorized holder of classified information is allowed to challenge the classified status of such information if the holder believes that status is improper. Id. at § 1.8.

[1570] Id. at § 5.5.

[1571] 18 U.S.C. § 1924. Agencies often require employees to sign non-disclosure agreements prior to obtaining access to classified information, the validity of which was upheld by the Supreme Court in Snepp v. United States, 444 U.S. 507 (1980).

[1572] 50 U.S.C. § 783.

communications intelligence utilized by the United States or a foreign government.[1573]

[1573] 18 U.S.C. § 798. This provision is part of the Espionage Act (codified at 18 U.S.C. §§ 792 799), which generally protects against the unauthorized transmission of a much broader category of "national defense" information, prescribing fines and a prison term of up to 10 years.

Protection of National Security Information, RL33502 (December 26, 2006).

JENNIFER K. ELSEA, CONGRESSIONAL RESEARCH SERV., PROTECTION OF NATIONAL SECURITY INFORMATION (2006), *available at* http://www.intelligencelaw.com/library/secondary/crs/pdf/RL33502_12-26-2006.pdf.

Order Code RL33502

Updated December 26, 2006

Jennifer K. Elsea
Legislative Attorney
American Law Division

Summary

Recent cases involving alleged disclosures of classified information to the news media or others who are not entitled to receive it have renewed Congress's interest with regard to the possible need for legislation to provide for criminal punishment for the "leaks" of classified information. The Espionage Act of 1917 and other statutes and regulations provide a web of authorities for the protection of various types of sensitive information, but some have expressed concern that gaps in these laws may make prosecution of some disclosures impossible. The 106th Congress passed a measure to criminalize leaks, but President Clinton vetoed it. The 108th Congress reconsidered the same provision, but instead passed a requirement for the relevant agencies to review the need for such a proscription. The Department of Justice in turn reported that existing statutes and regulations are sufficient to prosecute disclosures of information that might harm the national security.

This report provides background with respect to previous legislative efforts to criminalize the unauthorized disclosure of classified information; describes the current state of the laws that potentially apply, including criminal and civil penalties that can be imposed on violators; and some of the disciplinary actions and administrative procedures available to the agencies of federal government that have been addressed by federal courts. Finally, the report considers the possible First Amendment implications of applying the Espionage Act to prosecute newspapers for publishing classified national defense information.

Introduction

Continued revelations involving alleged disclosures of classified information to the news media or to others who are not entitled to receive it have renewed

Congress's interest with regard to the possible need for legislation to provide for criminal punishment for the "leaks" of classified information. Opponents of any such legislation express concern regarding the possible consequences to freedom of the press and other First Amendment values. The current laws for protecting classified information have been criticized as a patchwork of sometimes abstruse and antiquated provisions that are not consistent and do not cover all the information the government legitimately needs to protect.[1574] Certain information is protected regardless of whether it belongs to the government or is subject to normal classification. Information related to "the national defense" is protected even though no harm to the national security is intended or is likely to be caused through its disclosure. However, nonmilitary information with the potential to cause serious damage to the national security is only protected from willful disclosure with the requisite intent or knowledge regarding the potential harm. For example, under 50 U.S.C. § 783, the communication of classified information by a government employee is expressly punishable only if the discloser knows or has reason to believe the recipient is an agent or representative of a foreign government, but not, for example, if the recipient is an agent of an international terrorist organization.

To close some perceived gaps, the 106th Congress passed a measure to criminalize all leaks of classified information; however, President Clinton vetoed the measure.[1575] The 108th Congress considered passing an identical provision as

---

[1574] See E.E.B. and K.E.M., Note, *Plugging the Leak: The Case for a Legislative Resolution of the Conflict between the Demands of Secrecy and the Need for Open Government*, 71 VA. L. REV. 801, 811 (1985). With respect to a major component of the legal framework, one district court judge had the following to say:

The conclusion that the statute is constitutionally permissible does not reflect a judgment about whether Congress could strike a more appropriate balance between these competing interests, or whether a more carefully drawn statute could better serve both the national security and the value of public debate. Indeed, the basic terms and structure of this statute have remained largely unchanged since the administration of William Howard Taft. The intervening years have witnessed dramatic changes in the position of the United States in world affairs and the nature of threats to our national security. The increasing importance of the United States in world affairs has caused a significant increase in the size and complexity of the United States' military and foreign policy establishments, and in the importance of our nation's foreign policy decision making. Finally, in the nearly one hundred years since the passage of the Defense Secrets Act mankind has made great technological advances affecting not only the nature and potential devastation of modern warfare, but also the very nature of information and communication. These changes should suggest to even the most casual observer that the time is ripe for Congress to engage in a thorough review and revision of these provisions to ensure that they reflect both these changes, and contemporary views about the appropriate balance between our nation's security and our citizens' ability to engage in public debate about the United States' conduct in the society of nations.

United States v. Rosen, 445 F.Supp.2d 602, 646 (E.D. Va. 2006)(Ellis, J.).

[1575] H.R. 4392 § 304, 106th Congress; See Statement by the President to the House of Representatives, 36 WEEKLY COMP. PRES. DOC. 278 (Nov. 4, 2000).

part of the Intelligence Authorization Act for Fiscal Year 2001,[1576] but instead directed the Attorney General and heads of other departments to undertake a review of the current protections against the unauthorized disclosure of classified information, and to issue a report recommending legislative or administrative actions by May 1, 2002.[1577] In its response to Congress, the Department of Justice concluded that existing statutes and regulations are sufficient to prosecute disclosures of information that might harm the national security.[1578]

This report describes the current state of the law with regard to the unauthorized disclosure of classified information, including criminal and civil penalties that can be imposed on violators, as well as some of the disciplinary actions and administrative procedures available to federal agencies with respect to their employees, as such measures have been addressed by federal courts. The report also describes the background of legislative efforts to amend the laws, including the measure passed in 2000 and President Clinton's stated reasons for vetoing it. Finally, the report considers possible constitutional issues — in particular, issues related to the First Amendment — that may arise if Congress considers new legislation to punish leaks or if the Attorney General seeks to apply current law to punish newspapers that publish leaked classified information.

Background

The classification by government agencies of documents deemed sensitive has evolved from a series of executive orders.[1579] Congress has, for the most part, let the executive branch make decisions regarding the type of information to be subject to protective measures. The current criminal statutory framework providing penalties for the unauthorized disclosure of classified government materials traces its roots to the Espionage Act of 1917,[1580] which made it a crime

---

[1576] The Classified Information Protection Act of 2001, H.R. 2943, 107th Cong.

[1577] See Intelligence Authorization Act for Fiscal Year 2002, P.L. 107-108, § 310 (2001). An identical measure was introduced in the 109th Congress, S. 3774, but was not reported out of committee.

[1578] Letter from John Ashcroft, Attorney General of the United States, to Congress, October 15, 2002, reported 148 CONG. REC. S11,732 (daily ed. Nov. 20, 2002), available online at [http://www.fas.org/sgp/othergov/dojleaks.html](Last visited June 29, 2006).

[1579] See SENATE COMM'N ON PROTECTING AND REDUCING GOVERNMENT SECRECY, 103d CONG.,REPORT PURSUANT TO PUBLIC LAW 236 (Comm. Print 1997); CRS Report RS21900, The Protection of Classified Information: The Legal Framework, by Jennifer K. Elsea.

[1580] Act of June 15, 1917, ch. 30, title I, §§ 1, 6, 40 Stat. 217, 219, codified as amended at 18 U.S.C. §§ 793 et seq.

to disclose defense information during wartime.[1581] The National Security Act of 1947[1582] directed the Director of the CIA to protect "intelligence sources and methods."[1583] The Atomic Energy Act of 1954[1584] provided for secrecy of information related to nuclear energy and weapons.[1585] The Invention Secrecy Act of 1951[1586] gave the government the authority to declare a patent application secret if disclosure of an invention might expose the country to harm.

Criminal Statutes for the Protection of Classified Information

National defense information is protected by the Espionage Act, 18 U.S.C. § 793 et seq. The penalty for violation of 18 U.S.C. § 793 (gathering, transmitting, or losing defense information) is a fine or imprisonment for not more than 10 years, or both. Thus, under § 793, persons convicted of gathering defense information with the intent or reason to believe the information will be used against the United States or to the benefit of a foreign nation may be fined or sentenced to no more than 10 years imprisonment.[1587] Persons who have access to defense

---

[1581] See Anthony R. Klein, Comment, National Security Information: Its Proper Role and Scope in a Representative Democracy, 42 FED. COMM. L.J. 433, 437(1990) (describing evolution of anti-espionage laws).

[1582] Codified at 50 U.S.C. § 401 et seq.

[1583] 50 U.S.C. § 403(g).

[1584] Codified at 42 U.S.C. § 2271 et seq. The dissemination of certain unclassified information related to nuclear facilities may be restricted by the Secretary of Energy pursuant to 42 U.S.C. § 2168 upon a finding that dissemination "could reasonably be expected to result in a significant adverse effect on the health and safety of the public or the common defense and security...." 42 U.S.C. § 2168(a)(4)(B).

[1585] See Benjamin S. DuVal, Jr., The Occasions of Secrecy, 47 U. PITT. L. REV. 579, 596 (1986) (detailing restrictions directed at protecting nuclear secrets, or "Restricted Data").

[1586] Codified at 35 U.S.C. § 181 et seq.

[1587] 18 U.S.C. § 793(a)-(c) provides:
(a) Whoever, for the purpose of obtaining information respecting the national defense with intent or reason to believe that the information is to be used to the injury of the United States, or to the advantage of any foreign nation, goes upon, enters, flies over, or otherwise obtains information concerning any vessel, aircraft, work of defense, [etc.], or any prohibited place so designated by the President by proclamation in time of war or in case of national emergency in which anything for the use of the Army, Navy, or Air Force is being prepared or constructed or stored, information as to which prohibited place the President has determined would be prejudicial to the national defense; or
(b) Whoever, for the purpose aforesaid, and with like intent or reason to believe, copies, takes, makes, or obtains, or attempts to copy, take, make, or obtain any sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, document, writing, or note of anything connected with the national defense; or

information that they have reason to know could be used to harm the national security, whether the access is authorized or unauthorized, and who disclose that information to any person not entitled to receive it, or willfully retain the information despite an order to surrender it to an officer of the United States, are subject to the same penalty.[1588] Although it is not necessary that the information be classified by a government agency, the courts give deference to the executive determination of what constitutes "defense information."[1589] Information that is made available by the government to the public is not covered under the prohibition, however, because public availability of such information negates the bad-faith intent requirement.[1590] On the other hand, classified documents may remain within the ambit of the statute even if information contained therein is

---

(c) Whoever, for the purpose aforesaid, receives or obtains or agrees or attempts to receive or obtain from any person, or from any source whatever, any [protected thing] connected with the national defense, knowing or having reason to believe. . . that it has been or will be obtained, taken, made, or disposed of by any person contrary to the provisions of this chapter [18 U.S.C. §§ 792 et seq.];....

[1588] 18 U.S.C. § 793(d)-(f) provides:

(d) Whoever, lawfully having possession of, access to, control over, or being entrusted with any document [or other protected thing] relating to the national defense, or information relating to the national defense . . . the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits . . . to any person not entitled to receive it, or willfully retains the same and fails to deliver it on demand to the officer or employee of the United States entitled to receive it; or

(e) Whoever having unauthorized possession of, access to, or control over any document [or other protected thing], or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits . . . to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it; or

(f) Whoever, being entrusted with or having lawful possession or control of any document [or other protected thing], or information, relating to the national defense,

(1) through gross negligence permits the same to be removed from its proper place of custody or delivered to anyone in violation of his trust, or to be lost, stolen, abstracted, or destroyed, or

(2) having knowledge that the same has been illegally removed from its proper place of custody or delivered to anyone in violation of his trust, or lost, or stolen, abstracted, or destroyed, and fails to make prompt report of such loss, theft, abstraction, or destruction to his superior officer — Shall be fined under this title or imprisoned not more than ten years, or both.

[1589] See United States v. Morison, 844 F.2d 1057 (4th Cir.), cert. denied, 488 U.S. 908 (1988)(upholding conviction under 18 U.S.C. § 793 for delivery of classified photographs to publisher).

[1590] Gorin v. United States, 312, U.S. 9, 27-28 (1941) ("Where there is no occasion for secrecy, as with reports relating to national defense, published by authority of Congress or the military departments, there can, of course, in all likelihood be no reasonable intent to give an advantage to a foreign government.").

made public by an unauthorized leak.[1591] Any person who is lawfully entrusted with defense information and who permits it to be disclosed or lost, or who does not report such a loss or disclosure, is also subject to a penalty of up to 10 years in prison. The act covers information transmitted orally as well as information in tangible form.[1592]

18 U.S.C. § 794 (aiding foreign governments) provides for imprisonment for any term of years or life, or under certain circumstances, the death penalty.[1593] The provision penalizes anyone who transmits defense information to a foreign government (or certain other foreign entities) with the intent or reason to believe it will be used against the United States. The death penalty is available only upon a finding that the offense resulted in the death of a covert agent or directly concerns nuclear weapons or other particularly sensitive types of information. The death penalty is also available under §794 for violators who gather or transmit information related to military plans and the like during time of war, with the intent that the information reach the enemy.[1594] Offenders are also

---

[1591] United States v. Squillacote, 221 F.3d 542, 578 (4th Cir. 2000). But see United States v. Rosen, 445 F.Supp.2d 602, 620 (E.D. Va. 2006) (interpreting the reference in Squillacote to apply not to the document at issue, but rather, to information pertaining to the government's assessment of the validity of the information contained in it).

[1592] United States v. Rosen, 445 F.Supp.2d 602, 616 (E.D. Va. 2006).

[1593] § 794. Gathering or delivering defense information to aid foreign government
(a) Whoever, with intent or reason to believe that it is to be used to the injury of the United States or to the advantage of a foreign nation, communicates, delivers, or transmits. . . to any foreign government, or to any faction or party or military or naval force within a foreign country, whether recognized or unrecognized by the United States, or to any representative, officer, agent, employee, subject, or citizen thereof, either directly or indirectly, any document [or other protected thing], or information relating to the national defense, shall be punished by death or by imprisonment for any term of years or for life, except that the sentence of death shall not be imposed unless the jury or . . . the court, further finds that the offense resulted in the identification by a foreign power (as defined in section 101(a) of the Foreign Intelligence Surveillance Act of 1978 [50 U.C.S. § 1801(a)]) of an individual acting as an agent of the United States and consequently in the death of that individual, or directly concerned nuclear weaponry, military spacecraft or satellites, earlywarning systems, or other means of defense or retaliation against large-scale attack; war plans; communications intelligence or cryptographic information; or any other major weapons system or major element of defense strategy.

(b) Whoever, in time of war, with intent that the same shall be communicated to the enemy, collects, records, publishes, or communicates, or attempts to elicit any information with respect to the movement, numbers, description, condition, or disposition of any of the Armed Forces, ships, aircraft, or war materials of the United States, or with respect to the plans or conduct, or supposed plans or conduct of any naval or military operations, or with respect to any works or measures undertaken for or connected with, or intended for the fortification or defense of any place, or any other information relating to the public defense, which might be useful to the enemy, shall be punished by death or by imprisonment for any term of years or for life....

[1594] During time of war, any individual who communicates intelligence or any other information to the enemy may be prosecuted by the military for aiding the enemy under Article 104 of the

subject to forfeiture of any ill-gotten gains and property used to facilitate the offense.[1595]

Members of the military[1596] who commit espionage, defined similarly to the conduct prohibited in 18 U.S.C. § 794, may be tried by court-martial for violating Article 106a of the Uniform Code of Military Justice (UCMJ),[1597] and sentenced to death if certain aggravating factors are found by unanimous determination of the panel.[1598] Unlike offenses under § 794, Article 106a offenses need not have resulted in the death of a covert agent or involve military operations during war

---

Uniform Code of Military Justice (UCMJ), and if convicted, punished by "death or such other punishment as a court-martial or military commission may direct." 10 U.S.C. § 904. Persons convicted by a general court-martial or by a military commission for "lurking as a spy or acting as a spy in or about any place, vessel, or aircraft, [etc.]" during time of war are to be punished by death. 10 U.S.C. § 906. Alien unlawful combatants within the meaning of chapter 47A of title 10, who, "with intent or reason to believe that it is to be used to the injury of the United States or to the advantage of a foreign power, collects or attempts to collect information by clandestine means or while acting under false pretenses, for the purpose of conveying such information to an enemy of the United States, or one of the co-belligerents of the enemy, shall be punished by death or such other punishment as a military commission ... may direct." 10 U.S.C.A. § 950v(27).

[1595] 18 U.S.C. § 794(d). Proceeds go to the Crime Victims Fund.

[1596] Persons subject to the UCMJ include members of regular components of the armed forces, cadets and midshipmen, members of reserve components while on training, members of the national guard when in Federal service, members of certain organizations when assigned to and serving the armed forces, prisoners of war, persons accompanying the armed forces in the field in time of war or a "contingency operation," and certain others with military status. 10 U.S.C. § 802.

[1597] 10 U.S.C. § 906a(a) provides:

Art. 106a. Espionage

(a)(1) Any person subject to [the UCMJ, chapter 47 of title 10, U.S.C.] who, with intent or reason to believe that it is to be used to the injury of the United States or to the advantage of a foreign nation, communicates, delivers, or transmits, or attempts to communicate, deliver, or transmit, to any entity described in paragraph (2), either directly or indirectly, anything described in paragraph (3) shall be punished as a court-martial may direct, except that if the accused is found guilty of an offense that directly concerns (A) nuclear weaponry, military spacecraft or satellites, early warning systems, or other means of defense or retaliation against large scale attack, (B) war plans, (C) communications intelligence or cryptographic information, or (D) any other major weapons system or major element of defense strategy, the accused shall be punished by death or such other punishment as a court- martial may direct.

(2) An entity referred to in paragraph (1) is —

(A) a foreign government;

(B) a faction or party or military or naval force within a foreign country, whether recognized or unrecognized by the United States; or

(C) a representative, officer, agent, employee, subject, or citizen of such a government, faction, party, or force.

(3) A thing referred to in paragraph (1) is a document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, note, instrument, appliance, or information relating to the national defense.

[1598] 10 U.S.C. § 906a(b)-(c).

to incur the death penalty. One of the aggravating factors enabling the imposition of the death penalty under Article 106a is that "[t]he accused has been convicted of another offense involving espionage or treason for which either a sentence of death or imprisonment for life was authorized by statute."

The unauthorized creation, publication, sale or transfer of photographs or sketches of vital defense installations or equipment as designated by the President is prohibited by 18 U.S.C. §§ 795 and 797.[1599] Violators are subject to fine or imprisonment for not more than one year, or both.

The knowing and willful disclosure of certain classified information is punishable under 18 U.S.C. § 798 by fine and/or imprisonment for not more than 10 years.[1600] To incur a penalty, the disclosure must be prejudicial to the safety or interests of the United States or work to the benefit of any foreign government and to the detriment of the United States. The provision applies only to

---

[1599] § 795. Photographing and sketching defense installations
(a) Whenever, in the interests of national defense, the President defines certain vital military and naval installations or equipment as requiring protection against the general dissemination of information relative thereto, it shall be unlawful to make any photograph, sketch, picture, drawing, map, or graphical representation of such vital military and naval installations or equipment without first obtaining permission of the commanding officer of the military or naval post, camp, or station, or naval vessels, military and naval aircraft, and any separate military or naval command concerned, or higher authority, and promptly submitting the product obtained to such commanding officer or higher authority for censorship or such other action as he may deem necessary....

§ 797. Publication and sale of photographs of defense installations
On and after thirty days from the date upon which the President defines any vital military or naval installation or equipment as being within the category contemplated under section 795 of this title [18], whoever reproduces, publishes, sells, or gives away any photograph, sketch, picture, drawing, map, or graphical representation of the vital military or naval installations or equipment so defined, without first obtaining permission of the commanding officer ... or higher authority, unless such photograph, sketch, picture, drawing, map, or graphical representation has clearly indicated thereon that it has been censored by the proper military or naval authority, shall be fined under this title or imprisoned not more than one year, or both.

[1600] § 798. Disclosure of classified information
(a) Whoever knowingly and willfully communicates, furnishes, transmits, or otherwise makes available to an unauthorized person, or publishes, or uses in any manner prejudicial to the safety or interest of the United States or for the benefit of any foreign government to the detriment of the United States any classified information —
(1) concerning the nature, preparation, or use of any code, cipher, or cryptographic system of the United States or any foreign government; or
(2) concerning the design, construction, use, maintenance, or repair of any device, apparatus, or appliance used or prepared or planned for use by the United States or any foreign government for cryptographic or communication intelligence purposes; or
(3) concerning the communication intelligence activities of the United States or any foreign government; or
(4) obtained by the processes of communication intelligence from the communications of any foreign government, knowing the same to have been obtained by such processes —

Shall be fined under this title or imprisoned not more than ten years, or both.

information related to cryptographic systems and information related to communications intelligence specially designated by a U.S. government agency for "limited or restricted dissemination or distribution."[1601] The provision protects information obtained by method of communications intelligence only if the communications were intercepted from a "foreign government," which, while broadly defined, may not include a transnational terrorist organization.[1602]

18 U.S.C. § 641 punishes the theft or conversion of government property or records for one's own use or the use of another. While this section does not explicitly prohibit disclosure of classified information, it has been used for that purpose.[1603] Violators may be fined, imprisoned for not more than 10 years, or both, unless the value of the property does not exceed the sum of $100, in which case the maximum prison term is one year.

18 U.S.C. § 952 punishes employees of the United States who, without authorization, willfully publish or furnish to another any official diplomatic code or material prepared in such a code, by imposing a fine, a prison sentence (up to 10 years), or both. The same punishment applies for materials "obtained while in the process of transmission between any foreign government and its diplomatic mission in the United States."[1604]

18 U.S.C. § 1030(a)(1) punishes the willful retention, communication, or transmission, etc., of classified information retrieved by means of knowingly accessing a computer without (or in excess of) authorization, with reason to believe that such information "could be used to the injury of the United States, or to the advantage of any foreign nation." The provision imposes a fine or imprisonment for not more than ten years, or both, in the case of a first offense or attempted violation. Repeat offenses or attempts can incur a prison sentence of up to twenty years.

[1601] 18 U.S.C. § 798(b).

[1602] Id. ("The term 'foreign government' includes in its meaning any person or persons acting or purporting to act for or on behalf of any faction, party, department, agency, bureau, or military force of or within a foreign country, or for or on behalf of any government or any person or persons purporting to act as a government within a foreign country, whether or not such government is recognized by the United States.").

[1603] See United States v. Morison, 844 F.2d 1057 (4th Cir. 1988)(photographs and reports were tangible property of the government); United States v. Fowler, 932 F.2d 306 (4th Cir. 1991)("information is a species of property and a thing of value" such that "conversion and conveyance of governmental information can violate § 641,"citing United States v. Jeter, 775 F.2d 670, 680-82 (6th Cir. 1985)); United States v. Girard, 601 F.2d 69, 70-71 (2d Cir. 1979).

[1604] 18 U.S.C. § 952.

18 U.S.C. § 1924 prohibits the unauthorized removal of classified material.[1605] The provision imposes a fine of up to $1,000 and a prison term up to one year for government officers or employees who knowingly take material classified pursuant to government regulations with the intent of retaining the materials at an unauthorized location.[1606]

42 U.S.C. § 2274 punishes the unauthorized communication by anyone of "Restricted Data,"[1607] or an attempt or conspiracy to communicate such data, by imposing a fine of not more than $500,000, a maximum life sentence in prison, or both, if done with the intent of injuring the United States or to secure an advantage to any foreign nation.[1608] An attempt to disclose or participate in a conspiracy to disclose restricted data with the belief that such data will be used to injure the United States or to secure an advantage to a foreign nation, is punishable by imprisonment for no more than 10 years, a fine of no more than $100,000, or both.[1609] The disclosure of "Restricted Data" by an employee or contractor, past or present, of the federal government to someone not authorized to receive it is punishable by a fine of not more than $12,500.[1610]

[1605] 18 U.C.S. § 1924 provides:
(a) Whoever, being an officer, employee, contractor, or consultant of the United States, and, by virtue of his office, employment, position, or contract, becomes possessed of documents or materials containing classified information of the United States, knowingly removes such documents or materials without authority and with the intent to retain such documents or materials at an unauthorized location shall be fined not more than $ 1,000, or imprisoned for not more than one year, or both.
(b) For purposes of this section, the provision of documents and materials to the Congress shall not constitute an offense under subsection (a).

(c) In this section, the term "classified information of the United States" means information originated, owned, or possessed by the United States Government concerning the national defense or foreign relations of the United States that has been determined pursuant to law or Executive order to require protection against unauthorized disclosure in the interests of national security.

[1606] Id.

[1607] The term "Restricted Data" is defined by the Atomic Energy Act of 1954 to include "all data concerning (1) design, manufacture, or utilization of atomic weapons; (2) the production of special nuclear material; or (3) the use of special nuclear material in the production of energy, but shall not include data declassified or removed from the Restricted Data category pursuant to [42 U.C.S. § 2162]." 42 U.C.S. § 2014(y).

[1608] 42 U.S.C. § 2274(a). Receipt or tampering with Restricted Data with like intent is punishable in the same way under 42 U.S.C. §§ 2275 and 2276.

[1609] 42 U.S.C. § 2274(b).

[1610] 42 U.S.C. § 2277.

50 U.S.C. § 421 provides for the protection of information concerning the identity of covert intelligence agents.[1611] Any person authorized to know the identity of such agents who intentionally discloses the identity of a covert agent is subject to imprisonment for not more than 10 years or a fine or both.[1612] A person who learns the identity of an agent through authorized access to classified information[1613] and discloses the agent's identity to someone not authorized to receive classified information is subject to a fine, a term of imprisonment not more than five years, or both. A person who learns of the identity of a covert agent through a "pattern of activities intended to identify and expose covert agents" and discloses the identity to any individual not authorized access to classified information, with reason to believe that such activities would impair U.S. foreign intelligence efforts, is subject to a fine or imprisonment for a term of not more than three years. To be convicted, a violator must have knowledge that the information identifies a covert agent whose identity the United States is taking affirmative measures to conceal. An agent is not punishable under this provision for revealing his or her own identity, and it is a defense to prosecution if the United States has already publicly disclosed the identity of the agent.[1614]

50 U.S.C. § 783 penalizes government officers or employees who, without proper authority, communicate classified information to a person whom the employee has reason to suspect is an agent or representative of a foreign government.[1615] It

---

[1611] The Intelligence Identities and Protection Act of 1982, codified at 50 U.S.C. §§ 421-26. For more information, see CRS Report RS21636, Intelligence Identities Protection Act, by Elizabeth B. Bazan.

[1612] 50 U.S.C. § 421(a) provides:

(a) Whoever, having or having had authorized access to classified information that identifies a covert agent, intentionally discloses any information identifying such covert agent to any individual not authorized to receive classified information, knowing that the information disclosed so identifies such covert agent and that the United States is taking affirmative measures to conceal such covert agent's intelligence relationship to the United States, shall be fined under title 18, United States Code, or imprisoned not more than ten years, or both.

[1613] "Classified Information" is defined in 50 U.S.C. § 426(1) as "information or material designated and clearly marked or clearly represented, pursuant to the provisions of a statute or Executive order (or a regulation or order issued pursuant to a statute or Executive order), as requiring a specific degree of protection against unauthorized disclosure for reasons of national security."

[1614] See Lawrence P. Gottesman, Note, The Intelligence Identities Protection Act of 1982: An Assessment of the Constitutionality of Section 601(c), 49 BROOKLYN L. REV. 479, 483 - 485 (1983)(outlining the elements of an offense under 50 U.S.C. § 421).

[1615] 50 U.S.C. § 783(a) provides:

Communication of classified information by Government officer or employee. It shall be unlawful for any officer or employee of the United States or of any department or agency thereof, or of any corporation the stock of which is owned in whole or in major part by the United States or any department or agency thereof, to communicate in any manner or by any means, to any other

is also unlawful for the representative or agent of the foreign government to receive classified information.[1616] Violation of either of these provisions is punishable by a fine of up to $10,000 or imprisonment for not more than 10 years.[1617] Violators are thereafter prohibited from holding public office.[1618] Violators must forfeit all property derived directly or indirectly from the offense and any property that was used or intended to be used to facilitate the violation.[1619]

Disclosure of a patent that has been placed under a secrecy order pursuant to the Invention Secrecy Act of 1951[1620] can result in a fine of $10,000, imprisonment for up to two years, or both. Publication or disclosure of the invention must be willful and with knowledge of the secrecy order to be punishable.[1621]

Civil Penalties and Other Measures

In addition to the criminal penalties outlined above, the executive branch employs numerous means of deterring unauthorized disclosures by government personnel using administrative measures based on terms of employment

---

person whom such officer or employee knows or has reason to believe to be an agent or representative of any foreign government , any information of a kind which shall have been classified by the President (or by the head of any such department, agency, or corporation with the approval of the President) as affecting the security of the United States, knowing or having reason to know that such information has been so classified, unless such officer or employee shall have been specifically authorized by the President, or by the head of the department, agency, or corporation by which this officer or employee is employed, to make such disclosure of such information.

[1616] 50 U.S.C. 783(b) provides:

Receipt of, or attempt to receive, by foreign agent or member of Communist organization, classified information. It shall be unlawful for any agent or representative of any foreign government knowingly to obtain or receive, or attempt to obtain or receive, directly or indirectly, from any officer or employee of the United States or of any department or agency thereof or of any corporation the stock of which is owned in whole or in major part by the United States or any department or agency thereof, any information of a kind which shall have been classified by the President (or by the head of any such department, agency, or corporation with the approval of the President) as affecting the security of the United States, unless special authorization for such communication shall first have been obtained from the head of the department, agency, or corporation having custody of or control over such information.

[1617] 50 U.S.C. § 783(c).

[1618] Id.

[1619] 50 U.S.C. § 783(e).

[1620] Codified at 35 U.S.C. § 181 et seq.

[1621] 35 U.S.C. § 186.

contracts.[1622] The agency may impose disciplinary action or revoke a person's security clearance.[1623] The revocation of a security clearance is usually not reviewable by the Merit System Protection Board[1624] and may mean the loss of government employment. Government employees may be subject to monetary penalties for disclosing classified information.[1625] Violators of the Espionage Act and the Atomic Energy Act provisions may be subject to loss of their retirement pay. [1626]

Agencies also rely on contractual agreements with employees, who typically must sign non-disclosure agreements prior to obtaining access to classified information,[1627] sometimes agreeing to submit all materials that the employee desires to publish to a review by the agency. The Supreme Court enforced such a contract against a former employee of the Central Intelligence Agency (CIA), upholding the government's imposition of a constructive trust on the profits of a book the employee sought to publish without first submitting it to CIA for review.[1628]

In 1986, the Espionage Act was amended to provide for the forfeiture of any property derived from or used in the commission of an offense.[1629] Violators of the Atomic Energy Act may be subjected to a civil penalty of up to $100,000 for

---

[1622] See DuVal, supra note 12, at 597 (identifying administrative regulations as principal means of enforcing secrecy procedures).

[1623] See, e.g., Exec. Order 12,958. Sanctions may include "reprimand, suspension without pay, removal, ... loss or denial of access to classified information, or other sanctions in accordance with applicable law and agency regulation." Id. at §5.7(c).

[1624] See Department of Navy v. Egan, 484 U.S. 518, 526-29 (1988). Federal courts may review constitutional challenges based on the revocation of security clearance. Webster v. Doe, 486 U.S. 592 (1988).

[1625] See 42 U.S.C. § 2282(b) (providing for fine of up to $100,000 for violation of Department of Energy security regulations).

[1626] 5 U.C.S. § 8312 (2001)(listing violations of 18 U.S.C. §§ 793 & 798, 42 U.S.C. § 227276, and 50 U.S.C. § 421, among those for which forfeiture of retirement pay or annuities may be imposed).

[1627] See United States v. Marchetti, 466 F.2d 1309 (4th Cir.), cert. denied, 409 U.S. 1063 (1972) (enforcing contractual non-disclosure agreement by former employee regarding "secret information touching upon the national defense and the conduct of foreign affairs" obtained through employment with CIA).

[1628] See Snepp v. United States, 444 U.S. 507 (1980); see also Alan E. Garfield, Promises of Silence: Contract Law and Freedom of Speech, 83 CORNELL L.REV. 261, 274 (1998)(noting the remedy in Snepp was enforced despite the agency's stipulation that the book did not contain any classified information).

[1629] See 18 U.S.C. §§ 793(h), 794(d), 798(d); Klein, supra note 8, at 438-439.

each violation of Energy Department regulations regarding dissemination of unclassified information about nuclear facilities.[1630]

The government can also use injunctions to prevent disclosures of information. The courts have generally upheld injunctions against former employees' publishing information they learned through access to classified information.[1631] The Supreme Court also upheld the State Department's revocation of passports for overseas travel by persons planning to expose U.S. covert intelligence agents, despite the fact that the purpose was to disrupt U.S. intelligence activities rather than to assist a foreign government.[1632]

Similarly, the government can enjoin publication of inventions when it is determined that the release of such information is detrimental to the national security. If an inventor files a patent application for an invention that the Commissioner of Patents believes should not be made public, the Commissioner may place a secrecy order on the patent and establish conditions for granting a patent, or may withhold grant of a patent as long as the "national interest requires [it]."[1633] In addition to criminal penalties cited previously, in the case of an unauthorized disclosure or foreign filing of the patent information, the Patent Office will deem the invention to be "abandoned," which means a forfeiture by the applicant, his successors, or assigns of all claims against the United States based on the invention.[1634]

The government has had less success trying to enjoin the media from disclosing classified information. Most famously, the government failed to enjoin publication of the Pentagon Papers by a newspaper, even though the information was clearly classified and had been stolen by someone with access to it.[1635] In that case, the Supreme Court set very high standards for imposing prior restraint on the press. Yet in another case, the government was able to enjoin a newspaper from printing information about the design of an atomic bomb, even though the

---

[1630] 42 U.S.C. § 2168(b).

[1631] See United States v. Marchetti, 466 F.2d 1309 (4th Cir. 1972) (granting an injunction to prevent a former CIA agent from publishing a book disclosing government secrets).

[1632] See Haig v. Agee, 453 U.S. 280 (1981).

[1633] 35 U.S.C. § 181. The determination must be renewed on a yearly basis.

[1634] 35 U.S.C. § 182.

[1635] United States v. New York Times, 403 U.S. 713 (1971). See Klein, supra note 8, at 439-40.

information did not originate from classified material and the author's purpose was not subversive.[1636]

Prior Legislative Efforts

The current laws for protecting classified information have been criticized as a patchwork of provisions that are not consistent and do not cover all the information the government legitimately needs to protect.[1637] Certain information is protected regardless of whether it belongs to the government or is subject to normal classification. Technical and scientific information, for example, can be restricted regardless of source.[1638] Information related to "the national defense" is protected even though no harm to the national security is intended or is likely to be caused through its disclosure. However, nonmilitary information with the potential to cause serious damage to the national security is only protected from willful disclosure with the specific intent to harm the national interest,[1639] or with the knowledge that such harm could occur.[1640]

In 2000, and again in 2002, Congress sought to create 18 U.S.C. § 798A, subsection (a) of which would have read:

> *Whoever, being an officer or employee of the United States, a former or retired officer or employee of the United States, any other person with authorized access to classified information, or any other person formerly with authorized access to classified information, knowingly and willfully discloses, or attempts to disclose, any classified information acquired as a result of such person's authorized access to classified information to a person*

[1636] See DuVal, supra note 12, at 604 (describing Progressive magazine article at issue in United States v. Progressive, Inc., 467 F.Supp. 990 (W.D. Wis. 1979)); Klein, supra note 8, at 435 (noting disparity between rulings in New York Times and Progressive). The information the Progressive sought to publish was related to the building of a nuclear bomb and was thus classified as "Restricted Data" under the Atomic Energy Act, even though the information had been compiled from unclassified, publicly available documents. One reason for the different outcomes in the two cases is that the Atomic Energy Act contains statutory authorization for the Attorney General to seek injunction. See 42 U.S.C. § 2280. In New York Times, a majority of Justices took into account the fact that Congress had not authorized an injunction. 403 U.S. at 718 (Black, J., concurring); id. at 721-22 (Douglas, J., concurring); id. at 730 (Stewart, J., concurring); id. at 731-40 (White, J., concurring); id. at 742 (Marshall, J., concurring).

[1637] See E.E.B. and K.E.M., Note, Plugging the Leak: The Case for a Legislative Resolution of the Conflict between the Demands of Secrecy and the Need for Open Government, 71 VA. L. REV. 801, 811 (1985).

[1638] See id. at 814.

[1639] See id. at 815.

[1640] See United States v. Morison, 844 F.2d 1057 (1988).

(other than an officer or employee of the United States) who is not authorized access to such classified information, knowing that the person is not authorized access to such classified information, shall be fined under this title, imprisoned not more than 3 years, or both.

The new provision would have penalized the disclosure of any material designated as classified for any reason related to national security, regardless of whether the violator intended that the information be delivered to and used by foreign agents (in contrast to 50 U.S.C. § 783). It would have been the first law to penalize disclosure of information to entities other than foreign governments or their equivalent solely because it is classified, without a more specific definition of the type of information covered.[1641] In short, the provision would have made it a crime to disclose or attempt to disclose classified information[1642] to any person who does not have authorized access to such information, with exceptions covering disclosures to Article III courts, or to the Senate or House committees or Members, and for authorized disclosures to persons acting on behalf of a foreign power (including an international organization). The provision would have amended the espionage laws in title 18 by expanding the scope of information they cover. The proposed language was intended to make it easier for the government to prosecute unauthorized disclosures of classified information, or "leaks" of information that might not amount to a violation of current statutes. The language was intended to ease the government's burden of proof in such cases by eliminating the need "to prove that damage to the national securityhas or will result from the unauthorized disclosure,"[1643] substituting a requirement to show that the unauthorized disclosure was of information that "is or has been properly classified" under a statute or executive order.

[1641] 18 USCS § 1924 prohibits removal of government-owned or controlled classified information by a government employee without authorization. 50 U.S.C. § 783 covers only information classified by the President or an executive agency transmitted by a government employee to a foreign government. 18 U.S.C. §§ 793 and 794 are potentially broader than these in that they cover information "related to the national defense," by government employees and others without regard to the identity of the recipient of the information, but these require intent or knowledge regarding harm to the national defense.

[1642] "Classified information" was defined in the proposed measure to mean "information or material designated and clearly marked or represented, or that the person knows or has reason to believe has been determined by appropriate authorities, pursuant to the provisions of a statute or Executive Order, as requiring protection against unauthorized disclosure for reasons of national security."

[1643] See H.Rept. 106-969 at 44 (2000).

The 106th Congress passed the measure,[1644] but President Clinton vetoed it, calling it "well-intentioned" as an effort to deal with a legitimate concerns about the damage caused by unauthorized disclosures, but "badly flawed" in that it was "overbroad" and posed a risk of "unnecessarily chill[ing] legitimate activities that are at the heart of a democracy."[1645] The President explained his view that

> *[a] desire to avoid the risk that their good faith choice of words — their exercise of judgment — could become the subject of a criminal referral for prosecution might discourage Government officials from engaging even in appropriate public discussion, press briefings, or other legitimate official activities. Similarly, the legislation may unduly restrain the ability of former Government officials to teach, write, or engage in any activity aimed at building public understanding of complex issues. Incurring such risks is unnecessary and inappropriate in a society built on freedom of expression and the consent of the governed and is particularly inadvisable in a context in which the range of classified materials is so extensive. In such circumstances, this criminal provision would, in my view, create an undue chilling effect.*[1646]

The 108th Congress considered passing an identical provision as part of the Intelligence Authorization Act for Fiscal Year 2001,[1647] but instead directed the Attorney General and heads of other departments to undertake a review of the current protections against the unauthorized disclosure of classified information, and to issue a report recommending legislative or administrative actions.[1648] An identical measure was introduced late in the 109th Congress, but was not reported out of committee.[1649]

The Attorney General, in his report to the 108th Congress, concluded that

> *[a]lthough there is no single statute that provides criminal penalties for all types of unauthorized disclosures of classified information, unauthorized disclosures of classified information*

[1644] H.R. 4392 § 304, 106th Congress.

[1645] Message on Returning Without Approval to the House of Representatives the "Intelligence Authorization Act for Fiscal Year 2001", 36 WEEKLY COMP. PRES. DOC. 278 (Nov. 4, 2000).

[1646] Id.

[1647] The Classified Information Protection Act of 2001, H.R. 2943, 107th Cong.

[1648] Intelligence Authorization Act for Fiscal Year 2002, P.L. 107-108, § 310 (2001).

[1649] S. 3774, 109th Cong.

fall within the scope of various current statutory criminal prohibitions. It must be acknowledged that there is no comprehensive statute that provides criminal penalties for the unauthorized disclosure of classified information irrespective of the type of information or recipient involved. Given the nature of unauthorized disclosures of classified information that have occurred, however, I conclude that current statutes provide a legal basis to prosecute those who engage in unauthorized disclosures, if they can be identified. It may be that carefully drafted legislation specifically tailored to unauthorized disclosures of classified information generally, rather than to espionage, could enhance our investigative efforts. The extent to which such a provision would yield any practical additional benefits to the government in terms of improving our ability to identify those who engage in unauthorized disclosures of classified information or deterring such activity is unclear, however.[1650]

Constitutional Issues

The publication of information pertaining to the national defense may serve the public interest by providing citizens with information necessary to shed light on the workings of government, but some observe a consensus that the public release of at least some defense information poses a significant enough threat to the security of the nation that the public interest is better served by keeping it secret. The Constitution protects the public right to access government information and to express opinions regarding the functioning of the government, among other things, but it also charges the government with "providing for the common defense." Policymakers are faced with the task of balancing these interests.

The First Amendment to the U.S. Constitution provides: "Congress shall make no law ... abridging the freedom of speech, or of the press...."[1651] Despite this absolute language, the Supreme Court has held that "[t]he Government may ... regulate the content of constitutionally protected speech in order to promote a compelling interest if it chooses the least restrictive means to further the articulated interest."[1652]

[1650] Report to Congress on Unauthorized Disclosure of Classified Information, Oct. 15, 2002 (citations omitted).

[1651] For an analysis of exceptions to the First Amendment, see CRS Report 95-815, Freedom of Speech and Press: Exceptions to the First Amendment, by Henry Cohen.

[1652] Sable Communications of California v. Federal Communications Commission, 492 U.S. 115, 126 (1989).

First Amendment Principles

Where speech is restricted based on its content, the Supreme Court generally applies "strict scrutiny," which means that it will uphold a content-based restriction only if it is necessary "to promote a compelling interest," and is "the least restrictive means to further the articulated interest."[1653]

Compelling Interest

Protection of the national security from external threat is without doubt a compelling government interest.[1654] It has long been accepted that the government has a compelling need to suppress certain types of speech, particularly during time of war or heightened risk of hostilities.[1655] Speech likely to incite immediate violence, for example, may be suppressed.[1656] Speech that would give military advantage to a foreign enemy is also susceptible to government regulation.[1657]

Where First Amendment rights are implicated, it is the government's burden to show that its interest is sufficiently compelling to justify enforcement. Whether the government has a compelling need to punish disclosures of classified information turns on whether the disclosure has the potential of causing damage to the national defense or foreign relations of the United States.[1658] Actual damage need not be proved, but potential damage must be more than merely speculative and incidental.[1659]

[1653] Id.

[1654] See Haig v. Agee, 453 U.S. 280 (1981) ("It is 'obvious and unarguable' that no governmental interest is more compelling than the security of the Nation.")(citing Aptheker v. Secretary of State, 378 U.S., at 509; accord Cole v. Young, 351 U.S. 536, 546 (1956)).

[1655] See Schenck v. United States, 249 U.S. 47 (1919) (formulating "clear and present danger" test).

[1656] Brandenburg v. Ohio, 395 U.S. 444 (1969).

[1657] Near v. Minnesota, 283 U.S. 697, 716 (1931) ("No one would question but that a government might prevent actual obstruction to its recruiting service or the publication of the sailing dates of transports or the number and location of troops.").

[1658] "National Security" is defined as national defense and foreign relations. See Exec.Order No. 12,958, 60 Fed. Reg.19,825 (Apr. 17, 1995).

[1659] See, e.g., New York Times Co. v. United States, 403 U.S. 713, 725 (1971) (Brennan, J., concurring) (rejecting as insufficient government's assertions that publication of Pentagon Papers "could," "might," or "may" prejudice the national interest); Elrod v. Burns, 427 U.S. 347, 362 (1976) ("The interest advanced must be paramount, one of vital importance, and the burden is on the government to show the existence of such an interest.")(citing Buckley v. Valeo, 424 U.S. 1, 94(1976); Williams v. Rhodes, 393 U.S. 23, 31-33(1968); NAACP v. Button, 371 U.S. 38, 45

Promotion of that Interest

In addition to showing that the stated interest to be served by the statute is compelling, the government must also show that the law actually serves that end. If the accused can show that the statute serves an unrelated purpose — for example, to silence criticism of certain government policies or to manipulate public opinion — a judge might be prepared to invalidate the statute.[1660] If, for example, the government releases some positive results of a secret weapons program while suppressing negative results, a person prosecuted for releasing negative information could challenge the statute by arguing that his prosecution is related to the negative content of his speech rather than to valid concerns about the damage it might cause. If he can show that those who disclose sensitive information that tends to support the administration's position are not prosecuted, while those who disclose truthful information that is useful to its opponents are prosecuted, he might be able to persuade a court that the statute as enforced is an unconstitutional restriction of speech based on impermissible content-related interests.[1661]

Least Restrictive Means

To survive a constitutional challenge, a law must be narrowly drawn to affect only the type of speech that the government has a compelling need to suppress.[1662] A statute that reaches speech that the government has no sufficiently compelling need to regulate may be subject to attack due to overbreadth. A law is overly broad if it prohibits more speech than is necessary to achieve its purpose. If a defendant can show that a statute regulating speech is "substantially overbroad," he may challenge its validity on its face.[1663] If the law is found to be substantially overbroad, a court will invalidate the law even if the defendant's conduct falls within the ambit of conduct that the government may legitimately prohibit. For this reason, a statute that relies solely on the Executive's classification of information to determine the need for its protection might be contested as

---

(1963); Bates v. Little Rock, 361 U.S. 516, 524 (1960); NAACP v. Alabama, 357 U.S. 449, 464-466 (1958); Thomas v. Collins, 323 U.S. 516, 530 (1945)).

[1660] In all likelihood, such a defendant would have to prove not only that such an impermissible use is possible, but also that it is pertinent to the particular case.

[1661] Cf. R.A.V. v. City of St. Paul, 505 U.S. 377 (1992); but see Snepp v. United States, 444 U.S. 507 (1980)(Stevens, J., dissenting). Snepp's assertion of selective enforcement against his book based on its critical treatment of the CIA failed to persuade the Supreme Court that any violation of the First Amendment had occurred. See Judith Schenk Koffler and Bennett L. Gershman, National Security and Civil Liberties: The New Seditious Libel, 69 CORNELL L. REV. 816, 847 (1984).

[1662] See E.E.B. and K.E.M., supra note 1, at 849.

[1663] Broadrick v. Oklahoma, 413 U.S. 601 (1973).

overbroad.[1664] If a challenger were able to show that agencies classify information that it is unnecessary to keep secret, he could argue that the statute is invalid as overly broad because it punishes protected speech that poses no danger to the national security.

Although information properly classified in accordance with statute or executive order carries by definition, if disclosed to a person not authorized to receive it, the potential of causing at least identifiable harm to the national security of the United States,[1665] it does not necessarily follow that government classification by itself will be dispositive of the issue in the context of a criminal trial. Government classification will likely serve as strong evidence to support the contention. Typically, courts have been unwilling to review decisions of the executive related to national security, or have made a strong presumption that the material at issue is potentially damaging.[1666] In the context of a criminal trial, especially in a case with apparent First Amendment implications, courts may be more willing to engage in an evaluation of the propriety of a classification decision than they would in a case of citizens seeking access to information under the Freedom of Information Act (FOIA).[1667]

The Supreme Court seems satisfied that national security is a vital interest sufficient to justify some intrusion into activities that would otherwise be protected by the First Amendment — at least with respect to federal employees.

[1664] Courts have rejected challenges of the Espionage Act based on overbreadth stemming from the imprecision of the term "information related to the national defense" by reading other requirements into the statute. See, e.g., United States v. Rosen, 445 F.Supp.2d 602, 643 (E.D. Va. 2006)(rejecting overbreadth challenge on the basis of judicial interpretation of 18 U.S.C. § 793 that requires the government to prove "(1) that the information relates to the nation's military activities, intelligence gathering or foreign policy, (2) that the information is closely held by the government, in that it does not exist in the public domain; and (3) that the information is such that its disclosure could cause injury to the nation's security").

[1665] Exec. Order No. 12,958, 60 Fed. Reg.19,825 (Apr. 17, 1995)("Classified National Security Information").

Sec. 1.3 defines three levels of classification:

(1) "Top Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.

(2) "Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.

(3) "Confidential" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe. (Emphasis added).

[1666] See, e.g., Haig v. Agee, 453 U.S. 280, 291 (1981) ("Matters intimately related to foreign policy and national security are rarely proper subjects for judicial intervention.").

[1667] 5 U.S.C. § 552(b)(1) exempts classified information from release to requesters.

Although the Court has not held that government classification of material is sufficient to show that its release is damaging to the national security,[1668] it has seemed to accept without much discussion the government's assertion that the material in question is damaging. Lower courts have interpreted 18 U.S.C. § 798, which criminalizes the unauthorized release of specific kinds of classified information,[1669] to have no requirement that the government prove that the classification was proper or personally approved by the President.[1670] It is unlikely that a defendant's bare assertion that information is unlikely to damage U.S. national security will be persuasive without some convincing evidence to that effect, or proof that the information is not closely guarded by the government.[1671]

Snepp v. United States[1672] affirmed the government's ability to enforce contractual non-disclosure agreements against employees and former employees who had had access to classified information. The Supreme Court allowed the government to impose a constructive trust on the earnings from Frank Snepp's book about the CIA because he had failed to submit it to the CIA for prepublication review, as he had agreed to do by signing an employment agreement. Although the CIA stipulated to the fact that the book contained no classified information,[1673] the Court accepted the finding that the book caused "irreparable harm and loss" to the American intelligence services.[1674] The Court suggested that the CIA did not need a signed agreement in order to protect its

---

[1668] See, e.g. Scarbeck v. United States, 317 F.2d 546 (D.C. Cir. 1962) (holding government did not have to show documents were properly classified "as affecting the national defense" to convict employee under 50 U.S.C.§ 783, which prohibits government employees from transmitting classified documents to foreign agents or entities).

[1669] 18 U.S.C. § 798 provides in pertinent part:

"(a) Whoever knowingly and willfully communicates, furnishes, transmits, or otherwise makes available to an unauthorized person, ... any classified information ... (2) concerning the design, construction, use, maintenance, or repair of any device, apparatus, or appliance used or prepared or planned for use by the United States ... for cryptographic or communication intelligence purposes; ... (s)hall be fined ... or imprisoned ...."

[1670] See, e.g. United States v. Boyce, 594 F.2d 1246, 1251 (9th Cir. 1979) ("Under section 798, the propriety of the classification is irrelevant. The fact of classification of a document or documents is enough to satisfy the classification element of the offense.").

[1671] See United States v. Dedeyan, 594 F.2d 36, 39 (4th Cir. 1978).

[1672] 444 U.S. 507 (1980).

[1673] Id. at 511.

[1674] Id. at 512.

interests by subjecting its former employees to prepublication review and possible censorship.[1675]

Haig v. Agee[1676] was a First Amendment challenge to the government's ability to revoke a citizen's passport because of his intent to disclose classified information. Philip Agee was a former CIA agent who engaged in a "campaign to fight the United States CIA," which included publishing names of CIA operatives around the world. In order to put a stop to this activity, the Department of State revoked his passport. Agee challenged that action as an impermissible burden on his freedom to travel and an effort to penalize his exercise of free speech to criticize the government.[1677] The Supreme Court disagreed, finding the passport regulations constitutional because they may be applied "only in cases involving likelihood of 'serious damage' to national security or foreign policy."[1678]

United States v. Morison[1679] is significant in that it represents the first case in which a person was convicted for selling classified documents to the media. Morison argued that the espionage statutes did not apply to his conduct because he could not have had the requisite intent to commit espionage. The Fourth Circuit rejected his appeal, finding the intent to sell photographs that he clearly knew to be classified sufficient to satisfy the scienter requirement under 18 U.S.C. § 793. The definition of "relating to the national defense" was not overbroad because the jury had been instructed that the government had the burden of showing that the information was so related.[1680]

Prior Restraint

In addition to restricting the disclosure of information by prosecuting the person responsible after the fact, the government may seek to prevent publication by prior restraint (i.e., seeking a temporary restraining order or an injunction from a

---

[1675] Id. at 509, n3 ("Moreover, this Court's cases make clear that - even in the absence of an express agreement - the CIA could have acted to protect substantial government interests by imposing reasonable restrictions on employee activities that in other contexts might be protected by the First Amendment")(citations omitted).

[1676] 453 U.S. 280 (1981).

[1677] Id. at 305.

[1678] Id. at 305-06.

[1679] 844 F.2d 1057 (4th Cir.), cert. denied, 488 U.S. 908 (1988).

[1680] But see Scarbeck v. United States, 317 F.2d 546 (D.C. Cir. 1962) (holding that government did not need to prove proper classification of documents to prove a violation).

court to enjoin publication).[1681] The Supreme Court, however, is unlikely to uphold such an order. It has written:

> *[P]rior restraints are the most serious and least tolerable infringement on First Amendment rights.... A prior restraint, ... by definition, has an immediate and irreversible sanction. If it can be said that a threat of criminal or civil sanctions after publication "chills" speech, prior restraint "freezes" it at least for the time. The damage can be particularly great when the prior restraint falls upon the communication of news and commentary on current events.*[1682]

The government's ability to protect sensitive information was explored in the context of prior restraints of the media in the Pentagon Papers case.[1683] In a per curiam opinion accompanied by nine concurring or dissenting opinions, the Court refused to grant the government's request for an injunction to prevent the New York Times and the Washington Post from printing a classified study of the U.S. involvement in Vietnam. A majority of the justices indicated in dicta, however, that the newspapers — as well as the former government employee who leaked the documents to the press — could be prosecuted under the Espionage Act.[1684]

Due Process

A statute is unconstitutionally vague if it does not permit the ordinary person to determine with reasonable certainty whether his conduct is criminally punishable. Therefore, a statute prohibiting the unauthorized disclosure of classified information must be sufficiently clear to allow a reasonable person to know what conduct is prohibited. Where First Amendment rights are implicated, the concern that a vague statute will have a chilling effect on speech not intended

---

[1681] The Supreme Court struck down an injunction against publishing the Pentagon Papers, writing: "Any system of prior restraints of expression comes to the Court bearing a heavy presumption against its constitutional validity." New York Times Co. v. United States, 403 U.S. 713, 714 (1971).

[1682] Nebraska Press Association v. Stuart, 427 U.S. 539, 559 (1976) (striking down a court order restraining the publication or broadcast of accounts of confessions or admissions made by the defendant at a criminal trial).

[1683] New York Times Co. v. United States, 403 U.S. 713 (1971).

[1684] See David Topol, Note, United States v. Morison: A Threat to the First Amendment Right to Publish Security Information, 43 S.C. L. REV. 581, 586 (noting that six of the nine Pentagon Papers justices suggested that the government could convict the newspapers under the Espionage Act even though it could not enjoin them from printing the documents).

to be covered may make that law particularly vulnerable to judicial invalidation.[1685]

The Espionage Act of 1917[1686] has been challenged for vagueness without success. There have been very few prosecutions under that act for disclosing information related to the national defense. The following elements are necessary to prove an unauthorized disclosure offense under 18 U.S.C. § 793:

1. The information or material disclosed must be related to the national defense, that is, pertaining to any matters "directly and reasonably connected with the defense of our nation against its enemies" that "would be potentially damaging to the United States, or might be useful to an enemy of the United States" and are "closely held" in that the relevant government agency has sought to keep them from the public generally and that these items have not been made public and are not available to the general public.[1687]
2. The disclosure must be made with knowledge that such disclosure is not authorized.
3. There must be an "intent or reason to believe that the information … is to be used to the injury of the United States, or to the advantage of any foreign nation.

There does not appear to be a requirement that the disclosure cause actual harm.[1688] An evil motive is not necessary to satisfy the scienter requirement; the willfulness prong is satisfied by the knowledge that the information may be used to the injury of the United States.[1689] It is irrelevant whether the information was passed to a friendly foreign nation.[1690] A patriotic motive will not likely change the outcome.[1691]

[1685] See Aptheker v. Secretary of State, 378 U.S. 500 (1964); United States v. Robel, 389 U.S. 258 (1967); Smith v. Goguen, 415 U.S. 566, 573 (1974); Village of Shaumberg v. Citizens for a Better Environment, 444 U.S. 620 (1980).

[1686] 18 U.S.C. § 793 et seq.

[1687] See United States v. Morison, 622 F. Supp. 1009, 1010 (D. Md.1985).

[1688] See United States v. Morison, 844 F.2d 1057, 1074 (4th Cir. 1988).

[1689] Id. at 1073.

[1690] Gorin v. United States, 312 U.S. 19, 29 (1941).

[1691] United States v. Morison, 622 F.Supp. 1009 (D. Md. 1985).

The Supreme Court, in *Gorin v. United States*,[1692] upheld portions of the Espionage Act now codified as sections 793 and 794 of title 18, U.S. Code (communication of certain information to a foreign entity) against assertions of vagueness, but only because jury instructions properly established the elements of the crimes, including the scienter requirement and a definition of "national defense" that includes potential damage in case of unauthorized release of protected information and materials. *Gorin* was a "classic case" of espionage, and there was no challenge based on First Amendment rights. The Court agreed with the government that the term "national defense" was not vague; it was satisfied that it "is a generic concept of broad connotations, referring to the military and naval establishments and the related activities of national preparedness."[1693] Whether information was "related to the national defense" was a question for the jury to decide,[1694] based on its determination that the information "may relate or pertain to the usefulness, efficiency or availability of any of the above places, instrumentalities or things for the defense of the United States of America. The connection must not be a strained one nor an arbitrary one. The relationship must be reasonable and direct."[1695] As long as the jury was properly instructed that information not likely to cause damage was not "related to the national defense" for the purpose of the statute, the term was not unconstitutionally vague.

No other challenge to a conviction under the Espionage Act has advanced to the Supreme Court.

Conclusion

Under the present legal framework, the publication of national security information by non-government personnel may be prosecuted under various provisions, but only if the information meets the definition set forth by statute and the disclosure is made with the requisite knowledge or intent with regard to the nature of the damage it could cause. The First Amendment limits Congress's ability to prohibit the publication of information of value to the public, especially with regard to pre-publication injunctions against non-government employees. That the publication of some information has the potential to damage U.S. national security interests is rarely denied, but an agreement on how to protect such information without harming the public's right to know what its government is doing may remain elusive.

[1692] 312 U.S. 19 (1941).

[1693] Id. at 28.

[1694] Id. at 32.

[1695] Id. at 31.

Security Classification Policy and Procedure: E.O. 12958, as Amended, 97-771 (December 31, 2009).

KEVIN R. KOSAR & HAROLD C. RELYEA, CONGRESSIONAL RESEARCH SERV., SECURITY CLASSIFICATION POLICY AND PROCEDURE: E.O. 12958, AS AMENDED (2009), *available at* http://www.intelligencelaw.com/library/secondary/crs/pdf/97-771_12-31-2009.pdf.

Kevin R. Kosar
Analyst in American National Government
kkosar@crs.loc.gov, 7-3968

Acknowledgments
This report originally was written by Harold C. Relyea, who has retired from CRS. Readers with questions about this report's subject matter may contact Kevin R. Kosar.

December 31, 2009

Congressional Research Service

7-5700
www.crs.gov
97-771

Summary

Largely prescribed in a series of successive presidential executive orders issued over the past 50 years, security classification policy and procedure provide the rationale and arrangements for designating information officially secret for reasons of national security, and for its declassification as well. President Franklin D. Roosevelt issued the first executive order (E.O. 8381) in 1940.

Current security classification policy may be found in Executive Order 12958, which was signed by President William Clinton on April 17, 1995. It "prescribes a uniform system for classifying, safeguarding, and declassifying national security information." As issued, E.O. 12958 declared, "If there is significant doubt about the need to classify information, it shall not be classified." Additionally, the order stated "If there is significant doubt about the appropriate level of classification, it shall be classified at the lower level."

President George W. Bush amended Executive Order 12958 via Executive Order 13292 on March 25, 2003. E.O. 13292 made many changes to E.O. 12958, and eliminated both of the aforementioned "significant doubt" provisions.

On May 27, 2009, President Barack Obama ordered a review of E.O. 12958. The assistant to the President for National Security Affairs (commonly known as the National Security Advisor) is required to submit to the President "recommendations and proposed revisions" to E.O. 12958 within 90 days.

President Obama signed an executive order on December 29, 2009, that revoked E.O. 12958 and "prescribes a uniform system for classifying, safeguarding, and declassifying national security information." The order made a number of significant changes to current information policies, such as (1) requiring the establishment of a National Declassification Center at the National Archives; (2) ending the E.O. 13292 policy of empowering the Director of Central Intelligence to block declassification actions; and (3) declaring that "no information may remain classified indefinitely." The President's accompanying memorandum to agency heads orders that a "backlog" of 400 million pages of records be made available to the public by December 31, 2013.

This report will not be updated.

Background

Although formal armed forces information security orders had been in existence since 1869, security classification arrangements assumed a presidential character in 1940. The reasons for this late development are not entirely clear, but it probably was prompted by desires to clarify the authority of civilian personnel in the national defense community to create official secrets, to establish a broader basis for protecting military information in view of growing global hostilities, and to better manage a discretionary power of increasing importance to the entire executive branch.

Relying upon a 1938 statute concerning the security of armed forces installations and equipment and "information relative thereto,"[1696] Franklin D. Roosevelt issued the first presidential security classification directive, E.O. 8381, in March 1940.[1697] However, the legislative history of the statute which the President relied upon to issue his order provided no indication that Congress anticipated that such a security classification arrangement would be created.

Other executive orders followed. E.O. 10104, adding a fourth level of classified information, aligned U.S. information security categories with those of our allies

[1696] 52 Stat. 3.

[1697] President Franklin D. Roosevelt, "Defining Certain Vital Military and Naval Installations and Equipment," 5 Federal Register 1147, March 26, 1940.

in 1950.[1698] A 1951 directive, E.O. 10290, completely overhauled the security classification program.[1699] Information was now classified in the interest of "national security" and classification authority was extended to nonmilitary agencies which presumably had a role in "national security" policy.

Criticism of the 1951 order prompted President Dwight D. Eisenhower to issue a replacement, E.O. 10501, in November 1953.[1700] This directive and later amendments to it, as well as E.O. 11652 of March 8, 1972, and E.O. 12065 of June 28, 1978, successively narrowed the bases and limited discretion for assigning official secrecy to agency records.[1701]

President Ronald W. Reagan issued E.O. 12356 on April 2, 1982.[1702] Quickly, it came under criticism for reversing the limiting trend set by classification orders of the previous 30 years by expanding the categories of classifiable information, mandating that information falling within these categories be classified, making reclassification authority available, admonishing classifiers to err on the side of classification, and eliminating automatic declassification arrangements.

With the democratization of many Eastern European countries, the demise of the Soviet Union, and the end of the Cold War, President William J. Clinton, shortly after his inauguration, initiated a sweeping review of Cold War rules on security classification in general and of E.O. 12356 in particular with a view to reform.[1703]

Many began to suspect that the security classification program could be improved when the Department of Defense Security Review Commission, chaired by retired General Richard G. Stilwell, declared in 1985 that there were "no verifiable

---

[1698] President Harry S Truman, "Defining Certain Vital Military and Naval Installations and Equipment as Requiring Protection Against the General Dissemination of Information Relative Thereto," 15 Federal Register 597, February 3, 1950.

[1699] President Harry S Truman, "Prescribing Regulations Establishing Minimum Standards for the Classification, Transmission, and Handling, by Department and Agencies of the Executive Branch, of Official Information Which Requires Safeguarding in the Interest of the Security of the United States," 16 Federal Register 9795, September 27, 1951.

[1700] President Dwight D. Eisenhower, "Safeguarding Official Information in the Interests of the Defense of the United States," 18 Federal Register 7049, November 10, 1953.

[1701] President Richard M. Nixon, "Classification and Declassification of National Security Information and Material," 37 Federal Register 5209, March 10, 1972; and President James E. Carter, "National Security Information," 43 Federal Register 28249, July 3, 1978.

[1702] President Ronald W. Reagan, "National Security Information," 14 Federal Register 14874, April 6, 1982.

[1703] Tim Weiner, "President Moves to Release Classified U.S. Documents," New York Times, May 5, 1993, p. A18.

figures as to the amount of classified material produced in DoD and in defense industry each year." Nonetheless, it was concluded that "too much information appears to be classified and much at higher levels than is warranted."[1704]

The cost of the security classification program became clearer when the General Accounting Office (now Government Accountability Office) reported in October 1993 that it was "able to identify government wide costs directly applicable to national security information totaling over $350 million for 1992." After breaking this figure down—it included only $6 million for declassification work—the report added that "the U.S. government also spends additional billions of dollars annually to safeguard information, personnel, and property."[1705]

Established in April 1993, the President's security classification task force transmitted its initial draft order to the White House seven months later. Circulated among the departments and agencies for comment, the proposal encountered strong opposition from officials within the intelligence and defense communities.[1706] More revision of the draft directive followed.

As delay in issuing the new order continued, some in Congress considered legislating a statutory basis for classifying information in the spring of 1994.[1707] In the fall, the President issued E.O. 12937 declassifying selected retired records at the National Archives.[1708] After months of unresolved conflict over designating an oversight and policy direction agency, a compromise version of the order was given presidential approval in April 1995.

Clinton's Executive Order 12958 As Issued

The Clinton order, as initially issued, authorizes the classification of information for reasons of "national security," which "means the national defense or foreign

---

[1704] U.S. Department of Defense, Department of Defense Security Review Commission, Keeping The Nation's Secrets (Washington: GPO, 1985), pp. 48-49.

[1705] U. S. General Accounting Office, Classified Information: Costs of Protection Are Integrated With Other Security Costs, GAO Report GAO/NSIAD-94-55 (Washington: October 1993), p. 1.

[1706] See David C. Morrison, "For Whose Eyes Only?," National Journal, vol. 26, February 26, 1994, pp. 472-476; Tim Weiner, "U.S. Plans Overhaul on Secrecy, Seeking to Open Millions of Files," New York Times, March 18, 1994, pp. A1, B6; and R. Jeffrey Smith, "CIA, Others Opposing White House Move to Bare Decades-Old Secrets," Washington Post, March 30, 1994, p. A14.

[1707] See U. S. Congress, House Permanent Select Committee on Intelligence, A Statutory Basis for Classifying Information, hearing, 103rd Cong., 2nd sess., March 16, 1994 (Washington: GPO, 1995).

[1708] President William J. Clinton, "Declassification of Selected Records within the National Archives of the United States," 59 Federal Register 59097, November 15, 1994, at http://www.archives.gov/federal-register/executive-orders/ pdf/12937.pdf.

relations of the United States."[1709] Regarding the threshold consideration as to whether a classification action should occur, the order states: "If there is significant doubt about the need to classify information, it shall not be classified." No explanation of the term "significant" is provided. Nonetheless, it reversed the policy of E.O. 12356, which directed classifiers to err on the side of classification in questionable cases.

E.O. 12958 retains three classification levels, identified by the traditional Top Secret, Secret, and Confidential markings. Again reversing E.O. 12356 policy, the Clinton order states: "If there is significant doubt about the appropriate level of classification, it shall be classified at the lower level." This too was a reversal of E.O. 12356, which required classification at the higher level. The classification categories specified in E.O. 12958—identifying inclusively the information subjects that may be considered for classification—are the same as those of E.O. 12356, with one exception. E.O. 12356 explicitly provided for the President to create additional classification categories. No such allowance is stated in E.O. 12958; any additional category had to be appended by a subsequent executive order.

Prescribing Declassification

Unlike E.O. 12356, E.O. 12958 limits the duration of classification. When information is originally classified, an attempt is to be made "to establish a specific date or event for declassification." Alternatively, if a short-term time or event for declassification cannot be determined, the new order sets a 10-year terminus. However, allowance is made for extending the duration of classification beyond the 10-year limit in selected cases and in accordance with prescribed procedures and conditions. In brief, the intent appears to be that only a small quantity of the most highly sensitive information would be maintained under security classification for periods longer than 10 years.

Other arrangements are specified for the automatic declassification of historic government records—those that are more than 25 years old and have been determined by the Archivist of the United States to have permanent historical value. E.O. 12958 mandates the beginning of government wide declassification of historic records five years hence, shortly after the turn of the century. Allowance is made for continuing the classification of these materials in selected cases and in accordance with prescribed procedures and conditions. Once again, the intent appears to be that only a small quantity of the most highly sensitive historic records would be maintained under security classification. The Archivist,

---

[1709] President William J. Clinton, "Executive Order 12958—Classified National Security Information," 60 Federal Register 19825, April 20, 1995, at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=1995_register&docid= fr20ap95-135.pdf.

according to the Clinton order, "shall establish a Government wide database of information that has been declassified."

Furthermore, E.O. 12958 continues the mandatory declassification review requirement of E.O. 12356. This provision authorizes a person to request that almost any classified record be reviewed with a view to being declassified and publicly disclosed. Similarly, if an agency record requested pursuant to the Freedom of Information Act is found to be security classified, mandatory declassification review also occurs.

Controversial Areas

A few provisions of E.O. 12958 may be considered controversial. The Clinton order states that information "may not be reclassified after it has been declassified and released to the public under proper authority." The reference to "proper authority" means that the information has not been disclosed through a leak. However, some question remains as to how "public" the proper disclosure must be to preclude retrieval and reclassification when some higher authority, having second thoughts, wants to stop disclosure.

Similarly, the Clinton order states: "Compilations of items of information which are individually unclassified may be classified if the compiled information reveals an additional association or relationship that (1) meets the standards for classification under this order; and (2) is not otherwise revealed in the individual items of information." At issue here is the so-called "mosaic theory" that individual items of unclassified information, in aggregation, result in classifiable information. At dispute is the question of perception: government officials classify aggregated unclassified information items because they fear that harm to the national security could result if the aggregation were publicly disclosed.

E.O. 12958 continues to allow agency officials to "refuse to confirm or deny the existence or nonexistence of requested information whenever the fact of its existence or nonexistence is itself classified under this order."

Classification Challenges

E.O. 12958 authorized classification challenges. "Authorized holders of information who, in good faith, believe that its classification status is improper," says the order, "are encouraged and expected to challenge the classification status of the information in accordance with agency procedures."

A Balancing Test

Another innovation, first introduced by E.O. 12065, President Jimmy Carter's security classification directive, but eliminated in E.O. 12356, is the so-called balancing test. According to E.O. 12958, where "the need to protect ... information may be outweighed by the public interest in disclosure of the

information, and in these cases the information should be declassified," the question "shall be referred to the agency head or the senior agency official" responsible for classification matters for resolution. Because there was insufficient opportunity for the balancing test of E.O. 12065 to be implemented, the effect of the provision could not be assessed. E.O. 12958 provides an opportunity to conduct such an analysis sometime in the future.

Program Direction

E.O. 12958 originally vested responsibility for implementing and supervising the security classification program in the director of the Office of Management and Budget (OMB), assisted by the director of the Information Security Oversight Office (ISOO).[1710] The Clinton order also indicates that the Security Policy Board, a secretive body established in May 1994 by Presidential Decision Directive 29, a classified instrument, "shall make a recommendation to the President ... with respect to the issuance of a Presidential directive on safeguarding classified information." This subsequent directive, according to E.O. 12958, "shall pertain to the handling, storage, distribution, transmittal and destruction of and accounting for classified information."

New Organizations

Finally, E.O. 12958 creates two new entities. The first of these, the Interagency Security Classification Appeals Panel (ISCAP), is composed of senior level representatives of the Secretary of State, Secretary of Defense, Attorney General, Director of Central Intelligence, Archivist of the United States, and Assistant to the President for National Security Affairs. The President selects the panel's chair from among its members. The ISOO director serves as the ISCAP executive secretary and provides support staff. The functions of the panel, as specified in the Clinton order, are (1) to make final determinations on classification challenges appealed to it; (2) to approve, deny, or amend exemptions from automatic declassification sought by agencies; (3) to make final determinations on mandatory declassification review requests appealed to it; and, (4) generally, to advise and assist the President "in the discharge of his constitutional and discretionary authority to protect the national security of the United States."

The second body established by the Clinton executive order, the Information Security Policy Advisory Council (ISPAC), is "composed of seven members appointed by the President for staggered terms not to exceed four years, from among persons who have demonstrated interest and expertise in an area related

---

[1710] Conferees on the FY1995 Treasury, Postal Service, and Executive Office of the President appropriation transferred ISOO from the General Services Administration to OMB (H.Rept. 103-741, p. 42). At the recommendation of the OMB director, conferees on the FY1996 Treasury, Postal Service, and Executive Office of the President appropriation transferred ISOO to the National Archives and Records Administration (H.Rept. 104-291, pp. 41-42).

to the subject matters of [E.O. 12958] and are not otherwise employees of the Federal Government." The functions of the ISPAC, as specified in the order, are to "(1) advise the President, the Assistant to the President for National Security Affairs, the Director of the Office of Management and Budget, or such other executive branch officials as it deems appropriate, on policies established under [E.O. 12958] or its implementing directives, including recommended changes to those policies; (2) provide recommendations to agency heads for specific subject areas for systematic declassification review; and (3) serve as a forum to discuss policy issues in dispute."

E.O. 12958 became effective on October 15, 1995, 180 days from the date of its issuance by the President.[1711] An amending directive, E.O. 13142 of November 19, 1999, largely effected technical changes reflecting the transfer of ISOO to the National Archives and the administrative direction of the Archivist.[1712]

Bush's Amendments to E.O. 12958

Further amendment of E.O. 12958 occurred in late March 2003 when President George W. Bush issued E.O. 13292.[1713] The product of a review and reassessment initiated in the summer of 2001, the directive, among other changes,

- eliminated the Clinton order's standard that information should not be classified if there is "significant doubt" about the need to do so;
- treats information obtained in confidence from foreign governments as classified;
- authorizes the Vice President, "in the performance of executive duties," to classify information originally;
- adds "infrastructures" and "protection services" to the categories of classifiable information;
- eases the reclassification of declassified records;
- postpones the starting date for automatic declassification of protected records 25 or more years old from April 17, 2003, to December 31, 2006;
- eliminates the requirement that agencies prepare plans for declassifying records;
- cancels the order requiring the Archivist to create a "government wide database of information that has been declassified," and instead requires

---

[1711] The implementing regulation is Office of Management and Budget, "Information Security Oversight Office; Classified National Security Information," 60 Federal Register 53493, October 13, 1995.

[1712] President William J. Clinton, "Amendment to Executive Order 12958–Classified National Security Information," 64 Federal Register 66089, November 23, 1999.

[1713] See Federal Register, vol. 68, March 28, 2003, pp. 15315-15334, at http://edocket.access.gpo.gov/2003/pdf/037736.pdf. E.O. 12958 as amended also may be found at http://www.archives.gov/isoo/policy-documents/eo-12958amendment.html.

the "Director of the Information Security Oversight Office … [to] coordinate the linkage and effective utilization of existing agency databases of records that have been declassified and publicly released"; and

- permits the Director of Central Intelligence to block declassification actions of the ISCAP, unless overruled by the President.

Since E.O. 13292 was issued, there have been no further changes to E.O. 12958.

Obama's Review of E.O. 12958

On May 27, 2009, President Barack H. Obama issued a memorandum ordering a review of E.O. 12958.[1714] The President wrote,

> *[M]y Administration is committed to operating with an unprecedented level of openness. While the Government must be able to prevent the public disclosure of information where such disclosure would compromise the privacy of American citizens, national security, or other legitimate interests, a democratic government accountable to the people must be as transparent as possible and must not withhold information for self-serving reasons or simply to avoid embarrassment.*[1715]

To achieve these goals, the assistant to the President for National Security Affairs (commonly known as the National Security Advisor) is to submit to the President "recommendations and proposed revisions" to E.O. 12958 regarding[1716]

(i) Establishment of a National Declassification Center to bring appropriate agency officials together to perform collaborative declassification review under the administration of the Archivist of the United States;

(ii) Effective measures to address the problem of over classification, including the possible restoration of the presumption against classification, which would preclude classification of information where there is significant doubt about the need for such classification, and the implementation of increased accountability for classification decisions;

[1714] President Barack H. Obama, "Memorandum of May 27, 2009—Classified Information and Controlled Unclassified Information," 74 Federal Register 26277-26280, June 1, 2009.

[1715] Ibid., p. 26277.

[1716] The memorandum also orders a review of the procedures for controlled unclassified information. For an introduction to this topic, see the National Archives, "What is Controlled Unclassified Information?" at http://www.archives.gov/ cui/.

(iii) Changes needed to facilitate greater sharing of classified information among appropriate parties;
(iv) Appropriate prohibition of reclassification of material that has been declassified and released to the public under proper authority;
(v) Appropriate classification, safeguarding, accessibility, and declassification of information in the electronic environment, as recommended by the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction and others; and
(vi) Any other measures appropriate to provide for greater openness and transparency in the Government's security classification and declassification program while also affording necessary protection to the Government's legitimate interests.[1717]

The National Security Advisor's response was due in 90 days.

Obama Revokes E.O. 12958 and Issues a New Executive Order

President Obama signed an executive order on December 29, 2009, that revokes E.O. 12958 and "prescribes a uniform system for classifying, safeguarding, and declassifying national security information."[1718] The order made a number of significant changes to current information policies, such as (1) requiring the establishment of a National Declassification Center at the National Archives; (2) ending the E.O. 13292 policy of empowering the Director of Central Intelligence to block declassification actions; and (3) declaring that "no information may remain classified indefinitely." The President's accompanying memorandum to agency heads directs that

> *Under the direction of the National Declassification Center (NDC), and utilizing recommendations of an ongoing Business Process Review in support of the NDC, referrals and quality assurance problems within a backlog of more than 400 million pages of accessioned Federal records previously subject to automatic declassification shall be addressed in a manner that will permit public access to all declassified records from this backlog no later than December 31, 2013.*[1719]

[1717] President Barack H. Obama, "Memorandum of May 27, 2009—Classified Information and Controlled Unclassified Information," p. 26277.

[1718] President Barack H. Obama, "Executive Order—Classified National Security Information," December 29, 2009, at http://www.whitehouse.gov/the-press-office/executive-order-classified-national-security-information, p. 1.

[1719] President Barack H. Obama, "Presidential Memorandum—Implementation of the Executive Order, 'Classified National Security Information,'" December 29, 2009, at

The memorandum requires the Archivist to "make public a report on the status of the backlog every 6 months."[1720]

---

http://www.whitehouse.gov/the-press-office/presidentialmemorandum-implementation-executive-order-classified-national-security, p. 1.

[1720] Ibid.

Protection of National Security Information by Congress

Protection of Classified Information by Congress: Practices and Proposals, RS20748 (January 27, 2010).

FREDERICK M. KAISER, CONGRESSIONAL RESEARCH SERV., PROTECTION OF CLASSIFIED INFORMATION BY CONGRESS: PRACTICES AND PROPOSALS (2010), *available at* http://www.intelligencelaw.com/library/secondary/crs/pdf/RS20748_1-27-2010.pdf.

Frederick M. Kaiser
Specialist in American National Government
fkaiser@crs.loc.gov, 7-8682

Specialist in American National Government

January 27, 2010

Congressional Research Service

7-5700
www.crs.gov
RS20748

Summary

The protection of classified national security and other controlled information is of concern not only to the executive branch—which determines what information is to be safeguarded, for the most part—but also to Congress, which uses the information to fulfill its constitutional responsibilities, particularly overseeing the executive as well as legislating public policy. It has established mechanisms to safeguard controlled information in its custody, although these arrangements have varied over time, between the two chambers, and among panels in each. Both chambers, for instance, have created offices of security to consolidate relevant responsibilities, although these were established two decades apart. Other differences exist at the committee level. Proposals for change, some of which are controversial, usually seek to set uniform standards or heighten requirements for access. Classification of national security information is governed for the most part by executive order as well as public law. For coverage of this issue, see CRS Report RL33494, Security Classified and Controlled Information: History, Status, and Emerging Management Issues, by Kevin R. Kosar, and CRS Report RS21900, The Protection of Classified Information: The Legal Framework, by Jennifer K. Elsea, for more information.

This report will be updated as conditions require.

Current Practices and Procedures

Congress relies on a variety of mechanisms and instruments to protect classified information in its custody. These include House and Senate offices responsible for setting and implementing standards for handling classified information; detailed committee rules for controlling access to such information; a secrecy oath for all Members and employees of the House and of some of its committees; security clearances and nondisclosure agreements for staff; and formal procedures for investigations of suspected security violations. Public law, House and Senate rules, and committee rules, as well as custom and practice (including informal arrangements), constitute the bases for these requirements.[1721]

Chamber Offices of Security and Security Manuals

The chambers have approached their security program differently, although each now has an office of security.

Senate

The Senate established an Office of Senate Security in 1987, as the result of a bipartisan effort over two Congresses. It is charged with consolidating

---

[1721] For background, see Herrick S. Fox, "Staffers Find Getting Security Clearances Is Long and Often a Revealing Process," Roll Call, October 30, 2000, pp. 24-25; Frederick M. Kaiser, "Congressional Rules and Conflict Resolution: Access to Information in the House Select Committee on Intelligence," Congress and the Presidency, vol. 15 (1988), pp. 49-73; U.S. Commission on Protecting and Reducing Government Secrecy, Secrecy: Report of the Commission (1997); House Committee on Government Operations, Subcommittee on Legislation and National Security, Congress and the Administration's Secrecy Pledges, Hearings, 100th Cong., 2nd sess. (1988); House Permanent Select Committee on Intelligence, United States Counterintelligence and Security Concerns—1986, 100th Cong., 1st sess., H. Rept. 100-5 (1987), pp. 3-4; Joint Committee on the Organization of Congress, Committee Structure, Hearings, 103rd Cong., 1st sess. (1993), pp. 64-79, 312-316, 406-417, and 832-841; and Senate Select Committee on Intelligence, Meeting the Espionage Challenge, S. Rept. 99-522, 99th Cong., 2nd sess. (1986), pp. 90-95. A number of CRS reports deal with aspects of this area: CRS Report R40136, Congress as a Consumer of Intelligence Information, by Alfred Cumming; CRS Report R40691, Sensitive Covert Action Notifications: Oversight Options for Congress, by Alfred Cumming; CRS Report R40698, "Gang of Four" Congressional Intelligence Notifications, by Alfred Cumming; CRS Report RL32525, Congressional Oversight of Intelligence: Current Structure and Alternatives, by Frederick M. Kaiser; CRS Report R40602, The Department of Homeland Security Intelligence Enterprise: Operational Overview and Oversight Challenges for Congress, by Mark A. Randol; and CRS Report RL33616, Homeland Security Intelligence: Perceptions, Statutory Definitions, and Approaches, by Mark A. Randol.

information and personnel security.[1722] Located in the Office of the Secretary of the Senate, the Security Office sets and implements uniform standards for handling and safeguarding classified and other sensitive information in the Senate's possession. The Security Office's standards, procedures, and requirements—detailed in its Senate Security Manual, initially issued in 1988—"are binding upon all employees of the Senate."[1723] These cover committee and Member office staff and officers of the Senate as well as consultants and contract personnel—but not Members themselves. The regulations extend to a wide range of matters on safeguarding classified information: physical security requirements; procedures for storing materials; mechanisms for protecting communications equipment; security clearances and nondisclosure agreements for all Senate staff needing access; and follow-up investigations of suspected security violations by employees.

House

The House put its own security office in place, under the jurisdiction of the Sergeant at Arms, in 2005, following approval of the chamber's Committee on House Administration.[1724] The office, similar to the Senate predecessor, is charged with developing an Operations Security Program for the House. Its responsibilities and jurisdiction encompass processing security clearances for staff, handling and storing classified information, managing a counterintelligence program for the House, and coordinating security breach investigations. Unlike its Senate counterpart, however, the House Office of Security has not issued a security manual. Prior to the House Office of Security, the chamber had relied on individual committee and Member offices to set requirements following chamber and committee rules, guidelines in internal office procedural manuals, and custom.

Security Clearances and Nondisclosure Agreements for Staff

Security clearances and written nondisclosure agreements can be required for congressional staff but have been handled differently by each chamber.[1725] The

---

[1722] Congressional Record, vol. 133, July 1, 1987, pp. 18506-18507. The resolution creating the new office (S.Res. 243, 100th Cong.) was introduced and approved on the same day.

[1723] U.S. Senate, Office of Senate Security, Security Manual (revised, 2007), preface.

[1724] The two relevant letters—one requesting an Operations Security Program under the direction of the House Sergeant at Arms and the other granting approval—are, respectively, to the Chairman of the House Committee on House Administration, from the House Sergeant at Arms, February 25, 2003; and to the House Sergeant at Arms, from the Chairman of the House Committee on House Administration, March 28, 2003.

[1725] The congressional support agencies—i.e., Congressional Budget Office, Congressional Research Service (as well as the Library of Congress), and Government Accountability Office—

Senate Office of Security mandates such requirements for all Senate employees needing access to classified information.[1726] No comparable across-the-board rules and regulations for security clearances or secrecy agreements yet exist for all House employees, although individual offices require these.[1727] These could be applied by the office of security in the future, if the House agrees.

Secrecy Oath for Members and Staff

The House and Senate differ with regard to secrecy oaths for Members and staff. Beginning with the 104th Congress, the House adopted a secrecy oath for all Members, officers, and employees of the chamber. Before any such person may have access to classified information, he or she must

> *solemnly swear (or affirm) that I will not disclose any classified information received in the course of my service with the House of Representatives, except as authorized by the House of Representatives or in accordance with its Rules.*[1728]

Previously, a similar oath was required for only Members and staff of the House Permanent Select Committee on Intelligence; its requirement had been added in the 102nd Congress as part of the Select Committee's internal rules, following abortive attempts to establish it in public law.[1729] It is still in effect for select committee Members and staff:

> *I do solemnly swear (or affirm) that I will not disclose or cause to be disclosed any classified information in the course of my service on the House Permanent Select Committee on Intelligence, except when authorized to do so by the Committee or the House of Representatives.*[1730]

Other adoptions have occurred under committee rules. The House Committee on Homeland Security, for instance, requires an oath from each Committee Member or staff seeking access, modeled after the one developed by the House

---

have separate personnel security systems and policies. Nonetheless, each requires security clearances for its staff to gain access to classified information.

[1726] Senate Office of Senate Security, Security Manual, pp. 8 and 10.

[1727] See, for example, U.S. House Permanent Select Committee on Intelligence, Rules of Procedure, 111th Cong, (2009), Rules 12(b) and 14(c).

[1728] House Rule XXIII, cl. 13, 111th Congress.

[1729] U.S. Congress, Committee of Conference, Intelligence Authorization Act, Fiscal Year 1992, 102nd Cong., 1st sess., H. Rept. 102-327 (Washington: GPO, 1991), pp. 35-36.

[1730] House Intelligence Committee, Rules, Rule 14(d).

Intelligence Committee.[1731] Neither the full Senate nor any Senate panel apparently imposes a similar obligation on its Members or employees.

Investigation of Security Breaches

The Senate Office of Security and the House counterpart are charged with investigating or coordinating investigations of suspected security violations by employees.[1732] In addition, investigations by the House and Senate Ethics Committees of suspected breaches of security are authorized by each chamber's rules, directly and indirectly. The Senate Ethics Committee, for instance, has the broad duty to "receive complaints and investigate allegations of improper conduct which may reflect upon the Senate, violations of law, violations of the Senate Code of Official Conduct, and violations of rules and regulations of the Senate."[1733] The panel is also directed "to investigate any unauthorized disclosure of intelligence information [from the Senate Intelligence Committee] by a Member, officer or employee of the Senate."[1734] The House, in creating its Permanent Select Committee on Intelligence, issued similar instructions. H.Res. 658 ordered the Committee on Standards of Official Conduct to "investigate any unauthorized disclosure of intelligence or intelligence-related information [from the House Intelligence Committee] by a Member, officer, or employee of the House .... "[1735]

Sharing Information with Non-Committee Members

Procedures controlling access to classified information held by committees exist throughout Congress. These committee and chamber rules set conditions for sharing such information with other panels and Members, determining who is eligible for access to a committee's classified holdings directly or its executive session hearings, who can be given relevant information, and, if so, to what extent and in what form.[1736]

[1731] U.S. House Committee on Homeland Security, Committee Rules, 111th Congress (adopted February 4, 2009), Rule XV(E).

[1732] For House staff, see citations in note 4, above. For Senate staff, see Senate Office of Senate Security, Security Manual, pp. 10-11, which spells out the investigative procedures and penalties for violations.

[1733] S.Res. 388, 88th Congress.

[1734] S.Res. 400, 94th Congress.

[1735] H.Res. 658, 95th Congress.

[1736] For examples of this in the intelligence area, see the following CRS reports: CRS Report R40136, Congress as a Consumer of Intelligence Information, by Alfred Cumming; CRS Report R40691, Sensitive Covert Action Notifications: Oversight Options for Congress, by Alfred Cumming; CRS Report R40698, "Gang of Four" Congressional Intelligence Notifications, by

The most exacting requirements along all of these lines have been developed by the House Permanent Select Committee on Intelligence; the rules are based on its 1977 establishing authority and reinforced by intelligence oversight provisions in public law, such as the 1991 Intelligence Authorization.[1737] The panel's controls apply to select committee Members sharing classified information outside the committee itself as well as to non-committee Representatives seeking access to the panel's holdings.[1738] In the latter case, the requester must go through a multistage process to obtain access.[1739] Consequently, it is possible for a non-committee Member to be: denied attendance at its executive sessions or access to its classified holdings; given only a briefing on it; granted partial access; or allowed full access. When the House Intelligence Committee releases classified information to another panel or non-member, moreover, the recipient must comply with the same rules and procedures that govern the intelligence committee's control and disclosure requirements.[1740] By comparison, rules of the House Armed Services Committee are to "ensure access to information [classified at Secret or higher] by any member of the Committee or any other Member, Delegate, or Resident Commissioner of the House of Representatives .... who has requested the opportunity to review such material."[1741]

Proposals for Change

A variety of proposals—coming from congressional bodies, government commissions, and other groups—have called for changes in the procedures for handling and safeguarding classified information in the custody of Congress. These plans, some of which might be controversial or costly, focus on setting uniform standards for congressional offices and employees and heightening the access eligibility requirements.

Mandate That Members of Congress Hold Security Clearances to Be Eligible for Access to Classified Information

---

Alfred Cumming; CRS Report RL32525, Congressional Oversight of Intelligence: Current Structure and Alternatives, by Frederick M. Kaiser; CRS Report R40602, The Department of Homeland Security Intelligence Enterprise: Operational Overview and Oversight Challenges for Congress, by Mark A. Randol; and CRS Report RL33616, Homeland Security Intelligence: Perceptions, Statutory Definitions, and Approaches, by Mark A. Randol.

[1737] H.Res. 658, 95th Congress; and P.L. 102-88, 105 Stat. 441. For background, see Kaiser, "Congressional Rules and Conflict Resolution."

[1738] Intelligence Committee, Rules, Rules 13(b) and 14(f).

[1739] Ibid., Rule 14(f).

[1740] Ibid., Rule 14(f)(4)(B).

[1741] U.S. House Committee on Armed Services, Rules of the Committee, 111th Congress, Rule 20(b).

This would mark a significant departure from the past. Members of Congress (as with the President and Vice President, Justices of the Supreme Court, or other federal court judges) have never been required to hold security clearances. Most of the proposals along this line appeared in the late 1980s, following charges and countercharges between the executive and legislative branches over unauthorized disclosure of classified information. A more recent bill, introduced in 2006, would have required a security clearance for Members serving on the House Permanent Select Committee on Intelligence and on the Subcommittee on Defense of the House Appropriations Committee.[1742] The resolution, however, did not specify which entity (in the legislative or executive branch) would conduct the background investigation or which officer (in Congress or in the executive) would adjudicate the clearances.

The broad mandate for such clearances could be applied to four different groups: (1) all Senators and Representatives, thus, in effect, becoming a condition for serving in Congress; (2) only Members seeking access to classified information, including those on panels receiving it; (3) only Members on committees which receive classified information; or (4) only those seeking access to classified information held by panels where they are not members.

Under a security clearance requirement, background investigations might be conducted by an executive branch agency, such as the Office of Personnel Management or Federal Bureau of Investigation; by a legislative branch entity, such as the House or Senate Office of Security, or the Government Accountability Office; or possibly by a private investigative firm under contract. Possible adjudicators—that is, the officials who would judge, based on the background investigation, whether applicants would be "trustworthy" and, therefore, eligible for access to classified information—could extend to the majority or minority leaders, a special panel in each chamber, a chamber officer, or even an executive branch officer, if Congress so directed.

The main goals behind this proposed change are to tighten and make uniform standards governing eligibility for access for Members. Proponents maintain that it would help safeguard classified information by ensuring access only by Members deemed "trustworthy" and, thereby, limit the possibility of leaks and inadvertent disclosures. In addition, the clearance process itself might make recipients more conscious of and conscientious about the need to safeguard this information as well as the significance attached to it. As a corollary, supporters might argue that mandating a clearance to serve on a panel possessing classified information could increase its members' appreciation of the information's importance and its protection's priority. This, in turn, might help the committee members gain the access to information that the executive is otherwise reluctant to share and improve comity between the branches.

[1742] H.Res. 747, 109th Congress.

Opponents, by contrast, contend that security clearance requirements would compromise the independence of the legislature if an executive branch agency conducted the background investigation; had access to the information it generated; or adjudicated the clearance. Even if the process was fully under legislative control, concerns might arise over: its fairness, impartiality, objectivity, and correctness (if determined by an inexperienced person); the effects of a negative judgment on a Member, both inside and outside Congress; and the availability of information gathered in the investigation, which may not be accurate or substantiated, to other Members or to another body (such as the chamber's ethics committee or Justice Department), if it is seen as incriminating in matters of ethics or criminality. Opponents might contend, moreover, that adding this new criterion could have an adverse impact on individual Members and the full legislature in other ways. Opponents also maintain that it might impose an unnecessary, unprecedented, and unique (among elected federal officials and court judges) demand on legislators; create two classes of legislators, those with or without a clearance; affect current requirements for non-Member access to holdings of committees whose own members might need clearances; possibly jeopardize participation by Members without clearances in floor or committee proceedings (even secret sessions); and retard the legislative process, while investigations, adjudications, and appeals are conducted.

Direct Senators or Senate Employees to Take or Sign a Secrecy Oath to Be Eligible for Access

This proposal would require a secrecy oath for Senators and staffers, similar to the current requirement for their House counterparts. An earlier attempt to mandate such an oath for all Members and employees of both chambers of Congress seeking access to classified information occurred in 1993; but it was unsuccessful.[1743] If approved, it would have prohibited intelligence entities from providing classified information to Members of Congress and their staff, as well as officers and employees of the executive branch, unless the recipients had signed a nondisclosure agreement—pledging that he or she "will not willfully directly or indirectly disclose to any unauthorized person any classified information"—and the oath had been published in the Congressional Record.[1744]

Direct All Cleared Staff—or Just Those Cleared for the Highest Levels—to File Financial Disclosure Statements Annually

This demand might make it easier to detect and investigate possible misconduct instigated for financial reasons. And many staff with clearances may already file

[1743] Congressional Record, daily ed., vol. 139, Aug. 4, 1993, pp. H5770-H5773; and Nov. 18, 1993, p. H10157.

[1744] Ibid.

financial disclosure statements because of their employment rank or salary level; consequently, few new costs would be added. Nonetheless, objections might arise because the proposal would impose yet another burden on staff and result in additional record-keeping and costs. This requirement's effectiveness in preventing leaks or espionage might also be questioned by opponents.

Require Polygraph Examinations and/or Drug Tests for Staff to Be Eligible for Access to Classified Information

Under such proposals, drug or polygraph tests could be imposed as a condition of employment for personnel in offices holding classified information, only on staff seeking access to such information, or for both employment and access. Objections have been expressed to such tests, especially as a pre-condition of employment, however, because of their cost and questioned reliability and validity.[1745]

[1745] For background on polygraph testing, see CRS Memorandum, Polygraph Examinations of Federal Employees and Applicants, by Frederick M. Kaiser.

National Security Whistleblowers

National Security Whistleblowers, RL33215 (December 30, 2005).

LOUIS FISHER, CONGRESSIONAL RESEARCH SERV., NATIONAL SECURITY WHISTLEBLOWERS (2005), *available at* http://www.intelligencelaw.com/library/secondary/crs/pdf/RL33215_12-30-2005.pdf.

Louis Fisher
Senior Specialist in Separation of Powers
Government and Finance Division

Summary

To discharge its constitutional duties, Congress depends on information obtained from the executive branch. Domestic and national security information is provided through agency reports and direct communications from department heads, but lawmakers also receive information directly from employees within the agencies. They take the initiative in notifying Congress, its committees, and Members of Congress about alleged agency illegalities, corruption, and waste within the agency. This type of information comes from a group known as whistleblowers.

Through such techniques as "gag orders" and nondisclosure agreements, Presidents have attempted to block agency employees from coming directly to Congress. In response, Congress has enacted legislation in an effort to assure the uninterrupted flow of domestic and national security information to lawmakers and their staffs. Members of Congress have made it clear they do not want to depend solely on information provided by agency heads. Overall, the issue has been how to protect employees who are willing to alert Congress about agency wrongdoing.

The first procedures enacted to protect agency whistleblowers appeared in the Civil Service Reform of 1978. It also contained language that excluded protections to whistleblowers who work in federal agencies involved in intelligence and counterintelligence. In 1989, Congress passed the Whistleblower Protection Act in an effort to strengthen statutory protections for federal employees who assist in the elimination of fraud, waste, abuse, illegality, and corruption. That statute continued the exemption for national security information. It did not authorize the disclosure of any information by an agency or any person that is (1) specifically prohibited from disclosure by any other provision of law, or (2) "specifically required by Executive order to be kept secret in the interest of national defense or the conduct of foreign affairs."

Several statutes apply expressly to national security information. Congress has passed a series of laws known collectively as the Military Whistleblowers Protection Act, under which members of the military may give information to Members of Congress. It also passed the Intelligence Community Whistleblower Protection Act of 1998 to encourage the reporting to Congress of wrongdoing within the intelligence agencies. In crafting this legislation, Congress has sought to balance its need for information with national security requirements, giving intelligence community whistleblowers access to Congress only through the intelligence committees. For legal analysis see CRS Report 97-787 A, Whistleblower Protections for Federal Employees, by L. Paige Whitaker and Michael Schmerling.

This report will be updated as events warrant.

National Security Whistleblowers

Congress and the President have often collided over access to information within the executive branch. Although executive officials recognize that they have a duty to keep Congress informed and to share agency documents, domestic as well as national security, on some occasions the executive branch will invoke different types of privileges to block congressional access. Congressional committees can issue subpoenas and either house may hold executive officials in contempt for refusing to release documents or to testify. However, those measures are extreme and are taken only after customary efforts to find a compromise have collapsed. In the midst of some of these confrontations, Presidents have issued orders to executive agencies to limit information to Congress, particularly to prevent agency employees from going directly to Congress. Congress has responded with statutes to keep the lanes of information open.

In cases involving the reporting of sensitive information related to national security, Congress has balanced the competing interests of keeping lawmakers informed while safeguarding secrets. For example, the Intelligence Community Whistleblower Protection Act of 1998 encourages employees of the Intelligence Community to contact Congress but only through the Intelligence Committees.

Introduction

Agency whistleblowers operate within a system of mixed messages. On the one hand, the Code of Ethics adopted by Congress in 1958 directs all government employees to "expose corruption wherever discovered."[1746] Over the years, agency employees have received credit for revealing problems of defense cost overruns, unsafe nuclear power plant conditions, questionable drugs approved for

[1746] 72 Stat. B12 (1958) (H. Con. Res. 175).

marketing, contractillegalities and improprieties, and regulatory corruption.[1747] On the other hand, exposing corruption can result in their being fired, transferred, reprimanded, denied promotion, or harassed. In 1978, a Senate panel found that the fear of reprisal "renders intra-agency communications a sham, and compromises not only the employee, management, and the Code of Ethics, but also the Constitutional function of congressional oversight itself."[1748]

Enacting statutory rights for whistleblowers and establishing new executive agencies to protect those rights has not produced the protections that some expected. As explained in this report, the Office of Special Counsel, the Merit Systems Protection Board, and the Federal Circuit——the agencies created by Congress to safeguard the rights of whistleblowers——have not in many cases provided the anticipated protections to federal employees. National security whistleblowers were exempted from the Civil Service Reform Act of 1978 and the Whistleblower Protection Act of 1989. Some protections are available in statutes passed in recent years, including the Intelligence Community Whistleblower Protection Act of 1998. Individual Members and congressional committees have attempted to provide long-term protections to whistleblowers, enabling them to provide the kinds of agency information that Congress wants without costs and injuries to their government careers.

The purpose of this report is to explore the statutory and political protections available to national security whistleblowers. First, an examination of the Civil Service Reform Act and the Whistleblower Protection Act will explain why national security whistleblowers were excluded from the protections provided in those statutes. Second, to the extent that those statutes are considered models to protect national security whistleblowers, the experience of the Office of Special Counsel, the Merit Systems Protection Board, and the Federal Circuit is relevant in evaluating protections for national security whistleblowers.

Whistleblower activity is often viewed as a struggle between the executive and legislative branches. Presidents may decide to centralize control of agency information by requiring the agency head to approve the release of any information. Members of Congress regularly express a need to obtain information from employees within the agency, without seeking the approval of the agency head. This conflict between the branches is seen in the issuance of executive orders by Presidents Theodore Roosevelt and William Howard Taft in 1902 and 1909 and the resulting legislation——the Lloyd-LaFollette Act of 1912——adopted by Congress to maintain access to agency information. The

---

[1747] The Whistleblowers: A Report on Federal Employees Who Disclose Acts of Governmental Waste, Abuse, and Corruption, prepared for the Senate Committee on Governmental Affairs, 95th Cong., 2nd sess. 1 (Comm. Print, Feb. 1978).

[1748] Id. at 49.

constitutionality of the Lloyd-LaFollette Act continues to be challenged today by the Justice Department.

"Gag Orders" and Lloyd-LaFollette

Both Presidents Theodore Roosevelt and William Howard Taft threatened to fire agency employees who attempted to contact Congress. Employees were ordered to communicate only through the head of their agency. Congress responded by passing legislation intended to nullify that policy and allow employees to contact lawmakers, committees, and legislative staff.

The "Gag Orders"

President Theodore Roosevelt issued an order in 1902 to prohibit employees of executive departments from seeking to influence legislation "individually or through associations" except through the heads of the departments. Failure to abide by this presidential order could result in dismissal from federal service. The order read:

> *All officers and employees of the United States of every description, serving in or under any of the executive departments or independent Government establishments, and whether so serving in or out of Washington, are hereby forbidden, either directly or indirectly, individually or through associations, to solicit an increase of pay or to influence or attempt to influence in their own interest any other legislation whatever, either before Congress or its committees, or in any way save through the heads of the departments or independent Government establishments in or under which they serve, on penalty of dismissal from the Government service.*[1749]

In 1909, President William Howard Taft prepared a similar order, this one forbidding any bureau chief or any subordinate in an agency from going directly to Congress concerning legislation, appropriations, or congressional action of any kind without the consent and knowledge of the department head. Here is the language:

> *It is hereby ordered that no bureau, office, or division chief, or subordinate in any department of the Government, and no officer of the Army or Navy or Marine Corps stationed in Washington, shall apply to either House of Congress, or to any committee of either House of Congress, or to any Member of Congress, for legislation, or for appropriations, or for congressional action of any kind, except with the consent and knowledge of the head of the*

[1749] 48 Cong. Rec. 4513 (1912).

department; nor shall any such person respond to any request for information from either House of Congress, or any committee of either House of Congress, or any Member of Congress, except through, or as authorized by, the head of his department.[1750]

Lloyd-LaFollette Act

Through language added to an appropriations bill in 1912, Congress rejected these presidential orders. Congressional debate emphasized the concerns of lawmakers that the orders, left unchecked, would put congressional committees in the position of hearing "only one side of a case": the views of Cabinet officials. Lawmakers wanted to hear from the rank-and-file members of a department, who could disclose what departments did not want communicated. Some Members of Congress argued that they would not place the welfare of citizens "in the hands and at the mercy of the whims of any single individual, whether he is a Cabinet officer or anyone else."[1751] They insisted on access to agency employees and their complaints and observations about the conduct of their supervisors.[1752] Legislative language was drafted to ensure that agency employees could exercise their constitutional rights to free speech, to peaceable assembly, and to petition the government for redress of grievances.[1753]

During House debate, some legislators objected to the presidential orders as an effort by Presidents to prevent Congress "from learning the actual conditions that surrounded the employees of the service."[1754] If agency employees were required to speak only through the heads of the departments, "there is no possible way of obtaining information excepting through the Cabinet officers, and if these officials desire to withhold information and suppress the truth or to conceal their official acts it is within their power to do so."[1755] If no agency employee was allowed to speak directly to Congress and could communicate only through the department and eventually the Cabinet officer, "then this is an aristocratic Government, dominated completely by the official family of the President."[1756] Another legislator remarked: "The vast army of Government employees have

---

[1750] Id.

[1751] Id. at 4657 (statement of Rep. Reilly).

[1752] Id.

[1753] Id. at 5201 (statement of Rep. Prouty).

[1754] Id. at 5235 (statement of Rep. Buchanan).

[1755] Id. at 5634 (statement of Rep. Lloyd).

[1756] Id.

signed no agreement upon entering the service of the Government to give up the boasted liberty of the American citizens."[1757]

Those themes also emerged during Senate debate. One Senator said "it will not do for Congress to permit the executive branch of this Government to deny to it the sources of information which ought to be free and open to it, and such an order as this, it seems to me, belongs in some other country than the United States."[1758] The language used to counter the presidential orders was added as Section 6 to the Postal Service Appropriations Act of 1912.[1759] Section 6, known as the Lloyd-LaFollette Act, provides for procedural safeguards to protect agency officials from arbitrary dismissals when they attempt to communicate with Congress. The final sentence of Section 6 reads: "The right of persons employed in the civil service of the United States, either individually or collectively, to petition Congress, or any Member thereof, or to furnish information to either House of Congress, or to any committee or member thereof, shall not be denied or interfered with."

Section 6 was later carried forward and supplemented by the Civil Service Reform Act of 1978 and is codified as permanent law.[1760] The conference report on the 1978 statute explained why Congress depends on agency employees to disclose information directly to the legislative branch. The Civil Service Reform Act placed limitations on the kinds of information an employee may publicly disclose without suffering reprisal, but the conference report stated that there was "no intent to limit the information an employee may provide to Congress or to authorize reprisal against an employee for providing information to Congress." Nothing in the statute was to be construed "as limiting in any way the rights of employees to communicate with or testify before Congress."[1761]

As codified in 1978, the "right of employees, individually or collectively," to petition Congress becomes an enforceable right, and other prohibited personnel practices are identified.[1762] The U.S. Code now provides that various qualifications to the provision on prohibited personnel practices "shall not be

---

[1757] Id. at 5637 (statement of Rep. Wilson).

[1758] Id. at 10674 (statement of Sen. Reed).

[1759] 37 Stat. 555, § 6 (1912).

[1760] 5 U.S.C. § 7211 (2000).

[1761] S.Rept. No. 95-1272, 95th Cong., 2nd sess. 132 (1978).

[1762] 92 Stat. 1216-17, § 703(a)(2) (1978). The section on prohibited personnel practices provides: "This subsection shall not be construed to authorize the withholding of information from the Congress or the taking of any personnel action against an employee who discloses information to the Congress." Id. at 1117.

construed to authorize the withholding of information from the Congress or the taking of any personnel action against an employee who discloses information to the Congress."[1763]

Civil Service Reform Act of 1978

Congress passed legislation in 1978 to abolish the Civil Service Commission and create such new institutions as the Office of Personnel Management (OPM), the Merits Systems Protection Board (MSPB), and the Office of Special Counsel (OSC). The statute was the first to establish procedural protections for whistleblowers, but also recognized an exception for the national security area. Because of conflicting values in the legislation, however, whistleblowers never received the anticipated protections, and Congress took note of that a decade later when it passed the Whistleblower Protection Act of 1989.[1764] This record is examined in subsequent sections on "Whistleblower Protections in Practice" and "Congressional Action, 1986-88." As explained in this report, the statutory safeguards in the Whistleblower Protection Act did not meet the expectations of some lawmakers, agency employees, and private organizations.

Whistleblowers

The Civil Service Reform Act included the following as one of nine merit systems principles: "Employees should be protected against reprisal for the lawful disclosure of information which the employees reasonably believe evidences (A) a violation of any law, rule, or regulation, or (B) mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety."[1765]

The Senate Committee on Governmental Affairs, in reporting the bill, remarked that "Often, the whistle blower's reward for dedication to the highest moral principles is harassment and abuse. Whistle blowers frequently encounter severe damage to their careers and substantial economic loss." Protecting these employees who disclose government illegality, waste, and corruption "is a major step toward a more effective civil service. . . . What is needed is a means to assure them that they will not suffer if they help uncover and correct administrative abuses."[1766] The House Committee on Post Office and Civil Service, in its report, said that the bill "prohibits reprisals against employees who divulge information to the press or the public (generally known as "whistleblowers") regarding violations of law, agency mismanagement, or dangers to the public's health and

---

[1763] 5 U.S.C. § 2302(b) (sentence following para. 12) (2000).

[1764] 103 Stat. 16, § 2 (1989).

[1765] 92 Stat. 1114, § 2301(b)(9) (1978).

[1766] S.Rept. No. 95-969, 95th Cong., 2nd sess. 8 (1978).

safety."[1767] The House committee therefore anticipated that the whistleblower could report on wrongdoing not only through agency channels but also to the press and the public. In supplemental views in this committee report, Representative Pat Schroeder linked whistleblower protection to the needs of legislative oversight: "If we in Congress are going to act as effective checks on excesses in the executive branch, we have to hear about such matters."[1768]

During floor debate, Senator Jim Sasser stated that "patriotic employees who bring examples of official wrongdoing to the public's attention have, in the past, enjoyed no meaningful protection against reprisals by their supervisors." He referred to "too many" examples of federal employees finding themselves "fired, transferred, or deprived of meaningful work simply because they were brave enough to place the public interest ahead of their own personal career interest." He saw no reason why an employee "should have to risk his career and his family's financial stability for performing a public service."[1769]

Special Counsel

In recommending the Civil Service Reform Act, President Jimmy Carter proposed an Office of Special Counsel "to investigate merit violations and to protect the so-called whistleblowers who expose gross management errors and abuses."[1770] At a news conference, he looked to the Special Counsel to protect "those who are legitimate whistleblowers and who do point out violations of ethics, or those who through serious error hurt our country."[1771] The House Committee on Post Office and Civil Service, in reporting the bill, said that the Special Counsel "will have broad authority to investigate, particularly 'whistleblower' cases."[1772]

The statute looked to the Special Counsel to protect the interests of whistleblowers. The Special Counsel, appointed to a term of five years with the advice and consent of the Senate, was directed to "investigate allegations involving prohibited personnel practices and reprisals against Federal employees

---

[1767] H.Rept. No. 95-1403, 95th Cong., 2nd sess. 4 (1978).

[1768] Id. at 387.

[1769] 124 Cong. Rec. 27548 (1978).

[1770] Public Papers of the Presidents, 1978, I, at 437.

[1771] Id. at 441.

[1772] H.Rept. No. 95-1403, 95th Cong., 2nd sess. 4-5 (1978).

for the lawful disclosure of certain information and may file complaints against agency officials and employees who engage in such conduct."[1773]

National Security Exception

As the Senate Committee on Governmental Affairs explained in reporting the Civil Service Reform Act, it was not intended to protect whistleblowers "who disclose information which is classified or prohibited by statute from disclosure."[1774] It was the committee's understanding that "section 102(d)(3) of the National Security Act of 1947, which authorizes protection of national intelligence sources and methods, has been held to be such a statute."[1775]

The section on prohibited personnel practices in the Civil Service Reform Act covered all executive agencies but did not include "the Federal Bureau of Investigation [FBI], the Central Intelligence Agency [CIA], the Defense Intelligence Agency [DIA], the National Security Agency [NSA], and, as determined by the President, any Executive agency or unit thereof the principal function of which is the conduct of foreign intelligence or counterintelligence activities."[1776]

Prohibited personnel practices in the FBI were treated in another section of the statute.[1777] During House debate, Representative Pat Schroeder argued that the FBI whistleblower protections were "necessitated, in part, by the woeful history of this agency in terms of eliminating internal wrongdoing." She stated that an FBI employee "is guaranteed protection if he or she follows the procedures set out." If the employee decided to make public disclosures of the wrongdoing, "this statute does not serve as authorization for the Bureau to take reprisals. The

---

[1773] 92 Stat. 1112, § 3(4).

[1774] S.Rept. No. 95-969, 95th Cong., 2nd sess. 8 (1978).

[1775] Id. at 21-22. Section 102(d)(3) of the National Security Act of 1947 provides: "For the purpose of coordinating the intelligence activities of the several Government departments and agencies in the interest of national security, it shall be the duty of the [Central Intelligence] Agency, under the direction of the National Security Council . . . to correlate and evaluate intelligence relating to the national security, and provide for the appropriate dissemination of such intelligence within the Government using where appropriate existing agencies and facilities: Provided, That the Agency shall have no police, subpena [sic], law-enforcement powers, or internal-security functions: Provided further, That the departments and other agencies of the Government shall continue to collect, evaluate, correlate, and disseminate departmental intelligence: And provided further, That the Director of Central Intelligence shall be responsible for protecting intelligence sources and methods from unauthorized disclosure." 61 Stat. 498.

[1776] 92 Stat. 1115, § 2302(a)(2)(C)(ii) (1978).

[1777] Id. at 1117, § 2302.

general policy of protecting whistleblowers runs to all Government instrumentalities."[1778]

Such intelligence agencies as the CIA and the DIA were not specifically covered by the Civil Service Reform Act. Moreover, a subsection on actions to be taken by authorized supervisory employees referred to the special category of confidential or secret information. Supervisors were prohibited from taking or failing to take a personnel action with respect to any employee or applicant for employment as a reprisal for a disclosure of information by an employee or applicant which they reasonably believed evidences (1) a violation of any law, rule, or regulation, or (2) mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety "if such disclosure is not specifically prohibited by law and if such information is not specifically required by Executive order to be kept secret in the interest of national defense or the conduct of foreign affairs."[1779] The language recognized the President's authority to designate certain information as confidential or secret, excluding national security whistleblowers from automatic protection. However, Representative Schroeder argued that the Civil Service Reform Act "applies the merit system principles to all units of the Federal Government," and that "while specific enforcement provisions are not mandated for agencies like CIA and GAO, the legislation makes it clear that whistleblowers should be protected in these agencies."[1780]

In the event the Special Counsel received from an agency employee foreign intelligence or counterintelligence information, "the disclosure of which is specifically prohibited by law or by Executive order," the statute directed the Special Counsel to transmit that information to the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence.[1781] The Special Counsel was directed to make available to the public a list of noncriminal matters referred to agency heads, but "shall take steps to ensure that any such public list does not contain any information the disclosure of which is prohibited by law or by Executive order requiring that information be kept secret in the interest of national defense or the conduct of foreign affairs."[1782]

Communications with Congress

[1778] 124 Cong. Rec. 34100 (1978).

[1779] 92 Stat. 1116, § 2302(b)(8).

[1780] 124 Cong. Rec. 34100 (1978).

[1781] 92 Stat. 1127, § 1206(b)(9).

[1782] 92 Stat. 1128, § 1206(d).

The Senate Committee on Governmental Affairs added to the bill a provision to ensure that nothing in the section on prohibited personnel practices "will authorize the withholding of any information from Congress, or will sanction any personnel action against an employee who discloses any information to a Member of Congress or its staff, either in public session or through private communications." Moreover, nothing in the bill was to be construed "as limiting in any way the rights of employees to communicate with or testify before Congress, such as is provided in 5 U.S.C. 7102 (right to furnish information protected), or in 18 U.S.C. 1505 (right to testify protected)."[1783]

The conference report, in adopting the Senate provision, explained that it "is intended to make clear that by placing limitations on the kinds of information any employee may publicly disclose without suffering reprisal, there is no intent to limit the information an employee may provide to Congress or to authorize reprisal against an employee for providing information to Congress." As further explanation:

> *For example, 18 U.S.C. 1905 prohibits public disclosure of information involving trade secrets. That statute does not apply to transmittal of such information by an agency to Congress. Section 2302(b)(8) of this act would not protect an employee against reprisal for public disclosure of such statutorily protected information, but it is not to be inferred that an employee is similarly unprotected if such disclosure is made to the appropriate unit of the Congress. Neither title I nor any other provision of the act should be construed as limiting in any way the rights of employees to communicate with or testify before Congress.*[1784]

As enacted, the subsection of prohibited personnel practices states that it "shall not be construed to authorize the withholding of information from the Congress or the taking of any personnel action against an employee who discloses information to the Congress."[1785]

Inspectors General

In the same year that Congress passed the Civil Service Reform Act, it completed action on legislation to establish offices of inspectors general in twelve executive agencies. More inspectors general would be created in subsequent statutes. The purpose was to create independent offices "to conduct and supervise audits and

---

[1783] S.Rept. No. 95-969, 95th Cong., 2nd sess. 23 (1978).

[1784] S.Rept. No. 95-1273, 95th Cong., 2nd sess. 132 (1978). The same language appears in H.Rept. No. 95-1717, 95th Cong., 2nd sess. 132 (1978) (conference report).

[1785] 92 Stat. 1117 (1978).

investigations relating to programs and operations" in these agencies.[1786] These offices were expected "to prevent and detect fraud and abuse in, such programs and operations."[1787]

Inspectors general were authorized to receive and investigate complaints or information received from agency employees concerning the "possible existence of an activity constituting a violation of law, rules, or regulations, or mismanagement, gross waste of funds, abuse of authority or a substantial and specific danger to the public health and safety."[1788] Supervisors were prohibited from taking or threatening to take "any action against any employee as a reprisal for making a complaint or disclosing information to an inspector general, unless the complaint was made or the information disclosed with the knowledge that it was false or with willful disregard for its truth or falsity."[1789]

In reporting the section on employee complaints, the Senate Committee on Governmental Affairs remarked: "Because of the employee's position within the agency, employee complaints carry with them a high likelihood of reliability." Given the difficulty of "blowing the whistle" on one's supervisors or colleagues, "the situation may often be serious." The committee believed that "most employees would much prefer an effective channel inside the agency to pursue complaints rather than seeking recourse or publicity outside the agency. This preference should be encouraged."[1790]

The legislative history of the Civil Service Reform Act anticipated that federal agency whistleblowers would report wrongdoing not only to their supervisors but to Congress, the public, and the press. In contrast, the inspectors general statute of 1978 authorized a set of procedures that were entirely in-house. The IGs were directed to keep Congress "fully and currently informed about problems and deficiencies relating to the administration of such programs and operations and the necessity for and progress of corrective action."[1791] Inspectors general would furnish semiannual reports to agency heads, who would transmit the reports without change to appropriate committees and subcommittees of Congress.[1792]

[1786] 92 Stat. 1101, § 2(1) (1978).

[1787] Id. at § 2(2)(b).

[1788] Id. at § 7(a).

[1789] Id. at § 7(c).

[1790] S.Rept. No. 95-1071, 95th Cong., 2nd sess. 35-36 (1978).

[1791] 92 Stat. 1101, at § 2(3).

[1792] Id. at 1103, § 5(b).

Defense Department IG

In 1982, Congress created an inspector general in the Defense Department, authorized to direct audits and investigations that require access to information concerning (1) sensitive operational plans, (2) intelligence matters, (3) counterintelligence matters, (4) ongoing criminal investigations by other administrative units of the Defense Department related to national security, and (5) "other matters the disclosure of which would constitute a serious threat to national security."[1793] The IG would serve as the principal adviser to the Secretary of Defense "for matters relating to the prevention and detection of fraud, waste, and abuse in the programs and operations of the Department."[1794]

The IG statute provided that nothing in the section "shall be construed to authorize the public disclosure of information which is (A) specifically prohibited from disclosure by any other provision of law; (B) specifically required by Executive order to be protected from disclosure in the interest of national defense or national security or in the conduct of foreign affairs; or (C) a part of an ongoing criminal investigation." However, nothing in that section or in any other provision of the statute "shall be construed to authorize or permit the withholding of information from the Congress, or from any committee or subcommittee thereof."[1795]

A Statutory IG for the CIA

The Central Intelligence Agency had an Office of Inspector General, but it was not statutory. Beginning in 1952, the CIA administratively established the position of IG.[1796] The limitations of that office were underscored by the Iran-Contra affair, which became public in November 1986 and highlighted the extent to which the CIA and other executive agencies had failed to comply with statutory restrictions and had not testified fully and accurately to congressional committees about covert operations.[1797] One of the recommendations by the House and Senate Iran-Contra Committees in November 1987 was the creation of an independent statutory IG confirmed by the Senate. The committees concluded that the existing

---

[1793] 96 Stat. 751, § 8(b)(1) (1982).

[1794] Id., § 8 (c)(1).

[1795] Id. at 752-53.

[1796] CRS Report 89-129 GOV, Office of Inspector General in the Central Intelligence Agency: Development and Proposals, by Frederick M. Kaiser, February 27, 1989.

[1797] Report of the Congressional Committee Investigating the Iran-Contra Affair, H.Rept. No. 100-433 and S.Rept. No. 100-216, 100th Cong., 2nd sess. (1987).

Office of Inspector General in the CIA "appears not to have had the manpower, resources or tenacity to acquire key facts uncovered by other investigations."[1798]

During hearings on March 1, 1988, by the Senate Intelligence Committee, Senator Arlen Specter reviewed some of the misleading testimony that Congress had received about the Iran-Contra affair, including testimony from the CIA.[1799] The next year, Congress established an inspector general for the CIA, "appropriately accountable to Congress" and designed to "promote economy, efficiency, and effectiveness in the administration of such programs and operations, and detect fraud and abuse in such programs and operations."[1800] The IG would provide a means of keeping the Director of the CIA "fully and currently informed about problems and deficiencies relating to the administration of such programs and operations, and the necessity for and the progress of corrective action," and would ensure that the House and Senate Intelligence Committees "are kept similarly informed of significant problems and deficiencies as well as the necessity for and the progress of corrective actions."[1801]

The IG reports directly to and is under the general supervision of the director, who may prohibit the IG "from initiating, carrying out, or completing any audit, inspection, or investigation if the Director determines that such prohibition is necessary to protect vital national security interests of the United States." In exercising that power, the director shall submit "an appropriately classified statement of the reasons for the exercise of such power within seven days to the intelligence committees."[1802]

The creation of the IG also included a whistleblower provision. The IG would receive and investigate "complaints or information from an employee of the Agency concerning the existence of an activity constituting a violation of laws, rules, or regulations, or mismanagement, gross waste of funds, abuse of authority, or a substantial and specific danger to the public health and safety." No action constituting a reprisal, or threat of reprisal, for making such complaint may be taken by any Agency employee in a position to take such actions, "unless the complaint was made or the information was disclosed with the knowledge that it was false or with willful disregard for its truth or falsity."[1803] Additional

---

[1798] Id. at 425.

[1799] "S. 1818——To Establish an Independent Inspector General," Hearings before the Senate Select Committee on Intelligence, 100th Cong., 2nd sess. 53-54 (1988).

[1800] 103 Stat. 1711, § 801 (1989).

[1801] Id. at 1711-12.

[1802] Id. at 1712 (paragraphs (b)(3) and (4)).

[1803] Id. at 1714 (paragraph (e)(3)).

procedures for CIA whistleblowing would be enacted in 1998, discussed later in the report.

Creating the Federal Circuit

Under the Civil Service Reform Act, any employee or applicant for employment adversely affected or aggrieved by a final order or decision of the MSPB could obtain judicial review in any of the federal appellate courts.[1804] In 1982, Congress created a new appellate court by consolidating the existing U.S. Court of Customs and Patent Appeals with the appellate division of the existing U.S. Court of Claims. Congress gave the new U.S. Court of Appeals for the Federal Circuit exclusive jurisdiction over any final order or final decision of the MSPB.[1805]

Whistleblower Protections in Practice

For a number of reasons, the whistleblower protections promised in the Civil Service Reform Act failed to materialize. In signing the bill, President Carter said that "it prevents discouraging or punishing [federal employees] for the wrong reasons, for whistleblowing or for personal whim in violation of basic employee rights."[1806] At the signing ceremony, Representative Morris Udall, who managed the bill on the House side, cautioned that "reform has consequences that you don't like sometimes, but the best reforms aren't going to work unless people make them work."[1807]

Competing Priorities

Part of the gap between promise and practice with regard to whistleblower protections resulted from the complex and in some ways conflicting values placed in the statute. Although it expressly stated its intention to protect whistleblowers, a dominant purpose behind the statute was to make it easier to hold federal employees accountable for their performance. In announcing the Administration's civil service reform proposals, President Carter noted "a widespread criticism of Federal Government performance. The public suspects that there are too many Government workers, that they are underworked, overpaid, and insulated from the consequences of incompetence."[1808] Although he immediately dismissed such "sweeping criticisms" as "unfair," much of the impetus behind civil service reform was driven by the belief that managers needed greater discretion in demoting and removing under-performing

---

[1804] 92 Stat. 1143, § 7703(b) (1978).

[1805] 96 Stat. 38, § 127(a)(9) (1982).

[1806] Public Papers of the Presidents, 1978, I, at 1761.

[1807] Id. at 1762.

[1808] Public Papers of the Presidents, 1978, I, at 436.

employees. In this same address, President Carter referred to the "sad fact" that it is "easier to promote and to transfer incompetent employees than it is to get rid of them."[1809]

Making it Easier to Punish

In reporting the bill, the Senate Committee on Governmental Affairs referred to conditions in federal agencies that made them "too often . . . the refuge of the incompetent employee."[1810] An employee "has no right to be incompetent."[1811] One of the "central tasks" of the bill was "simple to express but difficult to achieve: Allow civil servants to be able to be hired and fired more easily, but for the right reasons."[1812]

Senator Abraham Ribicoff, chairman of the committee that reported the bill, listed two purposes of the legislation without indicating any tension between them. The bill provided "new protection for whistleblowers who disclose illegal or improper Government conduct" while at the same time it "streamline[d] the processes for dismissing and disciplining Federal employees."[1813] He explained that the bill "lowered the standard of evidence needed to uphold the dismissal of an employee who has been fired for poor performance." Instead of a supervisor proving by a "preponderance of evidence" that an employee's performance had not been "up to par," the conferees adopted the "substantial evidence" test to give supervisors greater deference in assessing the work of an employee.[1814] Ironically, if a supervisor found a whistleblower's charges to reflect on poor management within the agency, or if a whistleblower threatened to release information embarrassing to the supervisor, it might now be easier to sanction or remove the whistleblower.

1985 House Hearings

One of the early statements by President Ronald Reagan urged whistleblowers to come forward: "Federal employees or private citizens who wish to report incidents of illegal or wasteful activities are not only encouraged to do so but will be guaranteed confidentiality and protected against reprisals." The "vital

---

[1809] Id.

[1810] S.Rept. No. 95-969, 95th Cong., 2nd sess. 3 (1978).

[1811] Id. at 4.

[1812] Id.

[1813] 124 Cong. Rec. 33388-89 (1978).

[1814] Id. For the "substantial evidence" test in the Civil Service Reform Act, see 92 Stat. 1138, § 7701 (c)(1)(A).

element" in fighting fraud and waste "is the willingness of employees to come forward when they see this sort of activity." Employees "must be assured that when they 'blow the whistle' they will be protected and their information properly investigated." He wanted to make it clear that "this administration is providing that assurance to every potential whistleblower in the Federal Government."[1815]

As presiding officer of House hearings on June 26, 1985, Representative Pat Schroeder heard contrary testimony from a variety of government officials, federal employees, and private organizations on the implementation of the whistleblower provisions in the Civil Service Reform Act. She concluded: "There is no dispute ——whistleblowers have no protection. We urge them to come forward, we hail them as the salvation of our budget trauma, and we promise them their place in heaven. But we let them be eaten alive."[1816] Much of the focus of the hearings fell on the performance of the Special Counsel.

Office of the Special Counsel

K. William O'Connor, Special Counsel of the MSPB, testified that his office "has only one client; it is the enforcement of the merit systems and the laws that carry it into effect."[1817] The commitment to protect "bona fide whistleblowers" would be done by "protection of the merit systems, the means designed by Congress to that end and the end that the OSC is charged with effecting."[1818] Federal employees who bring charges of agency wrongdoing "are not the clients of this office; the system is."[1819] Although some witnesses from the Schroeder subcommittee argued that the OSC was principally established to "protect whistleblowers," O'Connor testified that "protection of whistleblowers——even the word whistleblower——does not appear in the code at all. What is required by the statute is the protection of the Merit System . . . ."[1820]

Elsewhere O'Connor recognized the duties of his office with whistleblowers. In identifying the three primary statutory functions of the OSC, he listed this one first: "To provide a secure channel through which disclosures of waste, fraud, inefficiency or hazards to public health or safety may be received and referred

---

[1815] Public Papers of the Presidents, 1981, at 360.

[1816] "Whistleblower Protection," hearings before the House Committee on Post Office and Civil Service, 99th Cong., 1st sess. 237 (1985).

[1817] Id. at 238.

[1818] Id. at 239.

[1819] Id. at 240.

[1820] Id. at 243.

while providing anonymity to the discloser."[1821] He also described a number of recent improvements in the operations of OSC, including "[a]n effective outreach program . . . developed and maintained to apprise whistleblowers of the responsibilities of and protection afforded by this office."[1822] He pledged to "continue to use the statutory powers of this office to protect bona fide whistleblowers from prohibited retaliation for their protected disclosures by enforcing the law. That is, by prosecuting anyone who takes reprisal against them because of their protected disclosures, and by invoking appropriate agency corrective actions."[1823]

O'Connor described how he would handle an employee who had been sanctioned by an agency, even though the employee had been involved in protected whistleblower activities:

> *If an agency sanction was proper because of an employee's incompetence or misconduct, even though the motivation of the deciding or proposing official was contaminated by a de minimus vindictiveness or desire for retaliation and reprisal for protected conduct, the sanction against the employee will probably stand. The reprisal oriented official, however, may be prosecuted by my office and may be disciplined by the Board if the improper motivation of the conduct is not de minimus. This, it seems to me, is a proper and worthy result.*
>
> *It is not in the public interest to employ, retain or cosset drones, incompetents, disruptors of the workplace, malefactors, or those whose conduct is in other unlawful ways inappropriate to the execution of the mission of the organization, even though the person is also an individual who has engaged in specifically protected conduct like whistleblowing. The public interest is, after all, the execution of the public business; it is not a maintenance program for the incompetent, nor is it in the public interest to foster internal dissidence, vituperation, backbiting and disaffection.*[1824]

Representative Schroeder referred to some 11,000 federal employees who had contacted the Office of Special Counsel for relief. O'Connor acknowledged that these individuals had a complaint and thought they had a case, but added: "there

---

[1821] Id.

[1822] Id. at 244.

[1823] Id. at 252.

[1824] Id. at 250.

are many people who feel that they have complaints, and some of them are carrying bags and walking up and down Constitution Avenue right now, I have no doubt."[1825] When Representative Schroeder pointed out that the women carrying bags up and down the avenue are not on the federal payroll, O'Connor agreed. The point he wanted to make, he said, was that few of the 11,000 complaints were within the scope of responsibilities handled by his office.[1826]

Earlier O'Connor had offered his "firm belief" that most federal managers follow the law and have integrity, whereas "most whistleblowers are malcontents."[1827] In a newspaper article published on July 17, 1984, O'Connor was asked what advice he would give, as a private attorney, to a potential whistleblower. His reply: "I'd say that unless you're in a position to retire or are independently wealthy, don't do it. Don't put your head up, because it will get blown off."[1828]

Congressional Action, 1986-88

On February 20 and 21, 1986, a subcommittee of the House Post Office and Civil Service Committee held additional hearings on whistleblower protections. The testimony showed a wide gap between the perceptions of lawmakers and executive officials. As chair of the subcommittee, Representative Schroeder spoke of a "general consensus" that the whistleblower protections in the Civil Service Reform Act "must be changed if we are to treat Federal employees fairly and provide relief for victims of prohibited personnel practices."[1829] Special Counsel O'Connor testified against the need to pass a bill, introduced in the House, designed to strengthen whistleblower protections: "The bill is flawed conceptually, as well, from inception, for it proceeds upon the false premise that proper law enforcement systems now in effect do not work to protect bona fide whistleblowers. The fact is that, now, the statutory protection works. I oppose the bill."[1830] Stuart E. Schiffer, Deputy Assistant Attorney General, also testified against the bill. When asked whether he believed the existing statutory system was adequate, he replied: "Yes; I do." Asked again whether there was adequate protection for whistleblowers, he again answered: "Yes; I do."[1831]

[1825] Id. at 253.

[1826] Id. at 254.

[1827] Id. at 259.

[1828] Howard Kurtz, "Whistlin' the Blues," Washington Post, July 17, 1984, at A17.

[1829] "Whistleblower Protection Act of 1986," hearings before the Subcommittee on Civil Service of the House Committee on Post Office and Civil Service, 99th Cong., 2nd sess. 1 (1986).

[1830] Id. at 74 (emphasis in original).

[1831] Id. at 99.

Proposed Legislation in 1986

The House Post Office and Civil Service Committee reported a whistleblower protection act on September 22, 1986. The purpose was to "strengthen and improve protections for the rights of Federal employees by clarifying the role of the Office of Special Counsel (OSC) and emphasizing that its primary responsibility is to represent individuals who are victims of prohibited personnel practices; by providing Federal employees with a private right of action as an alternative to pursuing cases through the OSC; by permitting the Special Counsel to seek judicial review of MSPB decisions to which the Special Counsel was a party; by protecting the identity of Federal employees who make disclosures; by lessening the standard of proof needed to prove reprisal in the case of whistleblower disclosures;" and other objectives.[1832] The House Subcommittee on Civil Service had been "unable to find a single individual who has gone to the Office of Special Counsel since 1981 who has been satisfied with the investigation of his or her case."[1833]

Action in 1988

Congress did not act on the 1986 legislation, but the House Committee on Post Office and Civil Service reported the bill again in the 100th Congress. The report referred to the results of a study by Dr. Donald R. Soeken who concluded that "most whistleblowers were not protected, and in fact, they suffered cruel and disastrous retaliation for their efforts. . . . It seems to me that the protection has also been a cruel hoax. We ask people to act out of conscience and then we ignore their cries for protection. We allow their careers to be destroyed and watch as the lives of the whistleblowers and their families suffer under the strain."[1834] Mary Lawton, Special Counsel in 1987, testified that "to the extent that there may have been a lack of emphasis on the corrective action authority of the [OSC] office, I have called for an emphasis."[1835]

The Senate Committee on Governmental Affairs reported whistleblower protection legislation on July 6, 1988.[1836] The committee described the results of a 1984 report prepared by the MSPB, "Blowing the Whistle in the Federal Government." It estimated that a large percentage of federal employees (69-70 percent) knew of fraud, waste and abuse but chose not to report it. Moreover, the percentage of employees who did not report government wrongdoing because of

---

[1832] H.Rept. No. 99-859, 99th Cong., 2nd sess. 13 (1986).

[1833] Id. at 19.

[1834] H.Rept. No. 100-274, 100th Cong., 1st sess. 19 (1987).

[1835] Id. at 22.

[1836] S.Rept. No. 100-413, 100th Cong., 2nd sess. (1988).

fear of reprisal rose from an estimated 20 percent in 1980 to 37 percent in 1983.[1837]

In reviewing the board's report, the committee agreed that "statutory protections, alone, cannot guarantee the elimination of reprisal among civil servants. Agency heads and supervisors must foster an environment where employees are encouraged to come forward with suggestions and report problems and are appropriately rewarded, rather than punished, for doing so." The statistics included in the board's report "show that Congress' specific statutory efforts to protect whistleblowers thus far have had no observable impact on encouraging federal employees to blow the whistle."[1838]

The Mt. Healthy Test

The committee explained why whistleblowers were vulnerable to reprisal. Even if an employee was successful in proving a connection between a whistleblowing activity and a reprisal, the agency had an opportunity to show that it would have taken the personnel action even if the employee had not engaged in protected conduct. This type of agency defense had been developed by the Supreme Court in Mt. Healthy City School District Board of Education v. Doyle, 429 U.S. 274 (1977) and later had been applied by the MSPB and the courts in reprisal cases. The committee found that the Mt. Healthy test allowed an agency "to search an employee's work record for conduct that can be cited as the reason for taking an adverse action. It has proved to be difficult for employees to refute the agency's contention that it would have taken the personnel action anyway."[1839]

To overcome this problem, the committee proposed that the Mt. Healthy test be modified only for whistleblower reprisal cases. Once an employee had made a prima facie case of reprisal by showing that whistleblowing was a factor in a personnel action, the agency would be required to show by "clear and convincing evidence" that the whistleblowing was not a "material factor" in the personnel action. "Clear and convincing evidence" is less than the criminal standard of "beyond a reasonable doubt" but higher than "preponderance of the evidence," which was the current standard for this type of employee case.[1840]

The Whistleblowing Protection Act of 1988 passed the Senate and the House. Section 2(b) of the Senate bill stated the "primary role" of the OSC was to "protect employees, especially whistleblowers, from prohibited personnel practices," and

---

[1837] Id. at 5.

[1838] Id. at 6.

[1839] Id. at 14.

[1840] Id. at 15.

that the OSC "shall act in the interests of employees who seek assistance from the [OSC] and not contrary to such interests."[1841] The bill passed the Senate by voice vote on August 2, 1988.[1842] The House took up the Senate bill on October 3. Because the 100th Congress was about to end, the House skipped conference and worked out a compromise version of the bill with the Senate.[1843] A letter of October 3 to Representative Schroeder from Joseph R. Wright, Jr., Deputy Director of the Office of Management and Budget, indicated that the two branches were in agreement on the bill. There was no threat of a veto.[1844] The bill passed the House, 418 to zero.[1845] The Senate agreed to the House changes on October 7.[1846] Congress adjourned sine die on October 22.

Pocket Veto

President Reagan pocket vetoed the bill on October 26. He stated that reporting of "mismanagement and violations of the law, often called whistleblowing, contributes to efficient use of taxpayers' dollars and effective government. Such reporting is to be encouraged, and those who make the reports must be protected."[1847] However, he also said it was necessary to "ensure that heads of departments and agencies can manage their personnel effectively." It was his concern that the bill would have changed the law "so that employees who are not genuine whistleblowers could manipulate the process to their advantage simply to delay or avoid appropriate adverse personnel actions."[1848] He objected particularly to the "clear and convincing evidence" test, holding that it "essentially rigs the Board's process against agency personnel managers in favor of employees. The interests of both employees and managers should be fully protected."[1849]

[1841] 134 Cong. Rec. 19974 (1988).

[1842] Id. at 19983.

[1843] Id. at 27853.

[1844] Id. at 27855.

[1845] Id. at 28129.

[1846] Id. at 29544.

[1847] Public Papers of the Presidents, 1988-89, II, at 1391.

[1848] Id. at 1392.

[1849] Id.

The pocket veto memorandum also objected to restrictions placed on the power of the President to remove the Special Counsel.[1850] The Civil Service Reform Act provided that the Special Counsel "may be removed by the President only for inefficiency, neglect of duty, or malfeasance in office."[1851] Section 1211(b) of the bill passed by Congress in 1988 contained the same language.[1852]

President Reagan also objected to a provision that authorized the Special Counsel to obtain judicial review of most MSPB decisions in proceedings to which the Special Counsel was a party. Implementation of that provision "would place two Executive branch agencies before a Federal court to resolve a dispute between them. The litigation of intra-Executive branch disputes conflicts with the constitutional grant of the Executive power to the President, which includes the authority to supervise and resolve disputes between his subordinates."[1853]

Whistleblower Protection Act of 1989

The vetoed whistleblower bill was modified in 1989 and passed the Senate on March 16 by a vote of 97 to zero.[1854] The modified bill retained the language establishing that the "primary role" of the Special Counsel "is to protect employees, especially whistleblowers, from prohibited personnel practices," and provided that the OSC "shall act in the interests of employees who seek assistance" from the office.

The limitations on the President's power to remove the Special Counsel were retained, but no authority was granted to the Special Counsel to seek judicial review of an MSPB decision.

The "clear and convincing evidence" test remained. The bill modified the *Mt. Healthy* test to state that, "in cases involving allegations of reprisal for whistleblowing, an individual must prove that whistleblowing was a contributing factor in the agency's decision to take the action."[1855] The burden is then placed on the agency to prove by clear and convincing evidence that the same personnel action would have been taken in the absence of the protected disclosure. Also, for the first time, the bill gave whistleblowers the right to appeal their own cases to

---

[1850] Id.

[1851] 92 Stat. 1122, § 1204 (1978).

[1852] 134 Cong. Rec. 29537 (1988).

[1853] Public Papers of the Presidents, 1988-89, II, at 1392.

[1854] 135 Cong. Rec. 4535 (1989).

[1855] Id. at 5036 (statement of Rep. Horton).

the MSPB if the Special Counsel failed or refused to do so.[1856] The House passed the bill under suspension of the rules.[1857]

In the Whistleblower Protection Act (WPA) of 1989, Congress found that federal employees who make protected disclosures "serve the public interest by assisting in the elimination of fraud, waste, abuse, and unnecessary Government expenditures."[1858] Congress also found that protecting employees "who disclose Government illegality, waste, and corruption is a major step toward a more effective civil service." Moreover, the WPA stated that Congress, in passing the Civil Service Reform Act of 1978, "established the Office of Special Counsel to protect whistleblowers" who make protected disclosures.[1859] The WPA incorporates the exemptions for national security information included in the 1978 statute.[1860] In signing the WPA, President George H. W. Bush said that "a true whistleblower is a public servant of the highest order. . . . [T]hese dedicated men and women should not be fired or rebuked or suffer financially for their honesty and good judgment."[1861]

WPA Amendments in 1994

Congress passed legislation in 1994 to amend the Whistleblower Protection Act. Legislation was needed to reauthorize the Office of Special Counsel and to ensure that it functioned "as intended, to protect federal employee whistleblowers from on-the-job harassment, negative job ratings, unfavorable transfers, denial of promotions and other retaliation for their efforts to uncover waste and mismanagement in their agencies."[1862]

In reporting the legislation, the Senate Committee on Governmental Affairs expressed concern "about the extent to which OSC is aggressively acting to protect whistleblowers from prohibited personnel practices."[1863] On the House side, the Committee on Post Office and Civil Service stated that "while the Whistleblower Protection Act is the strongest free speech law that exists on paper, it has been a counterproductive disaster in practice. The WPA has created

---

[1856] Id. at 4508 (statement of Senator Levin).

[1857] Id. at 5040.

[1858] 103 Stat. 16, § 2(a)(1) (1989).

[1859] Id. at § 2(a)(2) and (3).

[1860] Id. at 23.

[1861] Public Papers of the Presidents, 1989, I, at 391.

[1862] S.Rept. No. 103-358, 103d Cong., 2nd sess. 1 (1994).

[1863] Id. at 3.

new reprisal victims at a far greater pace than it is protecting them."[1864] The House committee concluded that statutory mandates could easily be thwarted by a hostile agency climate: "There is little question that agency leadership is a far stronger factor than statutory provisions to establish a workplace environment of respect for the merit system."[1865]

MSPB and Federal Circuit

The House committee also found that the statistical record indicated that the MSPB and the Federal Circuit of Appeals "have not been favorable to Federal whistleblowers." In the first two years after enactment of the WPA, whistleblowers won approximately 20% of MSPB decisions on the merits. From FY1991 to FY1994, that rate dropped to 5%; instead of providing a balance, the Federal Circuit "has been more hostile than the Board. Since its 1982 creation, in reported decisions employees have prevailed only twice on the merits with the whistleblower defense." The committee said it had received "extensive testimony at hearings that the MSPB and the Federal Circuit have lost credibility with the practicing bar for civil service cases."[1866] In November 1993, GAO released a report indicating that 81 percent of federal employees who sought whistleblower reprisal protection from OSC gave the office a generally low to very low rating for overall effectiveness.[1867]

A more recent study indicates that whistleblowers continue to fare poorly in the MSPB and Federal Circuit. According to the Government Accountability Project, a nonprofit, whistleblower advocacy group, only two out of 30 whistleblowers prevailed on the merits before the MSPB from 1999 to 2005, and only one whistleblower claim out of 96 prevailed on the merits before the Federal Circuit from 1995 to 2005.[1868] Some, however, may view this as an indication that many whistleblowers present weak cases.

The Amendments

The 1994 legislation provided for reasonable attorney fees in certain cases if the federal employee or applicant for a federal job is the prevailing party and the MSPB or administrative law judge determines that payment by the agency "is in

---

[1864] H.Rept. No. 103-769, 103d Cong., 2nd sess. 12 (1994).

[1865] Id. at 13.

[1866] Id. at 17.

[1867] S.Rept. No. 103-358, 103d Cong., 2nd sess. 3 (1994). General Accounting Office, "Reasons for Whistleblower Complainants' Dissatisfaction Need to be Explored," Nov. 1993, GAO/GGD-94-21.

[1868] Project On Government Oversight, "Homeland and National Security Whistleblower Protections: The Unfinished Agenda," April 28, 2005, at 8.

the interest of justice."[1869] The statute required the Special Counsel, ten days before terminating an investigation of a prohibited personnel practice, to provide a written status report to the whistleblower of the proposed findings of fact and legal conclusions.[1870] The employee then has an opportunity to respond and provide additional supporting information. Through other provisions in the amendments, Congress attempted to even the field for legitimate whistleblowers.[1871]

Military Whistleblowers

During debate on the WPA, Representative Barbara Boxer said that Members of Congress "learned when we passed the Military Whistleblower Protection Act that without whistleblowers, frankly, we really could not do our job, because . . . we need information and we need a free flow of information from Federal employees, be they military or civilian."[1872] The Military Whistleblower Protection Act (10 U.S.C. § 1034) is not a single statute but rather an accumulation of several.

1956 Legislation

The first mention of Section 1034 was in 1956, with the codification of Title 10. Section 1034 provided: "No person may restrict any member of an armed force in communicating with a member of Congress, unless the communication is unlawful or violates a regulation necessary to the security of the United States."[1873] Congress adopted this language during a tense confrontation with the Eisenhower Administration over access to agency information. In 1954, President Eisenhower wrote a letter to Secretary of Defense Charles E. Wilson in which he prohibited testimony concerning certain conversations and communications between employees in the executive branch.[1874] Attorney General Herbert Brownnell, Jr. released a legal memorandum stating that the courts had "uniformly held that the President and the heads of departments have an uncontrolled discretion to withhold the information and papers in the public interest."[1875] The Justice Department prepared a 102-page brief concluding that Congress "cannot, under the Constitution, compel heads of departments to make

---

[1869] 108 Stat. 4361, § 2 (1994).

[1870] Id. at 4362.

[1871] For floor debate, see 140 Cong. Rec. 27357-61, 28823-26 (1994).

[1872] 135 Cong. Rec. 5037 (1989).

[1873] 70A Stat. 80 (1956).

[1874] CQ Almanac, 1956, at 737.

[1875] Id.

public what the President desires to keep secret in the public interest."[1876] Representative John Moss said the Justice Department analysis was a demand that Congress "rely upon spoon-fed information from the President."[1877]

Whistleblower Protection

Congress had created an inspector general for the Defense Department in 1982. Legislation in 1988 added a section on "Safeguarding of Military Whisteblowers," including prohibitions on retaliatory personnel actions against a member of the armed services for making or preparing a protected communication with a Member of Congress or an inspector general. The IG was authorized to investigate allegations by a member of the armed services who claims that a prohibited personnel action has been taken or threatened to be taken.[1878] The conference report explained:

> *The conferees note that in the course of their duties, members of the Armed Forces may become aware of information evidencing wrongdoing or waste of funds. It is generally the duty of members of the Armed Forces to report such information through the chain of command. Members of the armed forces, however, have the right to communicate directly with Members of Congress and Inspectors General (except to the extent that a communication is unlawful under applicable law or regulation), and there may be circumstances in which service members believe it is necessary to disclose information directly to a Member of Congress or an Inspector General. When they make lawful disclosures, they should be protected from adverse personnel consequences (or threats of such consequences), and there should be prompt investigations and administrative review of claims of reprisals. When such a claim is found to be meritorious, the Secretary concerned should initiate appropriate corrective action, including disciplinary action when warranted.*[1879]

Other modifications of the Military Whistleblower Protection Act are found in legislation passed in 1989, 1994, 1998, and 2000.[1880]

[1876] Id. at 740.

[1877] Id.

[1878] 102 Stat. 2027, § 846 (1988).

[1879] H.Rept. No. 100-989, 100th Cong., 2nd sess. 436-37 (1988). This language also appears at 134 Cong. Rec. 16977 (1988).

[1880] 103 Stat. 1910, § 202 (1989); 108 Stat. 2756, § 531 (1994); 112 Stat. 2107, § 993 (1998); 114 Stat. 1654A-224, § 903 (2000).

A current case of a military whistleblower concerns Bunnatine Greenhouse, who served as the chief of civilian contracting for the U.S. Army Corps of Engineers until she was demoted on August 27, 2005. She and the law firm representing her claim that she was demoted in retaliation for publicizing the concerns she had about no-bid contracts for work done in Iraq.[1881] This case received wide notice, including a PBS documentary and a *Washington Post* article.[1882]

Nondisclosure Agreements

In 1983, President Ronald Reagan directed that all federal employees with access to classified information sign "nondisclosure agreements" or risk the loss of their security clearance.[1883] Congress, concerned about the vagueness of some of the terms in the Reagan order and the loss of access to information, passed legislation in 1987 to prohibit the use of appropriated funds to implement the Administration's nondisclosure policy.[1884] The dispute was taken to court and in 1988 District Court Judge Oliver Gasch held that Congress lacked constitutional authority to interfere, by statute, with nondisclosure agreements drafted by the executive branch to protect the secrecy of classified information.[1885] Judge Gasch quoted from the Supreme Court's decision in Egan, issued in early 1988: "The authority to protect such [national security] information falls on the President as head of the Executive Branch and as Commander in Chief."[1886]

Department of the Navy v. Egan

Egan had been decided on statutory, not constitutional, grounds. The dispute involved the Navy's denial of a security clearance to Thomas Egan, who worked on the Trident submarine. He was subsequently removed. Egan sought review by the Merits Systems Protection Board (MSPB), but the Supreme Court upheld the Navy's action by ruling that the grant of security clearance to a particular employee, "a sensitive and inherently discretionary judgment call, is committed

---

[1881] For more detail, see [http://www.whistleblowers.org].

[1882] [http://www.pbs.org/now/politics.greenhouse.html]; Neely Tucker, "A Web of Truth: Whistle-Blower or Troublemaker, Bunny Greenhouse Isn't Backing Down," Washington Post, Oct. 19, 2005, at C1.

[1883] National Security Decision Directive 84 (1983); see Louis Fisher, "Congressional-Executive Struggles Over Information Secrecy Pledges," 42 Adm. L. Rev. 89, 90 (1990).

[1884] 101 Stat. 1329-432, § 630 (1987); 102 Stat. 1756, § 619 (1988).

[1885] National Federation of Federal Employees v. United States, 688 F.Supp. 671 (D.D.C. 1988).

[1886] Id. at 685 (citing Department of the Navy v. Egan, 198 S.Ct. at 824, 484 U.S. 518, 527 (1988)).

by law to the appropriate agency of the Executive Branch."[1887] The conflict in Egan was solely within the executive branch (Navy versus MSPB), not between Congress and the executive branch.

The focus on statutory, not constitutional, issues was reflected in briefs submitted by the parties. The Justice Department noted: "The issue in this case is one of statutory construction and 'at bottom . . . turns on congressional intent.'"[1888] The Court directed the parties to address this question: "Whether, in the course of reviewing the removal of an employee for failure to maintain a required security clearance, the Merit Systems Protection Board is authorized by statute to review the substance of the underlying decision to deny or revoke the security clearance."[1889]

The questions centered on 5 U.S.C. §§ 7512, 7513, 7532, and 7701. The Justice Department, after analyzing the relevant statutes and their legislative history, found no basis for concluding that Congress intended the MSPB to review the merits of security clearance determinations.[1890] Oral argument before the Court on December 2, 1987, explored the statutory intent of Congress. At no time did the Justice Department suggest that classified information could be withheld from Congress. The Court's ruling in favor of the Navy did not limit in any way the right of Congress to classified information. The Court decided the "narrow question" of whether the MSPB had statutory authority to review the substance of a decision to deny a security clearance.[1891]

Although the Court referred to independent constitutional powers of the President, including those as Commander in Chief and as head of the executive branch,[1892] and noted the President's responsibility with regard to foreign policy,[1893] its decision was based on statutory construction. In stating that courts "traditionally have been reluctant to intrude upon the authority of the Executive in military and national security affairs," the Court added this important

---

[1887] Department of the Navy v. Egan, 484 U.S. at 527 (emphasis added).

[1888] U.S. Department of Justice, "Brief for the Petitioner," Department of the Navy v. Egan, October Term 1987, at 22 (citing Clarke v. Securities Industry Ass'n, No. 85-971, Jan. 14, 1987).

[1889] Id. at (I) (emphasis added).

[1890] U.S. Department of Justice, "Petition for a Writ of Certiorari to the United States Court of Appeals for the Federal Circuit," Department of the Navy v. Thomas E. Egan, October Term 1986, at 4-5, 13, 15-16, 18.

[1891] 484 U.S. at 520.

[1892] Id. at 527.

[1893] Id. at 529.

qualification: "unless Congress specifically has provided otherwise."[1894] The Justice Department's brief had also stated: "Absent an unambiguous grant of jurisdiction by Congress, courts have traditionally been reluctant to intrude upon the authority of the executive branch in military and national security affairs."[1895] Nothing in the legislative history of the Civil Service Reform Act of 1978 convinced the Court that MSPB could review, on the merits, an agency's security-clearance determination.[1896]

The President's national security powers surfaced at times during oral argument before the Supreme Court, when the Justice Department and Egan's attorney, William J. Nold, debated the underlying statutory issues. After the department made its presentation, Nold told the Justices: "I think that we start out with the same premise. We start out with the premise that this is a case that involves statutory interpretation." Nold stated his view of the department's occasional references to constitutional matters: "What they seem to do in my view is to start building a cloud around the statute. They start building this cloud and they call it national security, and as their argument progresses . . . the cloud gets darker and darker and darker, so that by the time we get to the end, we can't see the statute anymore. What we see is this cloud called national security."[1897]

In disposing of the issue on statutory grounds, the Court also cited the President's role as Commander in Chief and said that the President's authority to protect classified information "flows primarily from this constitutional investment of power in the President and exists quite apart from any explicit congressional grant."[1898] The constitutional issue would have been joined had the Court faced statutory language that the administration objected to as an interference with executive power. That issue was not present in Egan.

The District Court's Decision

Having relied on *Egan*, Judge Gasch also looked to language in the Supreme Court's *Curtiss-Wright* decision.[1899] From the latter case Judge Gasch concluded that the "sensitive and complicated role cast for the President as this nation's emissary in foreign relations requires that congressional intrusion upon the

---

[1894] Id. at 530 (emphasis added).

[1895] U.S. Department of Justice, "Brief for the Petitioner," Department of the Navy v. Egan, October Term, 1987, at 21.

[1896] 484 U.S. at 531 n.6.

[1897] Transcript of Oral Argument, Dec. 2, 1987, at 19.

[1898] 484 U.S. at 527.

[1899] United States v. Curtiss-Wright Corp., 299 U.S. 304 (1936).

President's oversight of national security information be more severely limited than might be required in matters of purely domestic concern."[1900]

The central issue in Curtiss-Wright was the scope of congressional power. The Court was asked how broadly Congress could delegate its powers to the President in the field of foreign affairs. The previous year the Court had struck down the National Industrial Recovery Act because it had delegated an excessive amount of legislative power to the President in the field of domestic policy.[1901] The question before the Court in Curtiss-Wright was whether Congress could use more general standards in foreign affairs than it could in domestic affairs, and the Court said it could.

Several courts have remarked on Justice Sutherland's views in Curtiss-Wright regarding the scope of presidential power in foreign relations. In the Steel Seizure Case of 1952, Justice Robert Jackson noted that "much of the [Sutherland] opinion is dictum"——comments extraneous to the issue before the Court.[1902] In 1981, a federal appellate court cautioned against placing undue reliance on "certain dicta" in Sutherland's opinion: "To the extent that denominating the President as the 'sole organ' of the United States in international affairs constitutes a blanket endorsement of plenary Presidential power over any matter extending beyond the borders of this country, we reject that characterization."[1903]

On October 31, 1988, the Supreme Court noted probable jurisdiction in the case decided by Judge Gasch, now styled American Foreign Service Assn. v. Garfinkel.[1904] Both the House and the Senate submitted briefs protesting Judge Gasch's analysis of the President's powers over foreign affairs. During oral argument, the Justice Department spoke repeatedly about the President's constitutional role to control classified information. The attorney for AFSA challenging the Reagan nondisclosure policy objected that the decision by Judge Gasch, "by declaring that the Executive Branch has such sweeping power, has impeded the kind of accommodation that should take place in this kind of controversy," and hoped that the Court "wipes that decision off the books."[1905]

[1900] 688 F.Supp. at 685.

[1901] Schechter Corp. v. United States, 295 U.S. 495 (1935); Panama Refining Co. v. Ryan, 293 U.S. 388 (1935).

[1902] Youngstown Co. v. Sawyer, 343 U.S. 579, 636 n.2 (1952) (concurring op.).

[1903] American Intern. Group v. Islamic Republic of Iran, 657 F.2nd 430, 438 n.6 (D.C. Cir. 1981).

[1904] 488 U.S. 923 (1988).

[1905] Transcript of Oral Argument, March 20, 1989, at 60.

On April 18, 1989, the Court issued a per curiam order that vacated Judge Gasch's order and remanded the case for further consideration.[1906] In doing so, the Court cautioned Judge Gasch to avoid expounding on constitutional matters: "Having thus skirted the statutory question whether the Executive Branch's implementation of [Nondisclosure] Forms 189 and 4193 violated § 630, the court proceeded to address appellees' [the government's] argument that the lawsuit should be dismissed because § 630 was an unconstitutional interference with the President's authority to protect the national security."[1907] The Court counseled Judge Gasch that the district court "should not pronounce upon the relative constitutional authority of Congress and the Executive Branch unless it finds it imperative to do so. Particularly where, as here, a case implicates the fundamental relationship between the Branches, courts should be extremely careful not to issue unnecessary constitutional rulings."[1908]

On remand, Judge Gasch held that the plaintiffs (American Foreign Service Association and Members of Congress) failed to state a cause of action for courts to decide.[1909] Having dismissed the plaintiffs' complaint on that ground, Judge Gasch found it unnecessary to address any of the constitutional issues.[1910]

Funding Restrictions (Nondisclosure Forms)

Congress continues to enact provisions in appropriations bills to deny funds to implement nondisclosure forms. Legislation enacted on January 23, 2004 provided that no funds appropriated in the Consolidated Appropriation Act for fiscal 2004, or in any other statute, "may be used to implement or enforce the agreements in Standard Forms 312 and 4414 of the Government or any other nondisclosure policy, form, or agreement if such policy, form, or agreement does not contain the following provisions: 'These restrictions are consistent with and do not supersede, conflict with, or otherwise alter the employee obligations, rights or liabilities created'" by the Lloyd-LaFollette Act (5 U.S.C. § 7211), the Military Whistleblower Protection Act, the Whistleblower Protection Act, the Intelligence Identities Protection Act, and other statutes that enable Congress to receive information from agency employees. Notwithstanding that provision, a nondisclosure policy form or agreement that is executed by a person connected with the conduct of an intelligence or intelligence-related activity, other than an employee or officer of the federal government, "may contain provisions

---

[1906] American Foreign Service Assn. v. Garfinkel, 490 U.S. 153 (1989).

[1907] Id. at 158.

[1908] Id. at 161.

[1909] American Foreign Service Ass'n v. Garfinkel, 732 F.Supp. 13 (D.D.C. 1990).

[1910] Id. at 16.

appropriate to the particular activity for which such document is to be used." Such form or agreement shall, at a minimum, require that the person "will not disclose any classified information received in the course of such activity unless specifically authorized to do so by the United States Government." Furthermore, such nondisclosure forms "shall also make it clear that they do not bar disclosures to Congress or to an authorized official or an executive agency or the Department of Justice that are essential to reporting a substantial violation of law."[1911] That language also appears in the Transportation, Treasury appropriations law enacted on November 30, 2005.[1912]

Funding Restrictions (Access to Congress)

Also in annual appropriations acts, Congress adopts language to deny funds to pay the salary of any executive official who prevents agency employees from communicating with a Member of Congress, committee or subcommittee. Language in the Consolidated Appropriations Act for fiscal 2004 provided that no part of any appropriation contained in that statute or any other would be available for the payment of the salary of any federal government officer or employee who "(1) prohibits or prevents, or attempts or threatens to prohibit or prevent, any other officer or employee of the Federal Government from having any direct oral or written communication or contact with any Member, committee, or subcommittee of the Congress in connection with any matter pertaining to the employment of such other officer or employee or pertaining to the department or agency of such officer or employee in any way, irrespective of whether such communication or contact is at the initiative of such other officer or employee or in response to the request or inquiry of such Member, committee, or subcommittee." Funds are also denied for the payment of the salary of any federal officer or employee who "(2) removes, suspends from duty without pay, demotes, reduces in rank, seniority, status, pay, or performance of efficiency rating, denies promotion to, relocates, reassigns, transfers, disciplines, or discriminates in regard to any employment right, entitlement, or benefit, or any term or condition of employment of, any other officer or employee of the Federal Government, or attempts or threatens to commit any of the foregoing actions with respect to such other officer or employee, by reason of any communication or contact of such other officer or employee with any Member, committee, or subcommittee as described in paragraph (1)."[1913] That language appears also in the Transportation, Treasury appropriations statute for fiscal 2006.[1914]

[1911] 188 Stat. 355, § 620 (2004).

[1912] P.L. No. 109-115, § 820 (2005).

[1913] 118 Stat. 354, § 618 (2004).

[1914] P.L. 109-115, § 818 (2005).

OLC Opinion in 1996

On November 26, 1996, the Office of Legal Counsel (OLC) in the Justice Department issued an eight-page opinion on "(1) the application of executive branch rules and practices on disclosure of classified information to Members of Congress, in light of relevant congressional enactments; (2) the applicability of the Whistleblower Protection Act; and (3) the applicability of Executive Order 12674."[1915]

Executive Order 12674, signed by President Bush on April 12, 1989, established "Principles of Ethical Conduct for Government Officers and Employees." The principles included: "Employees shall disclose waste, fraud, abuse and corruption to appropriate authorities."[1916] The executive order defines "employee" to mean "any officer or employee of an agency, including a special Government employee,"[1917] and defines "agency" to mean "any executive agency as defined in 5 U.S.C. 105, including any executive department as defined in 5 U.S.C. 101, Government corporation as defined in 5 U.S.C. 103, or an independent establishment in the executive branch as defined in 5 U.S.C. 104 (other than the General Accounting Office), and the United States Postal Service and Postal Rate Commission."[1918] "Appropriate authorities" is not defined in the executive order.

Oversight of Intelligence Community

The question before the OLC was whether this executive order authorized an agency employee to disclose "waste, fraud, abuse and corruption" to a Member of Congress, particularly "members of oversight committees with direct interest in such abuse and corruption."[1919] The context of the memorandum focused on oversight committees that have jurisdiction over the Intelligence Community. OLC did "not question that in certain circumstances the term ["appropriate authorities"] could include a member of a congressional oversight committee." However, OLC concluded that the question of who is an "appropriate authority" to receive classified information "is governed by Executive Order 12356 and the related directives and practices." The latter executive order "should control

---

[1915] Memorandum for Michael J. O'Neil, General Counsel, Central Intelligence Agency, from Christopher H. Schroeder, Acting Assistant Attorney General, "Access to Classified Information," Nov. 26, 1996, at 1 (hereafter OLC Memo). Available from author.

[1916] Section 101(k) in Executive Order 12674, 54 Fed. Reg. 15159 (1989).

[1917] Id. at 15161 (§ 503(b)).

[1918] Id.at § 503(c)).

[1919] OLC Memo, at 7-8.

because it more directly and specifically addresses the subject at issue, the disclosure of classified information."[1920]

Executive Order 12356, signed by President Reagan on April 2, 1982, governed the handling of classified information in the executive branch.[1921] OLC was asked to address the relationship between that executive order and two congressional enactments concerning the rights of federal employees to provide information to Congress: the Lloyd-LaFollette Act and the annual provision that prohibited the use of appropriated funds to implement or enforce the nondisclosure agreement policy.

Reach of Lloyd-LaFollette

OLC cited the Justice Department's brief in the Garfinkel case to the Supreme Court, where the department held that a congressional enactment would be unconstitutional if it were interpreted "to divest the President of his control over national security information in the Executive Branch by vesting lower-ranking personnel in that Branch with a 'right' to furnish such information to a Member of Congress without receiving official authorization to do so."[1922] In effect, this position would support restraints such as those in the executive orders issued by Presidents Roosevelt and Taft, at least with respect to classified information. OLC concluded that Lloyd-LaFollette does not confer a right to furnish national security information to Congress, the nondisclosure agreements may be validly applied to a disclosure to a Member of Congress, and the appropriations language "does not authorize any disclosure to a Member of Congress that is not permitted under Executive Order 12356."[1923]

"Need to Know" by Lawmakers

OLC was also asked whether Executive Order 12356 could be read to permit a cleared employee of the executive branch "to disclose classified information to a cleared member of Congress based on the employee's determination of the member's need to know."[1924] OLC noted that Members of Congress, as constitutionally elected officers, do not receive security clearances but are instead presumed to be trustworthy. However, lawmakers are not exempt "from fulfilling the 'need-to-know' requirement." On the issue whether individual employees "are

---

[1920] Id. at 8.

[1921] 47 Fed. Reg. 14874 (1982).

[1922] OLC Memo, at 3.

[1923] Id. at 4.

[1924] Id. at 5.

free to make a disclosure to Members of Congress based on their own determination on the need-to-know question," OLC said that the answer "is most assuredly 'no.'"[1925] The determination of "need to know" regarding disclosures of classified information to Congress "is made through established decisionmaking channels at each agency." OLC stated the opinion that it would be "antithetical to the existing system for an agency to permit individual employees to decide unilaterally to disclose classified information to a Member of Congress——and we are unaware of any agency that does so."[1926]

Regarding the WPA, OLC was asked whether denial or revocation of a Sensitive Compartmented Information (SCI) security clearance is a "personnel action" within the meaning of the WPA. Citing such cases as the Supreme Court's decision in Egan and McCabe v. Department of the Air Force, decided by the Court of Appeals for the Federal Circuit, OLC concluded that the revocation of a security clearance is not a personnel action within the meaning of the WPA.[1927]

OLC also examined language in Title 5, under prohibited personnel practices, that nothing in that subsection shall be construed "to authorize the withholding of information from the Congress or the taking of any personnel action against an employee who discloses information to the Congress."[1928] OLC said the Justice Department in Garfinkel had rejected the argument that the quoted language conferred an affirmative right to make disclosures of classified information to Members of Congress. Subsection 2302(b)(8)(B) discussed disclosures of classified information only to inspectors general or the Office of Special Counsel of the MSPB.

CIA Whistleblower Act of 1998

OLC's memo prompted Congress to hold hearings and analyze the Administration's position that the President exercises exclusive control over the disclosure of classified information, including disclosure to Members of Congress and its committees. The Senate Intelligence Committee asked CRS to evaluate OLC's statutory and constitutional conclusions, and that analysis was published.[1929] The Committee also held two days of hearings.[1930] The Justice

---

[1925] Id.

[1926] Id. at 6.

[1927] Id.

[1928] 5 U.S.C. § 2302(b) (2000).

[1929] Prepared statement by Louis Fisher, Congressional Research Service, "Executive Employee Access to Congress," reprinted in "Disclosure of Classified Information to Congress," hearings before the Senate Select Committee on Intelligence, 105th Cong., 2nd sess. 5-13 (1998).

Department continued to hold that bills drafted to assure congressional access to classified information, submitted to Congress by intelligence community employees without the permission of their supervisors, were unconstitutional.

The Senate Bill

The Senate Intelligence Committee unanimously reported legislation after commenting that the Administration's "intransigence on this issue compelled the Committee to act."[1931] The Senate bill would have directed the President to inform employees within the intelligence community that it is not prohibited by law, executive order, or regulation, nor contrary to public law, to disclose certain information, including classified information, to an appropriate committee of Congress.[1932] The purpose of the bill was to make employees within the intelligence community aware that they may, without seeking or obtaining prior authorization from an agency supervisor, disclose certain information to Congress, including classified information, when they have reason to believe that the information is specific and direct evidence of "a violation of law, rule or regulation; a false statement to Congress on an issue of material fact; or gross mismanagement, a gross waste of funds, a flagrant abuse of authority, or a substantial and specific danger to public health or safety."[1933]

The House Bill

> *The House Intelligence Committee held two days of hearings on a bill that provided an alternative procedure for gaining information from national security whistleblowers.[1934] Chairman Porter J. Goss made these opening comments:*
>
> *The present arrangement, or lack of arrangement, for whistleblowers in our [intelligence] community is not the answer. CIA, as I understand, has no written regulation in place and NSA had one that was disavowed by the current administration. I know of no regulation or system within the Intelligence Community that*

[1930] Id. at 5-37 (testimony by Louis Fisher, CRS, and Peter Raven-Hansen, George Washington University Law School) and 39-61 (Louis Fisher and Randolph D. Moss, Deputy Assistant Attorney General, Office of Legal Counsel, Department of Justice).

[1931] S.Rept. No. 105-165, 105th Cong., 2nd sess. 5 (1998).

[1932] Id. at 1.

[1933] Id.

[1934] House Permanent Select Committee on Intelligence, "Record of Proceedings on H.R. 3829, The Intelligence Community Whistleblower Protection Act," 106th Cong., 1st sess. (1999) [Hearings on May 20 and June 10, 1998].

ensures the confidentiality of the whistleblower. There is no legal protective mechanism for an IC whistleblower against official and unofficial retaliation of which I am aware. Nothing currently gives him a right to be heard directly by the intelligence committees.

I think the only exception I can think of might be one under clauses of the Agent Identities Protection Act, which is a very narrow area.

The result of this system is unacceptable. Employees of the IC may, at present, have to take huge chances with classified documents, compartmented information and their careers in order to come down to report to us. . . . Worst of all, from an institutional point of view, is that very few employees dare to run this gauntlet to bring us the information we need to do appropriate oversight.[1935]

"Sole Process" and "Holdback"

Chairman Goss identified two central issues in the legislation. One was the question whether CIA employees should report their concerns only to the inspector general. Was the IG to be the "sole process" by which an employee may report a serious or flagrant problem to Congress? Second, should the head of an intelligence agency have a "holdback" power? That is, should the agency head be authorized to block a whistleblower's complaint "in the exceptional case and in order to protect vital law enforcement, foreign affairs on national security interest."[1936]

When the House bill was reported it was decided that the IG mechanism for whistleblowers should not be the "sole process" for them to report wrongdoing to Congress. The House bill would provide an additional procedure to the existing IG route.[1937] The House Intelligence Committee recognized that some agency employees might "choose not to report a problem either through the process outlined [in the bill] or through another process authorized by their management, but instead approach the committee directly."[1938] The committee also decided to eliminate the "holdback" provision. Agency heads would not have the authority to block disclosures byagency employees to Congress. A statutory

---

[1935] Id. at 2.

[1936] Id. at 4.

[1937] H.Rept. No. 105-747 (Part 1), 105th Cong., 2nd sess. 13 (1998).

[1938] Id. at 20.

acknowledgment of holdback authority was dropped because it was considered "unwarranted and could undermine important congressional prerogatives."[1939]

Authority Over Classified Information

Like the Senate, the House Intelligence Committee rejected the Administration's "assertion that, as Commander in Chief, the President has ultimate and unimpeded constitutional authority over national security, or classified, information. Rather, national security is a constitutional responsibility shared by the executive and legislative branches that proceeds according to the principles and practices of comity."[1940] Consistent with that position, the committee rejected the theory that the President, as Chief Executive, "has a constitutional right to authorize all contact between executive branch employees and Congress." The issue of whether an agency employee "must 'ask the boss' before approaching the intelligence committees with unclassified information about wrongdoing seems well below any constitutional threshold."[1941] The handling of classified information was addressed in the bill that became law.

The Statute

The two houses worked out their differences in conference committee and reported the Intelligence Community Whistleblower Protection Act as Title VII to the Intelligence Authorization Act for Fiscal Year 1999. The compromise bill established "an additional process to accommodate the disclosure of classified information of interest to Congress." The new procedure was not "the exclusive process by which an Intelligence Community employee may make a report to Congress." The conference report stated that "the managers agree that an Intelligence Community employee should not be subject to reprisals or threats of reprisals for making a report to appropriate Members or staff of the intelligence committees about wrongdoing within the Intelligence Community."[1942] The statute covered communications from the agency to Capitol Hill through the intelligence committees.

The statutory language lists six findings: "(1) national security is a shared responsibility requiring joint efforts and mutual respect by Congress and the President; (2) the principles of comity between the branches of Government apply to the handling of national security information; (3) Congress, as a co-equal branch of Government, is empowered by the Constitution to serve as a check on

---

[1939] Id. at 14.

[1940] Id. at 15.

[1941] Id.

[1942] H.Rept. No. 105-780, 105th Cong., 2nd sess. 34 (1998).

the executive branch; in that capacity, it has a "need to know" of allegations of wrongdoing within the executive branch, including allegations of wrongdoing in the Intelligence Community; (4) no basis in law exists for requiring prior authorization of disclosures to the intelligence committees of Congress by employees of the executive branch of classified information about wrongdoing within the Intelligence Community; (5) the risk of reprisal perceived by employees and contractors of the Intelligence Community for reporting serious or flagrant problems to Congress may have impaired the flow of information needed by the intelligence committees to carry out oversight responsibilities; and (6) to encourage such reporting, an additional procedure should be established that provides a means for such employees and contractors to report to Congress while safeguarding the classified information involved in such reporting."[1943]

Under the procedures set forth in the statute, an employee or contractor of the CIA "who intends to report to Congress a complaint or information with respect to an urgent concern may report such complaint or information to the Inspector General."[1944] The language "may report" is consistent with the congressional rejection of the IG office as being the "sole process" for reporting complaints.

The statute defines "urgent concern" to mean any of the following: (1) "A serious or flagrant problem, abuse, violation of law or Executive order, or deficiency relating to the funding, administration, or operations of an intelligence activity involving classified information, but does not include differences of opinion concerning public policy matters"; (2) "A false statement to Congress, or a willful withholding from Congress, or an issue of material fact relating to the funding, administration, or operation of an intelligence activity"; and (3) "An action, including a personnel action described in section 2302(a)(2)(A) of title 5, United States Code, constituting reprisal or threat of reprisal prohibited under subsection (e)(3)(B) in response to an employee's reporting an urgent concern in accordance with this paragraph."

Upon receiving the complaint or information, the IG has 14 calendar days to determine whether it appears credible. If the IG decides it is, the complaint must be transmitted to the CIA Director who has seven calendar days to forward the matter to the intelligence committees. If the IG does not transmit the complaint or information, or does not transmit it in an accurate form, the employee may submit the matter to Congress by contacting either or both of the intelligence committees. The statute provides for no "holdback" procedure.

[1943] 112 Stat. 2413-14, § 701 (1998).

[1944] Id. at 2414, § 702 (a)(1).

In 2001, Congress enacted modifications to this statute.[1945] The changes relate to communications between the IG and the director as to whether a complaint from an agency employee appears credible, and the authority of employees to contact the intelligence committees when the IG does not find the complaint credible.

The Richard Barlow Case

In 2002, the U.S. Court of Federal Claims decided the case of Richard Barlow, who in the late 1980s faced termination from the Defense Department and suspension of security clearances following disputes within the executive branch, and between the executive branch and Congress, about Pakistan's nuclear capabilities. Some central questions reportedly were whether executive officials had misled lawmakers, in secret briefings, regarding Pakistan's activities, and whether the Reagan Administration had improperly certified to Congress that Pakistan did not have nuclear weapons.[1946]

After a number of investigations by the Defense Department and several by inspectors general and the General Accounting Office regarding retaliations against Barlow's whistleblower activities, a bill was introduced (S. 2274) to provide for the relief of Barlow.[1947] The private bill included the sum of $1,100,000 to compensate him for losses incurred as a consequence of "(1) personnel actions taken by the Department of Defense affecting Mr. Barlow's employment at the Department (including Mr. Barlow's top secret security clearance) during the period of August 4, 1989, through February 27, 1992; and (2) Mr. Barlow's separation from service with the Department of Defense on February 27, 1992."[1948] On October 5, 1998, the Senate referred the matter to the Court of Federal Claims requesting that it report back findings of fact and conclusions "that are sufficient to inform the Congress of the nature, extent, and character of the claim for compensation referred to in such bill [S. 2274] as a legal or equitable claim against the United States or a gratuity."[1949]

State Secrets Privilege

Barlow and his attorneys, through the discovery process, sought documents which they alleged would show that Congress had been misled about Pakistan's capabilities. They claimed that the evidence would show a motivation on the part

---

[1945] 115 Stat. 1399-00, § 309 (2001).

[1946] Seymour M. Hersh, "On the Nuclear Edge," The New Yorker, March 29, 1993, at 56.

[1947] For a description of these investigations, see Barlow v. United States, 51 Fed.Cl. 380, 390-92 (2002).

[1948] S. 2274, 105th Cong., 2nd sess. (1998).

[1949] 144 Cong. Rec. 23357 (1998).

of Barlow's supervisor in the Defense Department to take adverse personnel actions against him for his whistleblowing. On February 10, 2000, CIA Director George Tenet signed a declaration and formal claim of state secrets privilege and statutory privilege. The declaration denied Barlow and his attorney access to any of the classified intelligence information under Tenet's control. Tenet said that it would not be possible "to sanitize or redact in any meaningful way" the information that Barlow sought.[1950] A separate declaration by Lt. Gen. Michael V. Hayden, Director of the National Security Agency, also invoked the state secrets privilege to assert the agency's privilege over NSA intelligence reports and information from intelligence reports contained in minutes of the Nuclear Export Violations Working Group (NEVWG) meetings.[1951]

The Tenet declaration did not automatically block Barlow's access to the requested materials. Tenet acknowledged that the branch that decides what evidence to admit is the judiciary, not the executive branch: "I recognize it is the Court's decision rather than mine to determine whether requested material is relevant to matters beings addressed in litigation."[1952] The Hayden declaration did not contain that language, but courts have discretion to determine whether an executive claim of state secrets privilege should be treated as absolute or as qualified. The Court of Federal Claims had several options. It could have ordered the government to provide a full public account of why disclosure of the information would harm national security.[1953] It could have conducted "an in camera examination of the requested materials"[1954] and also asked that sensitive material be redacted to permit access by Barlow.

Options for the Court

In a decision filed July 18, 2000, and reissued August 3, 2000, the Court of Federal Claims initially acknowledged that the state secrets privilege was qualified, not absolute. Although it noted that some courts have held that state

---

[1950] Declaration and Formal Claim of State Secrets Privilege and Statutory Privilege by George J. Tenet, Director of Central Intelligence, Feb. 10, 2000, Barlow v. United States, Congressional Reference No. 98-887X, at 9 (hereafter "Tenet Declaration"). Available from author.

[1951] "Declaration of Lieutenant General Michael V. Hayden, United States Air Force, Director of the National Security Agency, Feb. 2000, Barlow v. United States, Congressional Reference No. 98-887X. Available from author.

[1952] Tenet Declaration, at 7.

[1953] Ellsberg v. Mitchell, 709 F.2nd 51, 60-64 (D.C. Cir. 1983).

[1954] Id. at 64.

secrets are "absolutely privileged from disclosure in the courts,"[1955] it stated that "the mere formal declaration of the privilege does not end the court's inquiry."[1956] Toward the end of this analysis, however, the court ruled that state secrets were absolute: "The privilege is absolute, the law having evolved to reflect a choice of secrecy over any balancing of risks and harms."[1957] The court concluded that the documents sought by Barlow, "to the extent not already produced or located, are privileged *in toto*."[1958]

The court continued the trial and allowed the government to introduce the documents and testimony to support its case, while at the same time denying Barlow access to documents and testimony he requested to support his position. On May 4, 2000, Barlow's attorneys, Paul C. Warnke and Diane S. Pickersgill, objected that the state secrets privilege should not apply to congressional reference cases to prevent Barlow and the court access to "key evidence."[1959] Warnke and Pickersgill argued that the court should review the documents in camera.[1960] They noted that the Senate had ordered the court to "make a determination of the merits" of Barlow's claim for compensation and that the information he sought in discovery was "necessary for this Court to make a fully-informed decision and thus a fully-informed recommendation to Congress."[1961]

Applying Egan

In the January 14, 2002, ruling, the court recognized that there had been a "temporary suspension" of Barlow's security clearance.[1962] In Egan, the plaintiff's security clearance had been revoked. The court stated that in Egan the Supreme Court held that "the authority to protect classified information remains within the Executive Branch," determinations about security clearances are an attempt to predict an individual's future behavior, and that such "'[p]redictive judgment of this kind must be made by those with the necessary expertise in protecting

---

[1955] Barlow v. United States, No. 98-887X, 2000 WL 1141087, at 4, citing Halkin v. Helms, 690 F.2nd 977, 990 (D.C. Cir. 1982).

[1956] Barlow v. United States, WL 1141087, at 4.

[1957] Id. at 8-9.

[1958] Id. at 9.

[1959] Plaintiff's Opposition to Defendant's Motion for a Protective Order, Barlow v. United States, Congressional Reference No. 98-887 X, at 1.

[1960] Id. at 9.

[1961] Id. at 14.

[1962] Barlow v. United States, 51 Fed.Cl. at 393.

classified information' and, in turn, not by the courts."[1963] The court then concluded: "Basing a claim to relief in any way on the suspension of the clearance would inevitably draw the court into improperly second guessing executive branch offices in a highly discretionary function. We decline to do so."[1964]

The Supreme Court in Egan supported the discretionary judgment of the executive branch to determine security clearances and to revoke them. The Court's decision did address the question of whether a court may examine, in camera, classified documents to determine whether they were properly withheld from a plaintiff under the state secrets privilege.

"Official Secrets"

In 2000, Congress passed a bill that would have established criminal penalties for leaking classified information. Fines and imprisonment for up to three years were included to punish any current or former government employee who "knowingly and willfully discloses, or attempts to disclose," any classified information to a person not authorized to receive the information, "knowing that the person is not authorized access to such classified information."[1965] Criminal liability did not apply to the disclosure of classified information to federal judges established under Article III or to any Member or committee of Congress.

During House debate on the bill reported from conference committee, several Members referred to it as an "official secrets" law.[1966] One Member said it would intimidate whistleblowers.[1967] Another thought it "would silence whistleblowers in a way that has never before come before this body and which has never before been enacted."[1968] Another disagreed: "I do not think that is true at all. First of all, whistle-blowers are protected under the current law. Secondly, whistle-blowers who have a concern about whether information is properly classified or there is a concern about the agency that they are working for, can come to Congress."[1969] Similarly, another Member regarded whistleblowers as protected

---

[1963] Id. at 394 (internal quote from Egan, 484 U.S. at 528).

[1964] Id.

[1965] Section 304 of H.R. 4392, as reported from conference committee; H.Rept. No. 106-969, 106th Cong., 2nd sess. 6-7 (2000).

[1966] 146 Cong. Rec. 22390 (Rep. Pelosi) and 22394 (Rep. Barr) (2000). In 1889, Great Britain enacted an Official Secrets Act to punish individuals who leak government secrets. It was revised in 1911, 1920, 1939, and 1989.

[1967] Id. at 22393 (Rep. Conyers).

[1968] Id. at 22394 (Rep. Barr).

[1969] Id. at 22395 (Rep. Hutchinson).

by the bill "[s]o long as they come forward with matters that are security matters about which they are concerned and they disclose them to people who are cleared to received such information."[1970]

This debate raised the possibility that leaking information to the press would put reporters at risk. One Member stated that "this [bill] does not pertain to the news media."[1971] Another saw "nothing [in the bill] to prevent reporters from being hauled in before grand juries and being forced to reveal their sources."[1972] Chief executives of four of the largest news organizations (CNN, the New York Times, Newspaper Association of America, and the Washington Post) wrote to President Clinton, urging him to veto the bill. The Radio-Television News Directors Association also joined in this appeal to President Clinton.[1973]

President Clinton vetoed the bill on November 4, 2000. Among other points, he said that the bill "was passed without benefit of public hearings——a particular concern given that it is the public that this law seeks ultimately to protect. The Administration shares the process burden since its deliberations lacked the thoroughness this provision warranted, which in turn led to a failure to apprise the Congress of the concerns I am expressing today."[1974]

Pending Legislation

Legislation has been introduced in the House and the Senate to make changes in the Whistleblower Protection Act. S. 494, called the Federal Employee Protection of Disclosures Act, was introduced on March 2, 2005, and reported from the Committee on Homeland Security and Governmental Affairs on May 25. The purpose is "to clarify the disclosures of information protection from prohibited personnel practices, require a statement in nondisclosure policies, forms, and agreements that such policies, forms, and agreements conform with certain disclosure protections, provide certain authority for the Special Counsel, and for other purposes."[1975]

[1970] Id. (Rep. Lewis).

[1971] Id. (Rep. Hutchinson).

[1972] Id. (Rep. Pelosi).

[1973] Raymond Bonner, "News Organizations Ask White House to Veto Secrecy Measure," New York Times, Nov. 1, 2000, at A32.

[1974] Public Papers of the Presidents, 2000-2001, III, at 2467. See also John M. Broder, "President Vetoes Measure to Punish Disclosing Secrets," New York Times, Nov 5, 2000, at 1; Walter Pincus, "Clinton Vetoes Bill Targeting Leaks of Classified Information," Washington Post, Nov. 5, 2000, at A5.

[1975] S. 494, 109th Cong., 1st sess. 1-2 (2005), as reported by the Committee on Homeland Security and Governmental Affairs.

In reporting the bill, the Senate Committee on Homeland Security and Governmental Affairs noted that the terrorist attacks of 9/11 "have brought renewed attention to those who disclose information regarding security lapses at our nation's airports, borders, law enforcement agencies, and nuclear facilities." It further states that the right of federal employees to be free from agency retaliation "has been diminished as a result of a series of decisions of the Federal Circuit Court of Appeals that have narrowly defined who qualifies as a whistleblower under the WPA and what statements are considered protected disclosures."[1976] The bill is designed to clarify that disclosures of classified information to appropriate committees of Congress are protected, to codify the "anti-gag" provision that Congress has placed in annual appropriations bills to protect agency employees who come forward with disclosures of illegality, to authorize the OSC to file amicus briefs in whistleblower cases, and to allow whistleblower cases to be heard by all federal appellate courts for a period of five years.[1977]

The committee report also discusses a provision in the bill that relates to whistleblower actions after 9/11, when agency employees "in several high profile cases have come forward to disclose government waste, fraud, and abuse that posed a risk to national security," but then faced retaliatory action by having their security clearance removed. The Federal Circuit had held that the MSPB lacks jurisdiction over an employee's claim that his security clearance was revoked in retaliation for whistleblowing. Former Special Counsel Elaine Kaplan testified in 2001 that revoking a security clearance "can be a basis for camouflaging retaliation."[1978] The Senate bill makes it a prohibited personnel practice for a manager to suspend, revoke, or take other actions regarding an employee's security clearance or access to classified information in retaliation for whistleblowing. Further, the bill provides for expedited review of whistleblower cases by the OSC, the MSPB, and the reviewing cases where a security clearance has been revoked or suspended.[1979]

The Justice Department regards this provision as an intrusion into the President's prerogative to control national security information and those who have access to it. The committee regards executive branch authority over classified material as "not exclusive, and that Congress properly plays a role."[1980]

[1976] Id. at 2.

[1977] Id.

[1978] Id. at 15.

[1979] Id. at 16.

[1980] Id.

The committee cites Egan for support ("unless Congress has specifically provided otherwise, courts traditionally have been reluctant to intrude upon the authority of the Executive in military and national security affairs").[1981]

Title 5 has included a provision (Section 2302(b)) that nothing in the subsection shall be construed to authorize the withholding of information from Congress or the taking of any personnel action against an agency employee who discloses information to Congress. The Senate bill provides that a whistleblower must limit the disclosure to a Member of Congress who is authorized to receive the information or to a legislative staffer who holds the appropriate security clearance and is authorized to receive the information.[1982]

H.R. 1317, introduced on March 15, 2005, contains a number of provisions similar to S. 494, including clarification of disclosures that are protected from prohibited personnel practices and a statement to be placed in nondisclosure forms. The House bill directs the Comptroller General to conduct a study of security clearance revocations in whistleblower cases after 1996. H.R. 1317 was marked up on September 29, 2005, and ordered to be reported.

Conclusions

To perform its legislative and constitutional functions, Congress depends on information (domestic and national security) available from the executive branch. The Supreme Court remarked in 1927 that a legislative body "cannot legislate wisely or effectively in the absence of information respecting the conditions which the legislation is intended to affect or change; and where the legislative body does not itself possess the requisite information——which not infrequently is true—— recourse must be had to those who do possess it."[1983] Congress needs information to pass legislation, oversee the administration of programs, inform the public, and carry out its constitutional duties.

Balancing this legislative need for information with the protection of sensitive national security information remains a continuing policy issue. Congress has never accepted the theory that the President has exclusive, ultimate, and unimpeded authority over the collection, retention, and dissemination of national security information. Agency heads provide Congress with information, but some Members of Congress have also expressed a need to receive information directly from rank-and-file employees within an agency. Whistleblowers have helped uncover agency wrongdoing, illegalities, waste, and corruption. The interest of Congress in maintaining an open channel with agency employees is

---

[1981] Id. (emphasis added by committee).

[1982] Id. at 18.

[1983] McGrain v. Daugherty, 273 U.S. 135, 175 (1927).

demonstrated through such statutes as Lloyd-LaFollette, the appropriations riders on the nondisclosure policy, the Military Whistleblower Protection Act, and the Intelligence Community Whistleblower Act.

Congress also recognizes the need to protect national security information, especially that related to sources and methods, from disclosure. This awareness is reflected in legislation that allows and encourages intelligence community employees to report issues of waste, fraud, or mismanagement to the intelligence committees of Congress.

Appendix: Whistleblower Organizations

Several organizations have been active with whistleblowing issues. They testify before congressional committees, provide assistance with litigation, and offer other services. Some of these organizations cover whistleblowing in general. Others focus on national security whistleblowing. From October 9 to October 12, 2005, in Chincoteague, Va., the first annual National Security Whistleblowers Conference was held. It was sponsored by the National Security Whistleblower Coalition, the Cavallo Foundation, Harriet Crosby, the Fertel Foundation, the Fund for Constitutional Government, and Project on Government Oversight. The purpose was to bring together national security whistleblowers to learn from each other, to find collective support for their efforts, and to develop strategies.

Government Accountability Project (GAP)

Founded in 1977, GAP is a non-profit, public interest organization and law firm that receives funding from foundations, individuals, and legal fees. It describes its mission as protecting the public interest by promoting government and corporate accountability through advancing occupational free speech and ethical conduct, defending whistleblowers, and empowering citizen activists. It litigates whistleblower cases, publicizes whistleblower concerns, and develops policy and legal reforms for whistleblower laws. Much of its work has been in the area of nuclear oversight, food and drug safety, worker health and safety, international reform and national security.[1984]

National Security Whistleblowers Coalition

The coaliton is a nonpartisan organization dedicated to aiding national security whistleblowers. Its stated mission is to advocate governmental and legal reform, educate the public concerning whistleblowing activity, provide comfort and fellowship to national security whistleblowers subject to retaliation, and work with other public interest organizations to effect goals defined in the organization's mission statement. Its membership consists exclusively of current or former federal employees or civilians working under contract to the United

[1984] For information on GAP, see [http://www.whistleblower.org/about/index.cfm].

States who, to their detriment and personal risk, bring to light fraud, waste, and abuse in government operations and agencies related to national security.[1985]

National Whistleblower Center

The National Whistleblower Center is a non-profit, tax-exempt, educational, and advocacy organization dedicated to helping whistleblowers. Since 1988, it states it has used whistleblowers' disclosures to improve environmental protection, nuclear safety, and government and corporate accountability. The primary goal of the center is to ensure that disclosures about government or industry actions that violated the law or harm the environment are fully heard, and that the whistleblowers who risk their careers to expose wrongdoing are defended. In addition to assisting whistleblowers, the center lobbies Congress on the need to protect whistleblowers and insists that officials be held fully accountable for their conduct. The center maintains a national referral service and sponsors litigation.[1986]

Project On Government Oversight (POGO)

POGO began in 1981 as an independent, non-profit organization that investigates and exposes corruption in order to achieve a more accountable federal government. It operates on the principle that representation and accountability are fundamental to maintaining a strong and functioning democracy. Initially it was known as the Project on Military Procurement. It is committed to exposing waste, fraud and corruption in the following areas: defense, homeland security, energy and environment, contract oversight, and open government. POGO's "Contract Oversight Investigations" examine the federal government's policies and relationships with grant recipients as well as major companies that receive billions of dollars in contracts and subsidies annually.[1987]

[1985] See [http://www.nswbc.org].

[1986] See [http://www.whistleblowers.org].

[1987] See [http://www.pogo.org/p/x/aboutus.html].

18 U.S.C. Chapter 51: Homicide (18 U.S.C. §§ 1111-1122)

Assassination and Targeted Killing

Assassination Ban and E.O. 12333: A Brief Summary, RS21037 (January 4, 2002).

ELIZABETH B. BAZAN, CONGRESSIONAL RESEARCH SERV., ASSASSINATION BAN AND E.O. 12333: A BRIEF SUMMARY (2002), , *available at* http://www.intelligencelaw.com/library/secondary/crs/pdf/RS21037_1-4-2002.pdf.

Order Code RS21037
Updated January 4, 2002

CRS Report for Congress

Elizabeth B. Bazan
Legislative Attorney
American Law Division

Summary

In the wake of the September 11, 2001, terrorist attacks on the New York World Trade Center and the Pentagon, some attention has been focused upon the assassination ban contained in Executive Order (E.O.) 12333, Section 2.11, and whether it would prohibit the United States from responding to the attacks by targeting those who orchestrated these acts of terrorism. In considering the challenges involved in effectively combating terrorism and protecting the United States from future terrorist attacks, there has been wide-ranging debate as to what approaches might be beneficial. Part of that discussion has centered around whether assassination of terrorist leaders is, or should be, one of the options available. This report offers a summary discussion of the assassination ban in E.O. 12333, its context, and possible interpretations of its scope.

Introduction

On December 4, 1981, President Ronald Reagan issued Executive Order 12333 on "United States Intelligence Activities." Section 2.11 of the order provides: "Prohibition on Assassination. No person employed by or acting on behalf of the United States Government shall engage in, or conspire to engage in, assassination." Section 2.12 of the order prohibits indirect participation in

activities prohibited by the order, stating: "Indirect participation. No agency of the Intelligence Community shall participate in or request any person to undertake activities forbidden by this Order." E.O. 12333 is still in force.

E.O. 12333 is the latest in a series of three executive orders which included assassination bans. The first, Executive Order 11905, Sec. 5(g),[1988] 41 Fed. Reg. 7703, 7733 (President Gerald Ford, 2/19/76), was part of an executive order issued by President Ford in response to concerns raised in the 1970's with respect to alleged abuses by the U.S. intelligence community. A select committee chaired by Senator Frank Church (the Church Committee), in its interim report, addressed allegations of possible U.S. involvement in assassination plots against certain foreign leaders. In its recommendations section, the Church Committee condemned assassination and rejected it as an instrument of American policy.[1989] The assassination ban in E.O. 11905 was superseded by Executive Order 12036, Sec. 2-305 (assassination prohibition) and Sec. 2-309 (indirect participation prohibition),[1990] 43 Fed. Reg. 3674, 3688, 3689 (President Jimmy Carter, 1/26/78). The pertinent provisions in President Reagan's E.O. 12333, in turn, superseded those in President Carter's order.

What does the assassination ban in E.O. 12333 cover?

The term "assassination" is not defined in E.O. 12333, nor was it defined in the predecessor orders.[1991] In general, it appears that an assassination may be viewed as an intentional killing of a targeted individual committed for political purposes. However, the scope of the term seems to be the subject of differing interpretations, both generally, and depending upon whether the killing at issue took place in time of war or in time of peace. For example, it might be contended that the Ford executive order and its successors were responding to concerns raised with respect to killing of foreign officials or heads of state, and may not

---

[1988] This section of E.O. 11905 stated, "Prohibition of Assassination. No employee of the United States Government shall engage in, or conspire to engage in, political assassination."

[1989] See Alleged Assassination Plots Involving Foreign Leaders, An Interim Report of the Select Committee to Study Governmental Operations with respect to Intelligence Activities, United States Senate, S. Rept. 94-465, 94th Cong., 1st Sess. 281-84 (Nov. 20, 1975) (Church Committee).

[1990] The pertinent provisions of the Carter order read, "2-305. Prohibition on Assassination. No person employed by or acting on behalf of the United States Government shall engage in, or conspire to engage in, assassination. . . . 2-307. Restrictions on Indirect Participation in Prohibited Activities. No agency of the Intelligence Community shall request or otherwise encourage, directly or indirectly, any person, organization, or government agency to undertake activities forbidden by this order or by applicable law."

[1991] It is interesting to note that the Ford order referred to "political assassination," a term which was not defined in E.O. 11905, while the Carter and Reagan orders use the term "assassination," again without defining it. It is thus unclear from these orders and the statements accompanying their issuance whether or not this change in language was intended to portend any change in the scope of the ban.

have been intended to extend to killing of others. Such an interpretation would be consistent with the focus of the Church Committee's investigation, to which the Ford executive order responded. In his "Special Message to the Congress Proposing Legislation To Reform the United States Foreign Intelligence Community," (Special Message to Congress) delivered Feb. 18, 1976, accompanying the issuance of E.O. 11905, President Ford did not refer to the assassination ban in the order explicitly, but did indicate that he would "support legislation making it a crime to assassinate or attempt or conspire to assassinate a foreign official in peacetime."[1992] President Carter made only a passing reference to the assassination ban in his statement accompanying issuance of E.O. 12036,[1993] and did not refer to it in his remarks on signing the executive order. Nor did President Reagan reference the assassination ban in his "Statement on United States Intelligence Activities" of Dec. 4, 1981, accompanying the issuance of E.O. 12333.[1994]

Others might argue for a broader interpretation of the assassination ban, contending that any killing of a targeted individual for political purposes would be within the assassination ban in the sweep of the Ford, Carter, and Reagan executive orders. Alternatively, it might be suggested that the assassination ban's inclusion within an executive order on U.S. intelligence activities may serve to

---

[1992] Public Papers of the Presidents of the United States, Gerald R. Ford, 1976-77, Book I, 362, 364 (1979).

[1993] Public Papers of the Presidents of the United States, Jimmy Carter, 1978, Book I, 189-216 (1979). The context of President Carter's reference was as follows:

3. Our intelligence agencies have a critical role to play in collecting and analyzing information important to our national security interests and, on occasion, acting in direct support of major foreign policy objectives. It is equally important, however, that the methods employed by these agencies meet constitutional standards protecting the privacy and civil liberties of U.S. persons and are in full compliance with the law. To accomplish this objective a major section of the Executive order is devoted entirely to setting forth detailed restrictions on intelligence collection, covert activities in support of foreign policy objectives, experimentation, contracting, assistance to law enforcement authorities, personnel assigned to other agencies, indirect participation in prohibited activities,, dissemination and storage of information, and a prohibition on assassinations. The FBI's intelligence activities no longer have a blanket exception to these restrictions. At the heart of the restriction process is a greatly enhanced role for the Attorney General, as the Nation's top legal officer, to establish and approve procedures to regulate the conduct of the most sensitive intelligence activities. These detailed procedures, which will be made available to the congressional oversight committees, will ensure compliance with the law, protect constitutional rights and privacy, and ensure that any intelligence activity within the United States or directed against Americans will employ the least intrusive means possible and that the use, dissemination, and storage of such information is limited to that necessary to achieve lawful governmental purposes.

Id. at 215-16.

[1994] Public Papers of the Presidents of the United States, Ronald Reagan, 1981, 1126-27 (1982).

distinguish it from, and limit its applicability to, a use of military force in response to a foreign terrorist attack on U.S. soil or against U.S. nationals. Such an argument might place reliance on Article 51 of the United Nations Charter, which recognizes that nations have an inherent right of self-defense:

> *Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in exercise of this right of self-defense shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.*

The right of the United States to defend itself against armed attack has been the focus of some of the recent debate as the United States considers its options in responding to the terrorist attacks of September 11, 2001.[1995]

In the process of rewriting the U.S. Army Field Manual 27-10, The Law of War, a "Memorandum of Law: EO 12333 and Assassination" (hereinafter Memorandum of Law 27-1a) was prepared to explain the term "assassination" in the context of military operations. In Memorandum of Law 27-1a, it is suggested that, in time of peace, an element of covert action or surprise attack may be required for a killing for political purposes to be deemed an assassination, particularly where the target is a private individual rather than a public figure or national leader. The murder for political purposes of a national leader in time of peace may be regarded by some as an assassination solely because of the target, while others might also consider whether a surprise attack was involved.

> *For example, the 1978 "poisoned-tip umbrella" killing of Bulgarian defector Georgi Markov by Bulgarian State Security agents on the streets of London falls into the category of an act of murder carried out for political purposes, and constitutes an assassination. In contrast, the murder of Leon Klinghoffer, a private citizen, by the terrorist Abu el Abbas during the 1985 hijacking of the Italian cruise ship Achille Lauro, though an act of murder for political purposes, would not constitute an assassination. The distinction lies not merely in the purpose of the*

[1995] For a brief review of legal issues and authorities regarding the use of military force to respond to terrorist attacks, see CRS Report RS21009, Response to Terrorism: Legal Aspects of the Use of Military Force.. Cf., Stuart G. Baker, "Comparing the 1993 U.S. Airstrike on Iraq to the 1986 Bombing of Libya: The New Interpretation of Article 51," 24 Ga. J. Int'l & Comp. L. 99 (1994).

> *act and/or its intended victim, but also under certain circumstances in its covert nature. Finally, the killing of Martin Luther King and Presidents Abraham Lincoln, James A. Garfield, William McKinley and John F. Kennedy generally are regarded as assassination because each involved the murder of a public figure or national leader for political purposes accomplished through a surprise attack.*[1996]

In time of war, assassination appears to be distinguished in some discussions from cases of lawful killing, because the former is carried out in a "treacherous" manner.[1997] "Treacherous" is not defined in the Hague Convention IV, but does not appear to be interpreted to foreclose operations in time of war involving the element of surprise.[1998] However, putting a price on the head of an enemy appears to be regarded by some as an act which would render a resulting killing an assassination, as distinguished from a lawful attack on legitimate military targets, including the enemy chain of command.[1999] A review of historical discussions of assassination suggests that this may be, in part, because by putting a price on the head of an enemy, one could be encouraging treachery by those close to the target.[2000]

[1996] W. Hays Parks, "Memorandum of Law: Executive Order 12333 and Assassination,"DAJA-IA (271a), The Army Lawyer 4 (Dec. 1989).

[1997] See, Article 23(b) of the Annex to the Hague Regulations (Hague Convention IV) (1907).

[1998] Memorandum of Law 27-1a, The Army Lawyer 4, 5 (Dec. 1989).

[1999] See, e.g., U.S. Army General Orders no. 100, paragraph 148 (1863); Article 23b, Annex to Hague Convention IV (1907); U.S. Army Field Manual 27-10, paragraph 31 (The Law of Land Warfare) (1956), cited in Memorandum of Law 27-1a, at 5.

[2000] Lt. Commander Patricia Zengel, "Assassination and the Law of Armed Conflict," 134 Mil. L. Rev. 123, 127 (1991) (discussing the views of Hugo Grotius from De Jure Belli Ae Pacis Libri Tres (rev. ed. 1646); for further discussion, see Daniel B. Pickard, "Legalizing Assassination: Terrorism, the Central Intelligence Agency and International Law," 30 Ga. J. Int'l & Comp. L. 1 (2001); Thomas C. Wingfield, "Taking Aim at Regime Elites: Assassination, Tyrannicide, and the Clancy Doctrine," 22 Md. J. Int'l L. & Trade 287 (1999). Cf., "The Legality of Assassination of Independent Terrorist Leaders: An Examination of National and International Implications," 24 N.C.J. Int'l Law & Com. Reg. 669 (1999); Robert F. Turner, "Symposium: Legal Responses to International Terrorism: Constitutional Constraints on Presidential Power," 22 Houston J. Int'l L. 77 (1999); Boyd M. Johnson, III, "Executive Order 12,333: The Permissibility of an American Assassination of a Foreign Leader," 25 Cornell Int'l L.J. 401 (1992); Abraham D. Sofaer, "The Sixth Annual Waldemar A. Solf Lecture in International Law: Terrorism, the Law, and the National Defense," 126 Mil. L. Rev. 89 (1989).

Can the President revoke the assassination ban in E.O. 12333?

As it is part of an executive order, the President may modify or rescind the assassination ban in E.O. 12333, Section 2.11, by executive order. Except in specific circumstances, an executive order revoking a previous order would have to be published in the Federal Register under 44 U.S.C. § 1505(a) if it is deemed to be an order of general applicability. However, under 44 U.S.C. § 1505(c):

In the event of an attack or threatened attack upon the continental United States and a determination by the President that as a result of an attack or threatened attack–

(1) publication of the Federal Register or filing of documents with the Office of the Federal Register is impracticable, or
(2) under existing conditions publication in the Federal Register would not serve to give appropriate notice to the public of the contents of documents, the President may, without regard to any other provision of law, suspend all or part of the requirements of law or regulation for filing with the Office or publication in the Federal Register of documents or classes of documents. Such a suspension would remain in effect until revoked by the President or by concurrent resolution of Congress.

Can Congress revoke the assassination ban in E.O. 12333?

To the extent that an executive order relies upon statutory authority, Congress may also legislate to modify or repeal it. In issuing E.O. 12333, President Reagan relied upon the authority vested in him "by the Constitution and statutes of the United States of America, including the National Security Act of 1947, as amended, and as President of the United States of America, in order to provide for the effective conduct of United States intelligence activities and the protection of constitutional rights." While there is no express parallel to E.O. 12333's assassination ban in federal statutes, there is a provision in 18 U.S.C. § 1116 which provides criminal penalties for murder, manslaughter, or attempted murder or manslaughter of foreign officials, official guests, or internationally protected persons.[2001] This section applies to murder, manslaughter, or attempted murder or manslaughter committed within the United States. In addition, the U.S. may exercise jurisdiction over such acts committed against internationally protected persons outside the United States if "(1) the victim is a representative, officer, employee, or agent of the United States, (2) an offender is a national of the

[2001] Cf., "Prevention and Punishment of Crimes against Internationally Protected Persons, Including Diplomatic Agents," 28 U.S.T. 1975, TIAS 8532;, signed on behalf of the United States on Dec. 28, 1973; ratified by the U.S. Senate on Oct. 28, 1975; entered into force on Feb. 20, 1977.

United States, or (3) an offender is afterwards found in the United States."[2002] "Internationally protected person" is defined to mean "a Chief of State or the political equivalent, head of government, or Foreign Minister whenever such person is in a country other than his own and any member of his family accompanying him;" or "any other representative, officer, employee, or agent of the United States Government, a foreign government, or international organization who at the time and place concerned is entitled pursuant to international law to special protection against attack upon his person, freedom, or dignity, and any member of his family then forming part of his household."[2003] "International organization" is defined to mean "a public international organization designated as such pursuant to section 1 of the International Organizations Immunities Act (22 U.S.C. 288) or a public organization created pursuant to treaty or other agreement under international law as an instrument through or by which two or more foreign governments engage in some aspect of their conduct of international affairs."[2004] "International organization" does not appear to encompass terrorist organizations or networks, nor does "internationally protected person" appear to reach the leaders of such organizations or networks. The earliest version of this provision was first added in 1972, P.L. 92-539, Title I, Section 101 (Oct. 24, 1972), 86 Stat. 1071, which predates the Ford executive order. However, it was not referenced by President Ford in his Special Message to Congress accompanying issuance of E.O. 11905. Repeal or modification of 18 U.S.C. § 1116 would not necessarily have any clear bearing on the scope of the assassination ban in E.O. 12333. On the other hand, recent joint resolutions of Congress, discussed presently, may pertain.

Role of Congress/Legislation

On Friday, September 14, 2001, both the House and the Senate passed joint resolutions, S.J.Res. 23 and H.J.Res. 64, authorizing the President to "use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks that occurred on September 11, 2001, or harbored such organizations or persons, in order to prevent any future acts of international terrorism against the United

---

[2002] 18 U.S.C. § 1116(c).

[2003] 18 U.S.C. § 1116(b)(4).

[2004] 18 U.S.C. § 1116(b)(5). 22 U.S.C. § 288 defines "international organization" to mean:

. . . a public international organization in which the United States participates pursuant to any treaty or under the authority of any Act of Congress authorizing such participation or making an appropriation for such participation, and which shall have been designated by the President through appropriate Executive order as being entitled to enjoy the privileges, exemptions, and immunities provided in this subchapter. . . .

For a list of those organizations so designated, see 22 U.S.C. § 288 note.

States by such nations, organizations or persons."[2005] In addition, the "Congress declares that this section is intended to constitute specific statutory authorization within the meaning of section 5(b) of the War Powers Resolution."[2006] S. J. Res 23 was signed by the President, and became P.L. 107-40, 115 Stat. 224 (Sept. 18, 2001). This law makes no explicit reference to the assassination ban in E.O. 12333, section 2.11. However, if the assassination ban were to be interpreted to cover U.S. responses to terrorist attacks on U.S. soil, the breadth of the authority provided by these joint resolutions might be viewed as sufficient, insofar as U.S. responses to the events of September 11, 2001 are concerned, to encompass actions that might otherwise be prohibited under the assassination ban. Other legislation has been introduced to expressly revoke the express prohibition against assassination in the Ford, Carter, and Reagan executive orders. See, e.g., H.R. 19 (introduced 1/3/01 and referred to House Committee on International Relations).

[2005] Sec. 2(a).

[2006] Sec. 2(b)(1).

18 U.S.C. Chapter 67: Military and Navy (18 U.S.C. §§ 1381-1389)

The Posse Comitatus Act (18 U.S.C. § 1385)

The Posse Comitatus Act and Related Matters: A Sketch, RS20590 (June 6, 2005).

JENNIFER ELSEA, CONGRESSIONAL RESEARCH SERV., THE POSSE COMITATUS ACT AND RELATED MATTERS: A SKETCH (2005), , *available at* http://www.intelligencelaw.com/library/secondary/crs/pdf/RS20590_6-6-2005.pdf.

Order Code RS20590
Updated June 6, 2005

Jennifer Elsea
Legislative Attorney
American Law Division

Summary

The Posse Comitatus Act states that: Whoever, except in cases and under circumstances expressly authorized by the Constitution or Act of Congress, willfully uses any part of the Army or the Air Force as a posse comitatus or otherwise to execute the laws shall be fined under this title or imprisoned not more than two years, or both. 18 U.S.C. § 1385. It reflects an American tradition that bridles at military involvement in civilian affairs. Congress, however, has approved a number of instances where extraordinary circumstances warrant a departure from the general rule, particularly in cases where the armed forces provide civilian assistance without becoming directly involved in civilian law enforcement. This is an abridged version of The Posse Comitatus Act and Related Matters: The Use of the Military to Execute Civilian Law, CRS Report 95-964 in which the authorities for the statements made here may be found. This report summarizes proposed bills that could result in increased interaction between military and civil authorities. (H.R. 1986, H.R. 1815, S. 1042, S. 1043).

Introduction

The Posse Comitatus Act, 18 U.S.C. § 1385, is perhaps the most tangible expression of an American tradition , born in England and developed in the early years of our nation, that rebels against military involvement in civilian affairs. The Declaration of Independence listed among our grievances against Great Britain that the King had "kept among us, in times of peace, Standing Armies without the consent of our legislatures," had "affected to render the Military independent of and superior to the civil power." The Articles of Confederation addressed the threat of military intrusion into civilian affairs by demanding that the armed forces assembled during peacetime be no more numerous than absolutely necessary for the common defense, and by entrusting control to civil authorities within the states. The Constitution continued the theme. It provided that a civilian, the President, should be the Commander in Chief of the Army and Navy of the United States and that civilian authorities, the Congress, should be solely empowered to raise and support Armies, provide and maintain a Navy, and make rules for their government and regulation. The Bill of Rights limited the quartering of troops in private homes, U.S. Const. Amend. III, and noted that "a well regulated Militia, being necessary to the security of a free State, the right of the people to keep and bear Arms, shall not be infringed," U.S. Const. Amend. II. The Constitution, on the other hand, explicitly permitted the Congress to provide for calling out the militia to execute the laws, suppress insurrection, and repel invasion, U.S. Const. Art. I, § 8, cl.16. Soon after Congress was first assembled under the Constitution, it authorized the President to call out the militia, initially to protect the frontier against " hostile incursions of the Indians," and subsequently in cases of invasion, insurrection, or obstruction of the laws. The President's authority to call upon the state militia to aid in putting down insurrections is reminiscent of the authority enjoyed by the sheriff at common law to call upon the posse comitatus. In the beginning the two were comparable but unrelated. Even though Congress empowered the President to call out the militia to overcome obstructions to law enforcement, it continued to vest the federal equivalent of the sheriff, the federal marshal, with the power to call forth the posse comitatus in performance of his duties.

Congress in some cases specifically authorized recourse to the posse comitatus for the enforcement of particular statutes. Under the Fugitive Slave Act, for instance, owners whose slaves had escaped to another state were entitled to an arrest warrant for the slaves and to have the warrant executed by federal marshals. The marshals in turn might " summon and call to their aid the bystanders, or posse comitatus of the proper county . . . [and] all good citizens [were] commanded to aid and assist in the prompt and efficient execution of this law, whenever their services may be required, as aforesaid, for that purpose," 9 Stat. 462, 463 (1850). Attorney General Caleb Cushing declared that the " bystanders" contemplated by the Fugitive Slave Act might include members of a state militia even when not in federal service, and in fact encompassed members of the armed forces by virtue of their duties as citizens as part of the posse comitatus.

Following the Civil War, the use of federal troops to execute the laws, particularly in the states that had been part of the Confederacy, continued even after all other political restrictions had been lifted. The Posse Comitatus Act was passed as part of an Army appropriations bill in response. With exception of a reference to the Air Force, it has remained essentially unchanged ever since, although Congress has authorized a substantial number of exceptions and has buttressed the Act with an additional proscription against use of the armed forces to make arrests or conduct searches and seizures. While the war against terrorism has led some to call for a reexamination of the role of the military in domestic law enforcement, Congress, in establishing the Department of Homeland Security, expressed its sense reaffirming the continued importance and applicability of the Posse Comitatus Act. 6 U.S.C. § 466.

When the Act Does Not Apply

Constitutional Exceptions: The Posse Comitatus Act does not apply " in cases and under circumstances expressly authorized by the Constitution," 18 U.S.C. § 1385. It has been observed that the Constitution contains no provision expressly authorizing the use of the military to execute the law, that the exception was included as part of a face-saving compromise, and that consequently it should be ignored.

The older commentaries suggest that the word " expressly" must be ignored, for otherwise in their view the Posse Comitatus Act is a constitutionally impermissible effort to limit the powers of the President. The regulations covering the use of the armed forces during civil disturbances do not go quite that far, but they do assert two constitutionally based exceptions – sudden emergencies and protection of federal property. The question of whether the constitutional exception includes instances where the President is acting under implied or inherent constitutional powers is one the courts have yet to answer.

Statutory Exceptions—Generally

The Posse Comitatus Act does not apply where Congress has expressly authorized use of the military to execute the law. Congress has done so in three ways, by giving a branch of the armed forces civilian law enforcement authority, by establishing general rules for certain types of assistance, and by addressing individual cases and circumstances with more narrowly crafted legislation. Thus it has vested the Coast Guard, a branch of the armed forces, with broad law enforcement responsibilities. Second, over the years it has passed a fairly extensive array of particularized statutes, like those permitting the President to call out the armed forces in times of insurrection and domestic violence, 10 U.S.C. §§ 331-335. Finally, it has enacted general legislation authorizing the armed forces to share information and equipment with civilian law enforcement agencies, 10 U.S.C. §§ 371-382.

These last general statutes were crafted to resolve questions raised by the so-called Wounded Knee cases (see below). The legislation contains both explicit grants of authority and restrictions on the use of that authority for military assistance to the police – federal, state and local – particularly in the form of information and equipment, 10 U.S.C. §§ 371-382. Section 371 specifically authorizes the armed forces to share information acquired during military operations and in fact encourages the armed forces to plan their activities with an eye to the production of incidental civilian benefits. The section allows the use of military undercover agents and the collection of intelligence concerning civilian activities only where there is a nexus to an underlying military purpose. Under sections 372 through 374, military equipment and facilities may be made available to civilian authorities; members of the armed forces may train civilian police on the operation and maintenance of equipment and mayprovide them with expert advice; and military personnel may be employed to maintain and operate the equipment supplied. The authority granted in sections 371-382 is subject to three general caveats. It may not be used in any way that could undermine the military capability of the United States; the civilian beneficiaries of military aid must pay for the assistance; and the Secretary of Defense must issue regulations to ensure that the authority of sections 371 to 382 does not result in use of the armed forces to make arrests or conduct searches and seizures solely for the benefit of civilian law enforcement.

Military Purpose

The armed forces, when in performance of their military responsibilities, are beyond the reach of the Posse Comitatus Act and its statutory and regulatory supplements. Neither the Act nor its legislative history resolves the question of whether the Act prohibits the Army from performing its military duties in a manner which affords incidental benefits to civilian law enforcement officers. The courts and commentators believe that it does not. As long as the primary purpose of an activity is to address a military purpose, the activity need not be abandoned simply because it also assists civilian law enforcement efforts.

Willfully Execute the Laws

The Act is limited to " willful" misuse of the Army or Air Force. The Senate version of the original Act would have limited proscription to " willful and knowing" violations, 7 Cong. Rec. 4302 (1878); the House version had no limitation, 7 Cong. Rec. 4181 (1878). The compromise which emerged from conference opted to forbid only willful violations, but nothing in the legislative history explains what the limitation means. It seems unlikely that a court would convict for anything less than a deliberate disregard of the law's requirements.

When has the Army or Air Force been used " to execute the laws" ? Existing case law and commentary indicate that " execution of the law" in violation of the Posse Comitatus Act occurs (a) when the armed forces perform tasks ordinarily assigned not to them but to an organ of civil government, or (b) when the armed

forces perform tasks assigned to them solely for purposes of civilian government. While inquiries may surface in other contexts, such as the use of the armed forces to fight forest fires or to provide assistance in the case of other natural disasters, Posse Comitatus Act questions arise most often when the armed forces assist civilian police.

The tests used by most contemporary courts to determine whether military forces have been used improperly as police forces in violation of the Posse Comitatus Act were developed out of disturbances in 1973 at Wounded Knee on the Pine Ridge Indian Reservation in South Dakota and inquire: (1) whether civilian law enforcement officials made a direct active use of military investigators to execute the law; (2) whether the use of the military pervaded the activities of the civilian officials; or (3) whether the military was used so as to subject citizens to the exercise of military power which was regulatory, prescriptive, or compulsory in nature.

Military Coverage

Navy and Marines

The Posse Comitatus Act proscribes use of the Army or the Air Force to execute the law. It says nothing about the Navy, the Marine Corps, the Coast Guard, or the National Guard. The courts have generally held that the Posse Comitatus Act by itself does not apply to the Navy or the Marine Corps. They maintain, however, that those forces are covered by similarly confining administrative and legislative supplements, which appear in the Department of Defense (DoD) Directive.

Coast Guard

The Posse Comitatus Act likewise says nothing about the Coast Guard. The Coast Guard is a branch of the armed forces, located within the Department of Homeland Security, 14 U.S.C. § 1 (as amended), but relocated within the Navy in time of war or upon the order of the President, 14 U.S.C. § 3. The Act will apply to the Coast Guard while it remains part of the Department of Homeland Security. While part of the Navy, it is subject to the orders of the Secretary of the Navy, 14 U.S.C. § 3, and consequently to any generally applicable directives or instructions issued under the Department of Defense or the Navy. As a practical matter, however, the Coast Guard is statutorily authorized to perform law enforcement functions, 14 U.S.C. § 2. Even while part of the Navy its law enforcement activities would come within the statutory exception to the posse comitatus restrictions, and the restrictions applicable to components of the Department of Defense would only apply to activities beyond those authorized.

National Guard

The Act is silent as to what constitutes " part" of the Army or Air Force for purposes of proscription. There is little commentary or case law to resolve questions concerning the coverage of the National Guard, the Civil Air Patrol,

civilian employees of the armed forces, or regular members of the armed forces while off duty.

Strictly speaking, the Posse Comitatus Act predates the National Guard onlyin name for the Guard " is the modern Militia reserved to the States by Art. I, § 8, cls.15, 16, of the Constitution" which has become " an organized force, capable of being assimilated with ease into the regular military establishment of the United States," Maryland v. United States, 381 U.S. 41, 46 (1965). There seems every reason to consider the National Guard part of the Army or Air Force, for purposes of the Posse Comitatus Act, when in federal service. When not in federal service, historical reflection might suggest that it is likewise covered. Recall that it was the state militia, called to the aid of the marshal enforcing the Fugitive Slave Act, which triggered Attorney General Cushing's famous opinion. The Posse Comitatus Act's reference to " posse comitatus or otherwise" is meant to abrogate the assertion derived from Cushing's opinion that troops could be used to execute the law as long as they were acting as citizens and not soldiers when they did so.

On the other hand, the National Guard is creature of both state and federal law, a condition which as the militia it has enjoyed since the days of the Articles of Confederation. Courts have held that members of the National Guard when not in federal service are not covered by the Posse Comitatus Act. Similarly, the DoD directive is only applicable to members of the National Guard when they are in federal service.

Off Duty, Acting as Citizens and Civilian Employees

The historical perspective fares little better on the question of whether the Posse Comitatus Act extends to soldiers who assist civilian law enforcement officials in a manner which any other citizen would be permitted to provide assistance, particularly if they do so while off duty. Congress passed the Act in response to cases where members of the military had been used based on their civic obligations to respond to the call as the posse comitatus. The debate in the Senate, however, suggests that the Act was not intended to strip service members of all civilian rights and obligations. The more recent decisions have focused on the nature of the assistance provided and whether it is incidental to action taken primarily for a military purpose.

Some have questioned whether civilian employees of the armed forces should come within the proscription of the Act, but most, frequently without comment, seem to consider them " part" of the armed forces for purposes of the Posse Comitatus Act. The current DoD directive expressly includes civilian employees " under the direct command and control of a military officer" within its Posse Comitatus Act policy restrictions.

Geographical Application

The Posse Comitatus Act contains no expression of extraterritorial application, but it seems unlikely that it was meant to apply beyond the confines of the United

States, its territories and possessions. Congress enacted it in response to problems occurring within the United States and its territories, problems associated with the American political process and policies and actions that promoted military usurpation of civilian law enforcement responsibilities over Americans. Congress does appear to have intended the authority and restrictions contained in 10 U.S.C. §§ 371-382 to apply both in the United States and beyond its borders.

Consequences of Violation

Prosecution

The Posse Comitatus Act is a criminal statute under which there has apparently never been a prosecution. It has been invoked with varying degrees of success, however, to challenge the jurisdiction of the courts, as a defense in criminal prosecutions for other offenses, as a ground for the suppression of evidence, as the grounds for, or a defense against, civil liability, and as a means to enjoin proposed actions by the military.

Exclusion of Evidence

Allegations that the Posse Comitatus Act has been violated are made most often by defendants seeking to exclude related testimony or physical evidence, but most cases note the absence of an exclusionary rule, often avoiding unnecessary analysis of the scope of the Act and whether a violation has occurred.

Jurisdiction and Criminal Defenses

Defendants have found the Act helpful in prosecutions where the government must establish the lawfulness of its conduct as one of the elements of the offense. Several defendants at Wounded Knee persuaded the court that evidence of possible violations precluded their convictions for obstructing law enforcement officials " lawfully engaged" in the performance of their duties.

Civil Liability

The Eighth Circuit has declared that a violation of the Act might constitute an unreasonable search and seizure for purposes of the Fourth Amendment, giving rise to a Bivens cause of action against offending federal officers or employees.

Compliance

The most significant impact of the Posse Comitatus Act is attributable to compliance by the armed forces. As administrative adoption of the Act for the Navy and Marines demonstrates, the military has a long standing practice of avoiding involvement in civilian affairs which it believes are contrary to the Act, and which date back to military acceptance of civilian authority since the founding of the Republic.

Proposed New Exceptions

H.R. 1986 would amend title 10 to allow the Secretary of Defense to provide military personnel to assist the Department of Homeland Security when necessary to respond to " a threat to national security posed by the entry into the United States of terrorists, drug traffickers, or illegal aliens." Specially trained service members could be assigned to assist the Bureau of Border Security and the U.S. Customs Service, but would not be authorized to carry out searches, seizures, or other similar law enforcement activities. The Secretary would be empowered to establish ongoing joint task forces to carry out these activities. Military members would first have to undergo training in issues related to law enforcement in border areas and would have to be accompanied by civilian law enforcement officers. H.R. 1986 passed the House as section 1035 of the National Defense Authorization Act for FY2006 (H.R. 1815), but without a limitation that would have ended the authority after September 30, 2007.

S. 1042 and S. 1043, the Senate Defense authorization bills, would add a new section 383 to title 10, which would authorize the Secretary of Defense to use unmanned aerial vehicles and DoD personnel to conduct aerial reconnaissance within U.S. Northern Command' s area of responsibility, in order to monitor air and sea traffic along the border and coastline, and to communicate resulting information to the appropriate federal, state, and local law enforcement officials. The activity would be funded from counterdrug appropriations. The prohibitions against military personnel participating in searches, seizures, or arrests would apply.

The Posse Comitatus Act and Related Matters: The Use of the Military to Execute Civilian Law, 95-964 S (June 1, 2000).

CHARLES DOYLE, CONGRESSIONAL RESEARCH SERV., THE POSSE COMITATUS ACT AND RELATED MATTERS: THE USE OF THE MILITARY TO EXECUTE CIVILIAN LAW (2000), *available at* http://www.intelligencelaw.com/library/secondary/crs/pdf/95-964_6-1-2010.pdf.

Updated June 1, 2000

Charles Doyle
Senior Specialist
American Public Law

Summary

The Posse Comitatus Act outlaws willful use of any part of the Army or Air Force to execute the law unless expressly authorized by the Constitution or an Act of Congress. History supplies the grist for an argument that the Constitution prohibits military involvement in civilian affairs subject to only limited alterations by Congress or the President, but the courts do not appear to have ever accepted the argument unless violation of more explicit constitutional command could also be shown. The provision for express constitutional authorization when in fact the Constitution contains no such express authorizations has been explained alternatively as a meaningless political face saving device or as an unartful reference to the President's constitutional powers. The express statutory exceptions include the legislation which allows the President to use military force to suppression insurrection, 10 U.S.C. 331-335, and sections which permit the Department of Defense to provide federal, state and local police with information and equipment, 10 U.S.C. 371-381.

Existing case law indicates that "execution of the law" in violation of the Posse Comitatus Act occurs (a) when the armed forces perform tasks which are assigned not to them but to an organ of civil government, or (b) when the armed forces perform tasks assigned to them solely for purposes of civilian government. Questions arise most often in the context of assistance to civilian police. At least in this context, the courts have held that, absent a recognized exception, the Posse Comitatus Act is violated, (1) when civilian law enforcement officials make "direct active use" of military investigators; or (2) when the use of the military "pervades the activities" of the civilian officials; or (3) when the military is used so as to subject "citizens to the exercise of military power which was regulatory, prescriptive, or compulsory in nature." The Act is not violated when the armed forces conduct activities for a military purpose which have incidental benefits for civilian law enforcement officials.

The language of the Act mentions only the Army and the Air Force, but it is applicable to the Navy and Marines by virtue of administrative action and commands of other laws. The law enforcement functions of the Coast Guard have been expressly authorized by act of Congress and consequently cannot be said to be contrary to the Act. The Act has been applied to the National Guard when it is in federal service, to civilian employees of the armed forces, and to off-duty military personnel.

The Act is probably only applicable within the geographical confines of the United States, but the supplemental provisions of 10 U.S.C. 371-381 appear to apply world-wide. Finally, the Act is a criminal statute under which there has never been a prosecution. Although violations will on rare occasions result in the exclusion of evidence, the dismissal of criminal charges, or a civil cause of action, as a practical matter compliance is ordinarily the result of military self-restraint. This report appears in abridged form as CRS Report RS20590, *The Posse Comitatus Act: A Sketch*.

Introduction

> *Whoever, except in cases and under circumstances expressly authorized by the Constitution or Act of Congress, willfully uses any part of the Army or the Air Force as a posse comitatus or otherwise to execute the laws shall be fined under this title or imprisoned not more than two years, or both. 18 U.S.C. 1385.*

Americans have a tradition, born in England and developed in the early years of our nation, that rebels against military involvement in civilian affairs. It finds its most tangible expression in the nineteenth century Posse Comitatus Act, 18 U.S.C. 1385. The Act forbids use of the Army and Air Force to execute civil law except where expressly authorized.

The exception documents a contrary component of the tradition. It accepts the use of the armed forces in extraordinary circumstances if expressly approved by Congress. Striking the balance between rule and exception has never been easy, but failure to do so has often proven unfortunate. When the rule is too unforgiving, a Shays's Rebellion may go unchecked. When exceptions are too generously granted, a Boston Massacre or Kent State tragedy may follow.

Several times in the recent past, concerns that civil authorities may be overwhelmed by threats of natural disasters, civil disturbances, drug trafficking, and terrorism have produced calls for more generous exceptions to the rule. Some of those calls have been answered, others have not. This is an effort to sketch the current state of the law.

Background

The Magna Carta gives us the first recorded acknowledgment of the origins of the Anglo-American tradition against military involvement in civilian affairs with its declaration that "no free man shall be . . . imprisoned . . . or in any other way destroyed . . . except by the legal judgment of his peers or by the law of the land."[2007] Subsequent legislation in the reign of Edward III explained that this precluded punishment by the King except "in due Manner . . . or by Process made by Writ. . . [or] by Course of the Law,"[2008] or as later more simply stated, except "by due Process of the Law."[2009] Three hundred years after the passage of the Edwardian statutes, Lord Coke and other members of Parliament read these due process and law of the land requirements to include a broad prohibition against the use of martial law in peacetime, an interpretation they compelled King Charles I to acknowledge.[2010]

[2007] Magna Carta, ch. 39 (1225)[ch.29 in the Charter of King John (1215)], reprinted in SWINDLER, MAGNA CARTA: LEGEND AND LEGACY 315-16 (1965)("No freeman shall be taken, or imprisoned, or be disseised of any freehold, or liberties, or free customs, or outlawed, or banished, or in any other way destroyed, nor will we go or send against him, except by the lawful judgment of his peers or by the law of the land" (language added to ch.29 of the Charter of King John in the reissuance by King Henry III appears in italics). Although the Magna Carta in the modified version of King Henry remains in effect, the language quoted above is generally cited as "chapter 29," see e.g., THOMPSON, MAGNA CARTA: ITS ROLE IN THE MAKING OF THE ENGLISH CONSTITUTION 1300-1629 68 (1948); HALE, THE HISTORY OF THE COMMON LAW OF ENGLAND 49 (1716 ed.); I COKE, THE SECOND PART OF THE INSTITUTES OF THE LAWS OF ENGLAND 45 (1797 ed.); I BLACKSTONE, COMMENTARIES ON THE LAWS OF ENGLAND 400 (1765 ed.).

[2008] 25 Ed.III. Stat.5, ch.4 (1352), reprinted in, 1 STATUTES OF THE REALM, 1231-1377 321 (1993)("Whereas it is contained in the Great Charter of the Franchises of England, that none shall be imprisoned nor put out of his Freehold, nor of his Franchises nor free Custom, unless it be by the Law of the Land; It is accorded assented, and established, That from henceforth none shall be taken by Petition or Suggestion made to our Lord the King, or to his Council, unless it be by Indictment or Presentment of good and lawful People of the same neighbourhood where such Deeds be done, in due Manner, or by Process made by Writ original at the Common Law; nor that none be out of his Franchises, nor of his freeholds, unless he be duly brought into answer, and forejudged of the same by the Course of the Law; and if any thing be done against the same, it shall be redressed and holden for none").

[2009] 28 Ed.III. chs. 1, 3 (1354), reprinted in 1 STATUTES OF THE REALM, 1231-1377 345 (1993)("the Great Charter . . . [shall] be kept and maintained in all Points. . . . No Man of what[ever] Estate or Condition that he be, shall be put out of land or Tenement, nor taken, nor imprisoned, nor disinherited, nor put to Death, without being brought in Answer by due Process of the Law").

[2010] See, THOMPSON, MAGNA CARTA: ITS ROLE IN THE MAKING OF THE ENGLISH CONSTITUTION, 1300-1629, 347-50 (1948); Engdahl, Soldiers, Riots, and Revolution: The Law and History of Military Troops in Civil Disorders 51 IOWA LAW REVIEW 1 (1971). Coke's Institutes make the same point; proceedings under martial law are not proceedings under the "law of the land" (lex terrae), I COKE, THE SECOND PART OF THE INSTITUTES OF THE LAWS OF ENGLAND 50 ("And so if two English men doe goe into a foreine kingdome, and fight there, and the one murder the other, lex terrae extendeth not hereunto, but this offense shall be heard,

King Charles I, preparing for a military expedition in France, had quartered his troops in homes along the southern English coastline.[2011] Rioting resulted, and the participants, both military and civilian, were tried and punished by commissioners operating under the authority of martial law. Offended by this peacetime exercise of military judicial authority over civilians, Parliament sought and was granted the Petition of Right of 1628 which outlawed both quartering and martial law commissions.[2012]

---

and determined before the constable, and marshall [i.e. at martial law], and such proceedings shall be there, by attaching of the body, and otherwise, as the law, and custom of that court have been allowed by the lawes of the realme, [13 H.IV. ch.5 (1412)]").

[2011] For a more expansive examination, see Engdahl, Soldiers, Riots, and Revolution: The Law and History of Military Troops in Civil Disorders 51 IOWA LAW REVIEW 1 (1971).

[2012] "And whereas also by the statute called `The Greater Charter of the liberties of England,'[the Magna Carta] it is declared and enacted, that no freeman may be taken or imprisoned or be disseised of his freehold or liberties, or his free customs, or be outlawed or exiled, or in any manner destroyed, but by the lawful judgment of his peers, or by the law of the land. And in the eight-and-twentieth year of the reign of King Edward III, it was declared and enacted by authority of parliament, that no man, of what estate or condition that he be, should be put out of his land or tenements, nor taken, nor imprisoned, nor disinherited, nor put to death without being brought to answer by due process of law. . . . [N]everthess of late time divers commissions under your Majesty's great seal have issued forth, by which certain persons have been assigned and appointed commissioners with power and authority to proceed within the land, according to the justice of martial law, against such soldiers or mariners, or other dissolute persons joining with them, as should commit any murder, robbery, felony, mutiny, or other outrage or misdemeanour whatsoever, and by such summary course and order as is agreeable to martial law, and as is used in armies in time of war, to proceed to the trial and condemnation of such offenders, and them to cause to be executed and put to death according to the law martial . . . . They do therefore humbly pray your most excellent Majesty . . . that your Majesty would be pleased to remove the said soldiers and mariners, and that your people may not be so burdened in time to come; and that the aforesaid commissions, for proceeding by martial law, may be revoked and annulled; and that hereafter no commissions of like nature may issue forth to any person or persons whatsoever to be executed as aforesaid, lest by colour of them any of your Majesty's subjects be destroyed or put to death contrary to the laws and franchise of the land. Petition of Right, 3 Car.I, c.1, §§3, 4, 7, 10, reprinted in STUBBS, SELECT CHARTERS AND OTHER ILLUSTRATIONS OF ENGLISH CONSTITUTIONAL HISTORY FROM THE EARLIEST TIMES TO THE REIGN OF EDWARD THE FIRST 515-17 (8th ed. 1895); and in 5 STATUTES OF THE REALM 23, 24 (1993). See also, HALE, HISTORY OF THE COMMON LAW OF ENGLAND 39-40 (2d ed. 1716)("But touching the business of martial law, these things are to be observed, First, That in truth and reality it is not a law, but something indulged rather than allowed as a law; the necessity of government, order and discipline in an army, is that only which can give those laws a countenance. Secondly, This indulged law was only to extend to members of the army, or to those of the opposite army, and never was so much indulged as intended to be (executed or) exercised upon others; for others were not listed under the army, had no colour of reason to be bound by military constitutions, applicable only to the army; whereof they were not parts, but they were to be ordered and governed according to the laws to which they were subject, though it were a time of war. Thirdly, That the exercise of martial law, whereby any person should lose his life or member, or liberty, may not be permitted in time of peace, when the King's courts are open for all persons to receive justice, according to the laws of the land. This is the substance declared by Petition of Right, 3 Car. I. whereby such commissions and martial law were repealed and declared to be contrary to

When, in the following century, the British responded to colonial unrest by quartering troops in Boston, the colonists saw it as a breach of this fundamental promise of English law. Their circumstances, however, were not exactly identical to those surrounding the Petition of Right. First, the question arose in the colonies. England had stationed troops in the colonies to protect them against the French and Indians and had opted for military governorships in other territories. Second, there was no military usurpation of judicial functions. The colonists remained subject to civil rather than military justice, and soldiers who employed more force than civilian law permitted were themselves subject to civilian justice as the trials of the soldiers involved in the Boston Massacre demonstrates.

On the other hand, the troops involved in the Boston Massacre were stationed in Massachusetts not for protection against a marauding invader as they had been in the French and Indian Wars, not to accomplish the transition between civil governments within a conquered territory as they had been after the French lost Canada to the British as a consequence of those conflicts, but as an independent military force quartered among a disgruntled civilian population to police it.[2013]

---

law"); I BLACKSTONE, COMMENTARIES ON THE LAWS OF ENGLAND 400 (1765)("For martial law, which is build upon no settled principles, but is entirely arbitrary in its decisions, is, as Sir Matthew Hale observes, in truth and reality no law, but something indulged, rather than allowed as a law; the necessity of order and discipline in an army is the only thing which can give it countenance; and therefore it ought not to be permitted in time of peace, when the king's courts are open for all persons to receive justice according to the laws of the land. . . . And it is laid down, that if a lieutenant, or other, that hath commission of martial authority, doth in time of peace hang or otherwise execute any one by colour of martial law, this is murder; for it is against the magna carta. And the petition of right enacts, that no soldier shall be quartered on the subject without his own consent; and that no commission shall issue to proceed within this land according to martial law. And whereas, after the restoration, king Charles the second kept up about five thousand regular troops, by his own authority, for guards and garrisons; which king James the second by degrees increased to no less than thirty thousand, all paid from his own civil list; it was made one of the articles of the bill of rights, that the raising or keeping of a standing army within the kingdom in time of peace, unless it be with the consent of the parliament, is against the law").

[2013] ZOBEL, THE BOSTON MASSACRE 135 (1987) ("The soldiers, one ought always to remember, went into Boston not as an occupying army but rather as a force of uniformed peace-keepers, or policemen. Their role as even the radicals conceived it was to assist the executive and if necessary the courts to maintain order"); Engdahl, Soldiers, Riots, and Revolution: The Law and History of Military Troops in Civil Disorders, 57 IOWA LAW REVIEW 1,24-5 (1971) ("The last die was cast when two regiments of troops were quartered in Boston at the end of the decade. Boston was a hotbed of colonial discontent. The assemblage of military troops for control of possible disorders aggravated the discontent, not only because it affronted the English tradition against domestic use of military troops, but also because it was without warrant in the charter of Massachusetts Bay. The unwelcome troops were frequently taunted and vilified, and the ultimate and inevitable outrage soon occurred. A crowd of angry Bostonians . . . blocked the path of a detachment of soldiers marching to their post. The soldiers made ready to force their passage, but were ordered back to the main guard. . . . The crowd approached the main guard with angry and opprobrious taunts. A sentinel struck one particularly bothersome boy with the butt of his musket, and quickly a crowd converged on that spot throwing snowballs and rocks at the sentinel along with verbal

In any event, the experience was sufficiently vexing that the Declaration of Independence listed among our grievances against Great Britain that the King had "kept among us, in times of peace, Standing Armies without the consent of our legislatures," had "affected to render the Military independent of and superior to the civil power," and had "quarter[ed] large bodies of armed troops among us . . . protecting them, by a mock trial, from punishment for any murders which they should commit on the inhabitants of these States."[2014]

The Articles of Confederation addressed the threat of military intrusion into civilian affairs by demanding that the armed forces assembled during peacetime be no more numerous than absolutely necessary for the common defense, by entrusting control to civil authorities within the states, and by a preference for the farmer in arms as a member of the militia over the standing professional army.[2015]

The Constitution continued these themes albeit with greater authority vested in the federal government. It provided that a civilian, the President, should be the Commander in Chief of the Army and Navy of the United States and that civilian authorities, the Congress, should be solely empowered to raise and support

---

threats on his life. The sentinel loaded his musket and waved it at the mob, a squad of soldiers were sent to his aid. The soldiers, soon joined by a colonel, loaded their muskets as the crowd hooted and jeered and berated them and dared them to shoot. They kept the crowd back a time with bayonets, but then suddenly fired. It was never made clear -- it never is --whether they had fired on their officer's order, or upon their own compulsion. In any event, five Americans lay dead and several others seriously wounded. . . . Members of a distrusted standing army, whose quartering was in violation of the Petition of Right, and whose preparation to militarily suppress possible civil disorder was inconsistent with the oldest of England's own traditions, had slain English civilians in a time of peace").

[2014] This last charge presumably refers to the results of the murder trials of the officer and soldiers involved in the Boston Massacre. Two of the soldiers were convicted of manslaughter, branded on the hand and released; the officer and the other soldiers were acquitted. ZOBEL, THE BOSTON MASSACRE 241-94 (1987).

[2015] E.g., "No vessels of war shall be kept up in time of peace by any State, except such number only, as shall be deemed necessary by the United States in Congress assembled, for the defence of such State, or its trade; nor shall any body of forces be kept up by any State, in time of peace, except such number only, as in the judgment of the United States, in Congress assembled, shall be deemed requisite to garrison the forts necessary for the defence of such State; but every State shall always keep a well regulated and disciplined militia, sufficiently armed and accoutered, and shall provide and constantly have ready for public use, in public stores, a due number of field pieces and tents, and a proper quantity of arms, ammunition and camp equipage . . . . When land-forces are raised by any State for the common defence, all officers of or under the rank of colonel, shall be appointed by the Legislature of each State respectively by whom such forces shall be raised, or in such manner as such State shall direct, and all vacancies shall be filled up by the State which first made the appointment. . . . The United States in Congress assembled shall never . . . appoint a commander in chief of the army or navy, unless nine States assent to the same. . . ." Arts. of Conf. VI, VII, & IX.

Armies, provide and maintain a Navy, and make rules for their government and regulation.[2016] The Bill of Rights limited the quartering of troops in private homes, U.S. Const. Amend. III, and noted that "a well regulated Militia, being necessary to the security of a free State, the right of the people to keep and bear Arms, shall not be infringed," U.S. Const. Amend. II. The Constitution, on the other hand, explicitly permitted the Congress to provide for calling out the militia to execute the laws, suppress insurrection, and repel invasion, U.S.Const. Art.I, §8, cl.16.

Soon after Congress was first assembled under the Constitution, it authorized the President to call out the militia, initially to protect the frontier against "hostile incursions of the Indians," and subsequently in cases of invasion, insurrection, or obstruction of the laws.[2017]

Washington used this authority to put down the Whiskey Rebellion in Western Pennsylvania[2018] and subsequent Presidents have relied upon it with some

---

[2016] U.S.Const. Art.II, §2; Art.I, §8, cls.12, 13, 14. The Constitution treats the militia similarly. The President is the Commander in Chief of the militia while it is in federal service, and Congress is empowered to approve its organization, arms and discipline, U.S.Const. Art.II, §2; Art.I, §8, cl.15.

[2017] 1 Stat. 96 (1789); 1 Stat. 264 (1792). The Constitutional and statutory authority to use military force in case on insurrection seems to have been in direct response to a perceived weakness in government under the Articles of Confederation. In 1787, a group farmers in western Massachusetts, lead by a Revolutionary War veteran named Daniel Shays and feeling oppressed by tax and creditor protection policies within the Commonwealth, had harassed the state courts and constabulary, and had attempted to storm the federal arsenal at Springfield before being repulsed by the militia. Some saw in the insurrection evidence of the need for a stronger central government and implicitly that domestic tranquility might be more readily ensured if backed by centralized military capable. I MORISON, COMMAGER, & LEUCHTENBURG, THE GROWTH OF THE AMERICAN REPUBLIC 242 (7th ed. 1980)("Nevertheless, Shays's Rebellion had a great influence on public opinion. . . . When Massachusetts appealed to the Confederation for help, Congress was unable to do a thing. That was the final argument to sway many Americans in favor of a stronger federal government"); COLLIER & COLLIER, DECISION IN PHILADELPHIA: THE CONSTITUTIONAL CONVENTION OF 1787 13 (1986)("To men like Madison and Washington, Shays's Rebellion was an imperative. It hung like a shadow over the old Congress, and gave both impetus and urgency to the Constitutional Convention. It was the final, irrefutable piece of evidence that something had good badly wrong. For some time these men had known that the deficiencies of the American government must be remedied. Shays' Rebellion made it clear to them that it must be done now"). BOWEN, MIRACLE AT PHILADELPHIA: THE STORY OF THE CONSTITUTIONAL CONVENTION MAY TO SEPTEMBER 1787 10 (1966) ("Shays's Rebellion had been in the public mind when Congress, after debating the Annapolis report, had voted in favor of a convention in Philadelphia").

[2018] See Presidential Proclamations of Aug. 7, 1794 and Sept. 25, 1794, I RICHARDSON, A COMPILATION OF THE MESSAGES AND PAPERS OF THE PRESIDENTS 158-62 (1896); SLAUGHTER, THE WHISKEY REBELLION: FRONTIER EPILOGUE TO THE AMERICAN REVOLUTION (1986); BOYD, THE WHISKEY REBELLION: PAST AND PRESENT PERSPECTIVES (1985).

frequency for riot control or when in extreme cases they felt it necessary to ensure the execution of federal law.[2019]

The President's authority to call upon the state militia to aid in putting down insurrections is reminiscent of the authority enjoyed by the sheriff at common law to call upon the posse comitatus.[2020] In the beginning the two were comparable but unrelated. Even though Congress empowered the President to call out the militia to overcome obstructions to law enforcement, it continued to vest the federal equivalent of the sheriff, the federal marshal, with the power to call forth the posse comitatus in performance of his duties.[2021]

In some cases when it passed a particular statute Congress specifically authorized recourse to the posse comitatus for its enforcement. Under the Fugitive Slave Act, for instance, owners whose slaves had escaped to another state were entitled to an arrest warrant for the slaves and to have the warrant executed by the federal marshals. The marshals in turn might "summon and call to their aid the bystanders, or posse comitatus of the proper county . . . [and] all good citizens [were] commanded to aid and assist in the prompt and efficient execution of this law, whenever their services may be required, as aforesaid, for that purpose," 9 Stat. 462, 463 (1850).

[2019] Eighteenth and nineteenth century instances are collected, along with related proclamations and other documentation, in Federal Aid in Domestic Disturbances: 17871903, S.DOC.NO. 209, 57th Cong., 2d Sess. (1903); for a more selective treatment but one which extends well into this century, see, RICH, PRESIDENTS AND CIVIL DISORDER (1941).

[2020] At common law, the sheriff of every county was obligated "to defend his county against any of the king's enemies when they come into the land; and for this purpose, as well as for keeping the peace and pursuing felons, he may command all the people of his county to attend him; which is call the posse comitatus, or power of the county; which summons every person above fifteen years old, and under the degree of a peer, is bound to attend upon warning, under pain of fine and imprisonment." I BLACKSTONE, COMMENTARIES ON THE LAWS OF ENGLAND, 332 (1765).

The Latin phrase literally means attendants with the capacity to act from the words comes and posse meaning companions or attendants (comes) and to be able or capable (posse). Among the Romans comitatus referred to one who accompanied the proconsul to his province. Later, comes (sometimes referred to as comites or counts) meant the king's companions or his most trusted attendants and comitatus came to refer to the districts or counties entrusted to their care. BOUVIER'S LAW DICTIONARY AND CONCISE ENCYCLOPEDIA 529, 2635 (1914).

[2021] E.g., 1 Stat. 87 (1789)("a marshal shall be appointed in and for each district . . . whose duty it shall be . . . to execute throughout the district, all lawful precepts directed to him, and issued under the authority of the United States, and he shall have the power to command all necessary assistance in the execution of his duty. . . ."); 1 Stat. 265 (1792)("the marshals of the several districts and their deputies shall have the same powers in executing the laws of the United States, as sheriffs and their deputies in the several states have by law, in executing the laws of their respective states").

In June of 1851, a federal marshal in Chicago arrested a fugitive slave on a warrant issued under the Act. He called for the assistance of members of the police force and of the state militia to prevent abolitionists from rescuing the prisoner before he could be returned to his owner. The marshal subsequently filed a claim with the Treasury of the United States for reimbursement of the funds he had paid the members of the police force and the militia who responded to his call. Attorney General Caleb Cushing was asked whether the United States was obligated to honor the claim.

Cushing's response went well beyond the question of whether the "bystanders" contemplated by the Fugitive Slave Act might included members of a state militia when not in federal service, and announced a broader principle -- members of the military by virtue of their duties as citizens were part of the posse comitatus. He declared:

> *"The posse comitatus comprises every person in the district or county above the age of fifteen years, whatever may be their occupation, whether civilians or not; and including the military of all denominations, militia, soldiers, marines, all of whom are alike bound to obey the commands of the sheriff or marshal. The fact that they are organized as military bodies, under the immediate command of their own officers, does not in any wise affect their legal character. They are still the posse comitatus. (xxi Parl. Hist., p.672, 688, per Lord Mansfield)." 6 Op.Att'y Gen. 466, 473 (1854).*[2022]

[2022] Cushing's citation to Lord Mansfield is apparently a reference to the remarks of the English Chief Justice during debate in the House of Lords concerning the validity of use troops to quell rioters in London: "The Duke of Richmond began with observing, that he was much pleased with the speech he heard that day from the throne. . . . He hoped, before he should agree to the Address, that ministers would give him satisfaction in another point: he meant in the continuing on foot of a military government. . . . Lord Mansfield for some time argued [several points]. . . after which his lordship went on: `. . . .[I]t appears most clearly to me, that every man may legally interfere to suppress a riot, much more to prevent acts of felony, treason, and rebellion, in his private capacity, but he is bound to do it as an act of duty; and if called upon by a magistrate, is punishable in case of refusal. . . . A private man, if he sees a person committing an unlawful act, more particularly an act amounting to a violent breach of the peace, felony, or treason, may apprehend the offender, and in his attempt to apprehend him may use force to compel him, not to submit to him, but to the law. What a private man may do, a magistrate or peace officer may clearly undertake; and according to the necessity of the case, arising from the danger to be apprehended, any number of men assembled or called together for the purpose are justified to perform. This doctrine I take to be clear and indisputable, with all the possible consequences which can flow from it, and to be the true foundation for calling in of the military power to assist in quelling the late riots.

"The persons who assisted in the suppression of those riots and tumults, in contemplation of law, are to be considered as mere private individuals, acting according to law, and upon any abuse of the legal power with which they are invested, are amendable to the laws of their country. For instance, supposing a soldier, or any other military person, who acted in the course of the late

Two years later, Cushing's opinion supplied the justification for the use of federal troops at the call of civil law enforcement authorities in what some saw as partisan involvement in the conflict between pro and anti-slavery forces in Kansas. Congress reacted with a rider to an Army appropriations bill forbidding the use of any "part of the military forces of the United States to enforce territorial law in Kansas."[2023] After some discussion of whether the amendment was germane, it was defeated.

Following the Civil War, the use of federal troops to execute the laws, particularly in the states that had been part of the Confederacy, continued even after all other political restrictions had been lifted. By 1877, there was evidence that Republican

---

riots, had exceeded the powers with which he was invested, I have not a single doubt but he is liable to be tried and punished, not by martial law, but by the common and statute law of the realm; consequently, the false idea that we are living under a military government or that the military have any more power or other power, since the commencement of the riots, is the point which I rose to refute, and on that ground to remove those idle and ill-founded apprehensions, that any part of the laws or the constitution are either suspended or have been dispensed with. . . . On the whole, my lords, while I deprecate and sincerely lament the cause which rendered it indispensably necessary to call out the military to assist in the suppression of the late disturbances, I am clearly of the opinion, that no steps have been taken which were not strictly legal, as well as fully justifiable in point of policy. . . . The military have been called in, and very wisely called in, not as soldiers, but as citizens: no matter whether their coats be red or brown, they have been called in aid of the laws, not to subvert them, or overturn the constitution, but to preserve both." XXI HANSARD, THE PARLIAMENTARY HISTORY OF ENGLAND FROM THE EARLIEST PERIOD TO THE YEAR 1803, 690-98 (June 19, 1780).

Cushing seemed to turn Lord Mansfield's point on its head when he wrote that, "the fact that they are organized as military bodies, under the immediate command of their own officers, does not in any wise affect their legal character." English law prohibited martial law, the use of military force domestically, in peacetime England. Lord Mansfield justified an apparent breach of the martial law proscription by asserting that the soldiers had acted as individuals called, commanded, and governed exclusively by the dictates of law applicable to civilians. Civilians are not organized as military units and are not subject to the command of military officers. Military law governs such matters. Lord Mansfield's justification could only hold as long as the soldiers were not organized as military bodies and were not acting under the command of their officers. The fact that they were organized as military bodies, under the immediate command of their own officers, would determine their legal character; it was in fact the critical determinant of their legal character.

[2023] "But Congress hereby disapproving the code of alleged laws officially communicated to them by the President, and which are represented to have been enacted by a body claiming to be the Territorial Legislature of Kansas; and also disapproving of the manner in which said alleged laws have been enforced by the authorities of said Territory, expressly declare that, until those alleged laws shall have been affirmed by the Senate and House of Representatives as having been enacted by a legal Legislature, chosen in conformity with the organic law, by the people of Kansas, no part of the military force of the United States shall be employed in aid of their enforcement, nor shall any citizen of Kansas be required, under those provisions to act as a part of the posse comitatus of any officer acting as a marshal or sheriff in said Territory." Cong.Globe 34th Cong., 1st & 2d Sess. 1813 (1856).

---

state governments in more than one southern state owed their continued political existence to the presence of the military and that the activities of federal troops may have influenced the outcome of the Hayes-Tilden presidential election.[2024]

The House of Representatives, controlled by a Democratic majority, passed an Army appropriation bill which expressly prohibited use of the Army to shore up Republican state governments in the South, or more precisely, to shore up either side of the political dispute in Louisiana or anywhere else.[2025] The Senate, controlled by a Republican majority, refused to accept the provision. No compromise could be reached, and the session ended without passage of an Army appropriation bill. Money to pay the Army was subsequently appropriated in a special session,[2026] without reference to restrictions on use of the Army.[2027] But when the issue of Army appropriations next arose, the House included a posse

---

[2024] Members of the two political parties understandably disagreed as to whether the presence of federal troops in the South tainted or insured the integrity of the political process; compare, "[O]ur Army, degraded from its high position of the defenders of the country from foreign and domestic foes, has been used as a police; has taken possession of polls and controlled elections; has been sent with fixed bayonets into the halls of State Legislatures in time of peace and under the pretense of threatened outbreak; has been placed under the control of subordinate State officials, and, under the instructions of the Attorney General, has been notified to obey the orders of deputy United States marshals, `general and special,' appointed in swarms to do dirty work in a presidential campaign," 5 Cong.Rec. 2117 (remarks of Rep. Banning), with, "Nor do I think, sir, that the use of troops in the States recently in rebellion was uncalled for or inconsistent with the spirit of republican liberty. If they were recalled before every man, white and black, was safe -- safe and truly free, with all his civil rights in their fullest extent -- they were recalled too soon." 7 Cong.Rec. 3616.

[2025] Section 5 of H.R. 4691, as passed by the House, provided, "That no part of the money appropriated by this act, nor any money heretofore appropriated, shall be applied to the pay, subsistence, or transportation of troops used, employed, or to be used or employed, in support of the claim of Francis T. Nicholls or S.B. Packard to be governor the State of Louisiana. Nor shall any of said money be applied in support of the claim of the two bodies claiming to be the Legislature of said State, presided over respectively by L.A. Wiltz and Louis Bush; nor of the two bodies claiming to be the Legislature of said State, presided over respectively by C.C. Antonie and Michael Hahn; nor in support of the claim of Thomas C. Manning and associates to be the supreme court of said State; nor in support of the claim of John T. Ludeling and associates to the supreme court of said State; nor in the aid of the execution of any process in the hands of the United States marshal in said State issued in aid of and for the support of any such claims. Nor shall the Army, or any portion of it, be used in support of the claims, or pretended claim or claims, of any State government, or officer thereof, in any State, until the same shall have been duly recognized by Congress. Any person offending against any of the provisions of this act shall be guilty of a misdemeanor, and, upon conviction thereof, shall be imprisoned at hard labor for not less than five years or more than ten years," 5 Cong.Rec. 2119 (1877).

[2026] See Presidential Proclamation of May 5, 1877, 20 Stat. 803 (1877), calling Congress into session.

[2027] The bill contained no posse comitatus provisions because the President had withdrawn federal troops from Louisiana and South Carolina and because of concern over disturbances on the Mexican border and over Indian uprisings, 6 Cong.Rec. 287 (remarks of Rep. Atkins) (1877).

comitatus section.[2028] The Senate accepted the House version with minor amendments.[2029] (remarks of Rep. Philips).

The Posse Comitatus Act has remained essentially unchanged ever since,[2030] although Congress has authorized a substantial number of exceptions and has buttressed the Act with an additional proscription against use of the armed forces to make arrests or conduct searches and seizures.[2031]

[2028] "From and after the passage of this act it shall not be lawful to employ any part of the Army of the United States as a posse comitatus or otherwise under the pretext or for the purpose of executing the laws, except in such cases and under such circumstances as such employment of said forces may be expressly authorized by act of Congress; and no money appropriated by this act shall be used to pay any of the expenses incurred in the employment of any troops in violation of this section; and any person violating the provisions of the this section shall be deemed guilty of a misdemeanor, and on conviction thereof shall be punished by a fine not exceeding $10,000 or imprisonment not exceeding two years, or both such fine and imprisonment," 7 Cong.Rec. 3845 (1878).

[2029] The "pretext" language was stricken because it was thought to be "in the nature of a reflection upon the past administration of the Government," 7 Cong.Rec. 4648 (remarks of Sen. Sargent); instances of express Constitutional authority were added to the statutory exception, although then as now the precise effect of this change was a matter of dispute; the penalty was applicable only to willful violations although a Senate requirement that the penalty be restricted to willful and knowing violations was not accepted. Id.

[2030] For some time the Act was contained in title 10 of the United States Code and Alaska, while a territory was exempted, 10 U.S.C. 15 (1940 ed.). When title 10 was recodified and the section transferred tot title 18, the Air Force which had been covered while it was part of the Army was expressly added to the Act, 70A Stat. 626 (1956). Over the years, Congress has adjusted the impact of the Posse Comitatus Act by enlarging the number of statutes which expressly authorize the use of the Army or Air Force to execute the law. These are sometimes referred to as "amendments" to the Posse Comitatus Act. Since they do not change language of the Act itself, it seems to more accurate to characterize them as expansions of authority under the statutory exception to the Posse Comitatus Act rather than as amendments or changes in the Act itself.

[2031] "The Secretary of Defense shall prescribe such regulations as may be necessary to ensure that any activity (including the provision of any equipment or facility or the assignment or detail of any personnel) under this chapter [10 U.S.C. 371-381] does not include or permit direct participation by a member of the Army, Navy, Air Force, or Marine Corps in a search, seizure, arrest, or other similar activity unless participation in such activity by such member is otherwise authorized by law." 10 U.S.C. 375. Soon after the enactment of section 375, the Secretary of Defense promulgated such regulations which, subject to designated exceptions, prohibited: "(i) Interdiction of a vehicle, vessel, aircraft or other similar activity. (ii) A search or seizure, (iii) An arrest, stop and frisk, or similar activity. (iv) Use of military personnel for surveillance or pursuit of individuals, or as informants, undercover agents, investigators, or interrogators." 32 CFR 213(10)(a)(3), 47 Fed.Reg. 14899, 14902 (April 7, 1982). Some years later the regulations were removed, 53 Fed.Reg. 23776 (April 28, 1993) ("The Department of Defense hereby removes 32 CFR part 213 concerning DoD Cooperation with Civil and Law Enforcement Officials, part 372a . . . and part 390a . . . . These parts have served the purpose for which they were intended and are no longer valid"). Department of Defense Directive 5525.5, however, which with its enclosures replicates much of former 32 CFR part 213, remains in effect.

The Posse Comitatus Act raises at least three constitutional questions. (1) To what extent does the Posse Comitatus Act track constitutional requirements, beyond the power of the President or Congress to adjust or ignore? (2) To what extent do the powers which the Constitution vests in the President limit the power of Congress to enact the Posse Comitatus Act or any other provision restricting the President's discretion to involve the armed forces in civilian affairs? (3) What specifically are the military law enforcement activities "expressly authorized in the Constitution" for purposes of the Act?

Constitutional Origins

Lord Coke and his colleagues, in crafting the Petition of Right of 1628, found within that chapter of the Magna Carta and subsequent explanatory statutes which are the antecedents of our constitutional due process clauses a prohibition against martial law -- a proscription which in times of peace would not abide either the quartering of troops among civilians or any form of martial law, be it imposed by tribunal or more summarily dispatched by soldiers controlling or punishing civilians.

The Declaration of Independence lists the imposition of martial law upon us among those affronts to fundamental liberties which irrevocably ruptured our political ties to Great Britain.

Finally, it possible to see in the Second, Third, and Fifth Amendments, with their promises of a civilian militia, of freedom from the quartering of troops among us, and of the benefits of due process, the visible protrusions of a larger, submerged constitutional principle which bars the use of the armed forces to solve civilian inconveniences.

This view is not without judicial support. The courts have demonstrated a rather long standing reluctance to recognize the authority of military tribunals over civilians.[2032] And members of the Supreme Court seem to acknowledge possible components of a larger principle in both Youngstown Sheet and Tube Co. v. Sawyer, 343 U.S. 579 (1952)[2033] and Laird v. Tatum, 408 U.S. 1 (1972).[2034]

[2032] Ex parte Milligan, 71 U.S. (4 Wall.) 3, 123-25 (1866); Toth v. Quarles, 350 U.S. 11 (1955); Reid v. Covert, 354 U.S. 1 (1957); Kinsella v. Singleton, 361 U.S. 234 (1960); Grisham v. Hagan, 361 U.S. 278 (1960); McElroy V. Guagliardo, 361 U.S. 281 (1960); O'Callahan v. Parker, 395 U.S. 258 (1969); but see, Solorio v. United States, 483 U.S. 435 (1987), holding that the jurisdiction of military tribunals depends upon whether the accused was a member of the armed forces at the time of alleged misconduct and contrary to O'Callahan not whether the crime was "service connected."

[2033] "Article II, Section 2 make the Chief Executive the Commander in Chief of the Army and Navy. But our history and tradition rebel at the thought that the grant of military power carries with it authority over civilian affairs," 343 U.S. at 632 (Douglas, J., concurring). "Time out of

But if a larger anti-martial law principle lies beneath constitutional sands, visible only in these amendments and the spirit of the Posse Comitatus Act, it has remained remarkably dormant. Those regions from which it might have been expected to emerge have been characterized most by inactivity. The boundaries of the Third Amendment are virtually uncharted.[2035] The outreaches of the Second

---

mind, and even now in many parts of the world, a military commander can seize private housing to shelter his troops. Not so, however, in the United States, for the Third Amendment says, `No Soldier shall, in time of peace be quartered in any house, without the consent of the Owner, nor in time of war, but in a manner to be prescribed by law.' Thus, even in war time, his seizure of needed military housing must be authorized by Congress. It also was expressly left to Congress to `provide for calling forth the Militia to execute the laws of the Union, suppress Insurrections and repel Invasions . . . ." Such a limitation on the command power, written at a time when the militia rather than a standing army was contemplated as the military weapon of the Republic, underscores the Constitution's policy that Congress, not the Executive, should control utilization of the war power as an instrument of domestic policy. Congress, fulfilling that function, has authorized the President to use the army to enforce certain civil rights. On the other hand, Congress has forbidden him to use the army for the purpose executing general laws except when expressly authorized by the Constitution or Act of Congress," 343 U.S. at 644-45 (Jackson, J., concurring)(emphasis in the original). In Youngstown, the Court held that, when Congress had specifically refused to grant such authority by statute, the President's constitutional and statutory powers as President and Commander in Chief were not sufficient to support an executive order authorizing the Secretary of Commerce use the resources of the federal government, including its armed forces, to seize and operate the country's steel mills which were then threaten by a nationwide strike.

[2034] "The concerns of the Executive and Legislative Branches in response to disclosure of the Army surveillance activities -- and indeed the claims alleged in the complaint -- reflect a traditional and strong resistance of Americans to any military intrusion into civilian affairs. That tradition has deep roots in our history and found early expression, for example, in the Third Amendment's explicit prohibition against quartering soldiers in private homes without consent and in the constitutional provisions for civilian control of the military. Those prohibitions are not directly presented by this case, but their philosophical underpinnings explain our traditional insistence on limitations on military operations in peacetime," 408 U.S. at 15-6. In Laird v. Tatum, the Court refused to order the military to stop collecting information about civilians unless the civilians could show how they had been hurt by the what the military was doing. (More precisely the Court held that, in the absence of any showing of specific harm or the realistic threat of specific harm, a claim, that the data gathering activities of the military services had been conduct so as to chill the First Amendment rights of the targets of those intelligence collection efforts, was nonjusticiable).

[2035] See, Bell, The Third Amendment, Forgotten But Not Gone, 2 WILLIAM & MARY BILL OF RIGHTS JOURNAL 117 (1993); Fields & Hardy, The Third Amendment and the Issue of the Maintenance of Standing Armies: A Legal History, 35 AMERICAN JOURNAL OF LEGAL HISTORY 393 (1991); Fields, The Third Amendment: Constitutional Protection From the Involuntary Quartering of Soldiers, 124 MILITARY LAW REVIEW 195 (1989). In one of the few reported Third Amendment cases, striking state correctional officers brought a civil rights action against state authorities who had used the officers' prison facility resident quarters to house replacement national guard troops. The district court dismissed, Engblom v. Carey, 522 F.Supp. 57 (S.D.N.Y. 1981), the Court of Appeals reversed on the ground that it could not hold as a matter of law that the officers had no Third Amendment possession interest in the resident quarters, 677 F.2d 957 (2d Cir. 1982). On remand the district court dismissed based on the qualified immunity of the defendant state officials in light of the uncertainty of the light with respect to Third

---

Amendment are only slightly more visible.[2036] Even in the inviting context of the Posse Comitatus Act, the courts have generally avoided excursions into areas of its possible constitutional underpinnings.[2037]

Without more judicial guidance, it would appear that traditional reservations about military involvement in the execution of civilian law can only clearly be said to rise to the level of constitutional imperative when they take a form which offends some more explicit constitutional prohibition or guarantee such as the right to jury trial, to grand jury indictment, or to freedom from unreasonable searches and seizures.[2038] Consequently, beyond those specific constitutional provisions, Congress' constitutional authority to enact and adjust the provisions of the Posse Comitatus Act is largely a matter of the coordination of Congressional and Presidential powers.

Presidential v. Congressional Powers

The case of conflicting Congressional and Presidential powers is easily stated if not easily resolved. On one hand, the Constitution requires the President to take care to see that the laws are faithfully executed, and designates him as Chief Executive and Commander in Chief of the armed forces.[2039] In this dual capacity, the Presidency is the repository of both extensive responsibilities and broad prerogatives, not the least of which flow from Article IV, section 4 of the

---

Amendment questions, 572 F.Supp. 44 (S.D.N.Y. 1983), aff'd, 724 F.2d 28 (2d Cir. 1983). The implications of the case prior to remand are discussed in The Third Amendment's Protection Against Unwanted Military Intrusion, 49 BROOKLYN LAW REVIEW 857 (1983).

[2036] United States v. Miller, 307 U.S. 174 (1939). The academic commentary is considerably more extensive and reflects a considerably greater divergence of views than is the case of the Third Amendment, see Van Alstyne, The Second Amendment and the Personal Right to Bear Arms, 43 DUKE LAW JOURNAL 1236 (1994); Herz, Gun Crazy: Constitutional False Consciousness and Dereliction of Dialogic Responsibility, 75 BOSTON UNIVERSITY LAW REVIEW 57 (1995) and the sources cited therein.

[2037] E.g., United States v. Walden, 490 F.2d 372, 376 (4th Cir. 1974)("we do not find it necessary to interpret relatively unexplored sections of the Constitution in order to determine whether there might be constitutional objection to the use of the military to enforce civilian laws").

[2038] See, The Posse Comitatus Act: Reconstruction Politics Reconsidered, 13 AMERICAN CRIMINAL LAW REVIEW 703, 712-13 (1976).

[2039] U.S. Const. Art.II, §1 ("[t]he executive Power shall be vested in a President of the United States of America. . .), §2 ("[t]he President shall be Commander in Chief of the Army and Navy of the United States, and of the Militia of the several States, when called into actual Service of the United States. . .), §3 (". . . he [(the President)] shall take Care that the Laws be faithfully executed . . . ").

Constitution which guarantees the states a republican form of government and protection against invasion and domestic violence.[2040]

The Supreme Court has made it clear that the President is not dependent upon express Constitutional or statutory authorization for the exercise of his powers. Thus, he may meet an emergency by appointing a marshal to protect a threatened Supreme Court justice, although no statute expressly authorized appointment for such purposes, In re Neagle, 135 U.S. 1, 62-4 (1890). He must resist invasion by an enemy with force though Congress has yet to declare war, The Prize Cases, 67 U.S.(2 Black) 635, 668 (1863). And when an emergency arises threatening the freedom of interstate commerce, transportation of the mails, or some other responsibility entrusted to the federal government, he may call upon "the army of the Nation, and all its militia . . . to brush away the obstructions," In re Debs, 158 U.S. 364, 381 (1895).

Some commentators feel that this implied or incidental constitutional authority to use the armed forces not only exists in the absence of Congressional direction, but is immune from Congressional direction or limitation.[2041]

On the other hand, Congress shares constitutional power over the laws and armed forces with the President. The Constitution gives Congress the power to make the laws whose faithful execution the President must take care to observe and which carry into execution Congress' own powers and those of the President, U.S.Const. Art.I, §8, cl.18; it likewise vests Congress with the power to establish, maintain and regulate the armed forces, U.S.Const. Art.I, §8, cls.12, 13, & 14; and with the power to describe the circumstances under which the militia may be called into federal service, U.S. Const. Art.I, §8, cls.15 & 16.

The Supreme Court has shed some light on the coordination of Presidential and Congressional powers concerning use of the military to enforce civilian law. The Court has pointed out that the President's power under the guarantee clause of Article IV, section 4, which guarantees the states protection against domestic violence, is only provisionally effective until such time as Congress acts, Texas v. White, 74 U.S.(7 Wall.) 700 (1869). And the President may not always use the armed forces to met a domestic emergency when Congress has previously

---

[2040] "The United States shall guarantee to every State in this Union, a Republican Form of Government, and shall protect each of them against Invasion; and on Application of the Legislature, or of the Executive (when the Legislature cannot be convened) against domestic Violence," U.S. Const. Art.IV, §4.

[2041] E.g., Lorence, The Constitutionality of the Posse Comitatus Act, 8 UNIVERSITY OF KANSAS CITY LAW REVIEW 164, 185-91 (1940); Furman, Restrictions Upon Use of the Army Imposed by the Posse Comitatus Act, 7 MILITARY LAW REVIEW 85, 91-2 (1960); CORWIN, THE PRESIDENT: OFFICE AND POWERS, 1787-1984, 152-61 (5th ed. 1984).

resisted an invitation to sanction their employment.[2042] Finally, even when Congress has disclaimed any intent to limit the exercise of the President's constitutional powers, the President's inherent and incidental powers will not always trump conflicting, constitutionally grounded claims.[2043]

When the Act Does Not Apply

There is no violation of the Posse Comitatus Act when (1) the Constitution expressly authorizes use of part of the Army or Air Force as a posse comitatus or otherwise to execute the law; (2) when an act of Congress expressly authorizes use of part of the Army or Air Force as a posse comitatus or otherwise to execute the law; (3) when the activity in question does not involve use of part of the armed forces covered by the proscription; and (4) when the activity in question is does not constitute "execution of the law."

Constitutional Exceptions

The Posse Comitatus Act does not apply "in cases and under circumstances expressly authorized by the Constitution," 18 U.S.C. 1385.[2044] It has been said that the Constitution contains no provision expressly authorizing the use of the

---

[2042] Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579 (1952). In Youngstown President Truman attempted to invoke his powers as Commander in Chief and Chief Executive to seize and operate most of the Nation's steel mills during the Korean conflict when it appeared they might be shut down by a labor dispute. Congress had earlier specifically refused to grant the President such power legislatively.

[2043] United States v. United States District Court, 407 U.S. 297 (1972). Congress had established a warrant procedure to be used by law enforcement officials to permit wiretapping in criminal cases. In doing so, it expressly disclaimed any intent to "limit the constitutional power of the President to take such measures as he deems necessary to protect the Nation against actual or potential attack or other hostile acts of a foreign power, to obtain foreign intelligence information deemed essential to the security of the United States, or to protect national security information against foreign intelligence activities [or] to take such measures as he deems necessary to protect the United States against the overthrow of the Government by force or other unlawful means, or against any clear and present danger to the structure or existence of the Government," 18 U.S.C. 2511(3)(1970 ed.). Even in the absence of Congressionally asserted counter authority, a unanimous Court declined to accept the argument that President's inherent and incidental constitutional powers permitted a failure to comply with the Fourth Amendment's warrant requirements when gathering intelligence concerning purely domestic threats to national security.

[2044] Whoever, except in cases and under circumstances expressly authorized by the Constitution or Act of Congress, willfully uses any part of the Army or the Air Force as a posse comitatus or otherwise to execute the laws shall be fined under this title or imprisoned not more than two years, or both. 18 U.S.C. 1385 (emphasis added).

military to execute the law,[2045] that it was included as part of a face-saving compromise, and that consequently it should be ignored.[2046]

When the phrase was added originally those who opposed the Posse Comitatus Act believed that the Constitution vested implied and/or inherent powers upon the President to use the armed forces to execute the laws; those who urged its passage believed the President possessed no such powers. As initially passed by the House, the bill contained no constitutional exception.[2047] The Senate version contained an exception for instances authorized by the Constitution whether expressed or otherwise.[2048] The managers of each House described the

---

[2045] H.R.Rep.No.97-71, at 6 n.3, reprinted 1981 UNITED STATES CODE, CONGRESSIONAL AND ADMINISTRATIVE NEWS at 1789 n.3 ("The statute permits Constitutional exceptions. However, there are none"); LIEBER, THE USE OF THE ARMY IN AID OF THE CIVIL POWER 17 (1898); The Navy's Role in Interdicting Narcotics Traffic: War on Drugs or Ambush of the Constitution? 75 GEORGETOWN LAW JOURNAL 1947, 1951 (1987); Don't Call Out the Marines: An Assessment of the Posse Comitatus Act, 13 TEXAS TECH LAW REVIEW 1467, 1486 (1982); The Posse Comitatus Act: Reconstruction Politics Reconsidered, 13 AMERICAN CRIMINAL LAW REVIEW 703, 712 (1976). The Constitution does empower Congress "to provide for calling forth the Militia to execute the laws of the Union, suppress insurrections and repel invasions," U.S.Const. Art.I, §8, cl.16; but since this express grant of authority can only be activated by an Act of Congress it adds nothing to the "act of Congress" exception also included within the Posse Comitatus Act.

[2046] "The Act also provides that the Army and Air Force can be used on the basis of an express constitutional authorization. This language reflects a compromise reached in the debate over the Act. It is a meaningless proviso since the Constitution does not expressly authorize such a use of troops. "In any event, if the Constitution provided the President with authority over a purely executive function, Congress could not disable the President from acting on the basis of it, whether the authorization was express or implied. But since the Constitution provides Congress with the power to control military intervention in domestic affairs, the President's actions can be limited to the express terms of a statutory authorization," Honored in the Breech: Presidential Authority to Execute the Laws with Military Force, 83 YALE LAW JOURNAL 130, 143-44 (1973); see also, The Posse Comitatus Act: Reconstruction Politics Reconsidered, 13 AMERICAN CRIMINAL LAW REVIEW 703, 712-13 (1976).

[2047] "From and after the passage of this act it shall not be lawful to employ any part of the army of the United Sates as a posse comitatus or otherwise under the pretext or for the purpose of executing the laws, except in such cases and under such circumstances as such employment of said force may be expressly authorized by act of Congress; and no money appropriated by this act shall be used to pay any of the expenses incurred in the employment of any troops in violation of this section; and any person violating the provisions of this section shall be deemed guilty of a misdemeanor, and on conviction thereof shall be punished by a fine of not exceeding $10,000 or imprisoned not exceeding two years, or by both such fine and imprisonment," 7 Cong.Rec. 3877 (1878)(emphasis added).

[2048] "From and after the passage of this act it shall not be lawful to employ any part of the army of the United Sates as a posse comitatus or otherwise for the purpose of executing the laws, except in such cases and under such circumstances as such employment of said force may be authorized by the Constitution or by act of Congress; and no money appropriated by this act shall be used to pay

compromise reached at conference and subsequently enacted as upholding the position of their respective bodies on the issue.[2049]

The older commentaries suggest that the word "expressly" must be ignored, for otherwise in their view the Posse Comitatus Act is a constitutionally

---

any of the expenses incurred in the employment of any troops in violation of this section," 7 Cong.Rec. 4303-304 (1878)(emphasis added).

[2049] "But these [compromises on other differences in the Army appropriation bill] are all minor points and insignificant questions compared with the great principle which was incorporated by the House in the bill in reference to the use of the Army in time of peace. The Senate had already conceded what they called and what we might accept as principle; but they had stricken out the penalty and had stricken out the word `expressly,' so that the Army might be used in all cases where implied authority might be inferred. The House committee planted themselves firmly upon the doctrine that rather than yield this fundamental principle, for which for three years this House had struggled, they would all the bill to fail -- notwithstanding the reforms which we had secured; regarding these reforms as of but little consequence alongside the great principle in all its length and breadth, including the penalty which the Senate had stricken out. We bring you back, therefore, a report with the alteration of a single word, which the lawyers assure me is proper to be made, restoring to this bill the principle for which we have contended so long, and which is so vital to secure the rights and liberties of the people," 7 Cong.Rec. 4686 (1878 (remarks of Rep. Hewitt).

"With reference to the provisions of the bill inserted by the House prohibiting the use of the Army, which is section 29, Senators will remember that it was amended in the senate so as to strike out in lines 3 and 4 the words `under the pretext or,' in the sixth line the word `expressly' was stricken out, and in the seventh line the words `the Constitution or by' were inserted, so as to read `by the Constitution or by act of congress,' and the penalty was stricken form the bill. We found considerable difficult in agreeing upon this section, but the modification which the Senate had made in it made it possible to come to an understanding. I should like to say here that it is my firm judgment, after the experience of the last forty-eight hours, that unless the senate had made the duty easy for the committee by the modification which it made in that section, it would have been impossible to have come to any agreement on the Army bill with the original House section in controversy. I am satisfied it never would have been stricken from the bill. As it now stands, the House yielded that the words `under the pretext of' should go out, which we contended were in the autre of a reflection upon the past administration of the government, and we could not consent that anything in the nature of a reflection, and which was entirely useless for any practical purpose, should remain in the bill. We satisfied them, by our argument that ought to be done, and it was stricken out.

"With reference to the word `expressly.' we restored it and allowed it to go in, so that now the employment of such force must be expressly authorized by the Constitution or by act of Congress, they assenting that the words `the Constitution or by' before the words `act of Congress' might remain in, so that if the power arises under either the constitution or the laws it may be exercised and the Executive would not be embarrassed by the prohibition of Congress so to act where the Constitution requires him to act; and the embarrassments would not have the effect of retraining the action of an upright and energetic Executive, but still might raise a question which he would desire to avoid if possible. The penalty remains in the section as agreed upon, except that we procured that the word `willfully' should be put in before the word `violating;' so that it reads: `And any person willfully violating the provisions of this section shall be deemed guilty of a misdemeanor," 7 Cong.Rec. 4648 (1878) (remarks of Sen.Sargent).

---

impermissible effort to limit the powers of the President.[2050] The regulations covering the use of the armed forces during civil disturbances do not go quite that far, but they do assert two constitutionally based exceptions -- sudden emergencies and protection of federal property.[2051]

[2050] LIEBER, THE USE OF THE ARMY IN AID OF THE CIVIL POWER, 14-5 (1898)("The debate [on the Posse Comitatus section] was an interesting one, but too long to follow in detail. An attempt was made to strike out the word "expressly," but that failed. But, manifestly, the clause, as enacted, recognizes the Constitution as a direct source of authority for the employment of the Army. This is a very important consideration in the construction of the legislation. And another matter of great importance is also to be observed with reference to it. The enactment prescribes that it shall be unlawful to employ any part of the Army as a posse comitatus, or otherwise, for the purpose of executing the laws, except when it is expressly authorized by the Constitution or by act of Congress. Now, it is evident that the word `expressly' can not be construed as placing a restriction on any constitutional power. If authority so to use the Army is included in a constitutional power, although it be not expressly named, it can not, of course, be taken away by legislation"); Lorence, The Constitutionality of the Posse Comitatus Act, 8 UNIVERSITY OF KANSAS CITY LAW REVIEW 154, 185-86 (1940)("But it is evident that the word expressly in the Posse Comitatus Act cannot be construed as placing a restriction on the constitutional Power of the President, because even though not expressly named, such constitutional power cannot be taken away by legislation. . . . Thus, the Posse Comitatus Act appears to be a rather singular statute to pass, saying that the Army of the United States shall not be used for the purpose of executing the laws, in view of the fact that the Constitution expressly makes the President the Commander-in-Chief of the Army and Navy, and expressly makes it his duty to take care that the laws are faithfully executed").

[2051] "(b) Aside from the constitutional limitations of the power of the Federal Government at the local level, there are additional legal limits upon the use of military forces within the United States. The most important of these from a civil disturbance standpoint is the Posse Comitatus Act (18 U.S.C. 1385), which prohibits the use of any part of the Army or the Air Force to execute or enforce the laws, except as authorized by the Constitution or Act of Congress.

"(c) The Constitution and Acts of Congress establish six exceptions generally applicable within the entire territory of the United States, to which the Posse Comitatus Act prohibition does not apply.

"(1) The constitutional exceptions are two in number and are based upon the inherent legal right of the U.S. Government -- a sovereign national entity under the Federal Constitution -- to insure the preservation of public order and the carrying out of governmental operations within its territorial limits, by force if necessary.

"(i) The emergency authority. Authori[z]ies prompt and vigorous Federal action, including use of military force to prevent loss of life or wanton destruction of property and to restore governmental functioning and public order when sudden and unexpected civil disturbances, disasters, or calamities seriously endanger life and property and disrupt normal governmental functions to such an extent that duly constituted local authorities are unable to control the situation.

"(ii) Protection of Federal property and functions. Authorizes Federal action, including the use of military forces, to protect Federal property and Federal governmental functions when the need for protection exists and duly constituted local authorities are unable or decline to provide adequate protection." 32 CFR 215.4(b),(c)(1).

The question of whether the constitutional exception includes instances where the President is acting under implied or inherent constitutional powers or whether it was merely a face saving device is a question that may turn on whether Congress may constitutionally restrict the President's powers, if any, in the area -- a question the courts have yet to answer.

Statutory Exceptions

Generally

The Posse Comitatus Act does not apply where Congress has expressly authorized use of the military to execute the law.[2052] Congress has done so in three ways, by giving a branch of the armed forces civilian law enforcement authority, by establishing general rules for certain types of assistance, and by addressing individual cases and circumstances with more narrowly crafted legislation. Thus it has vested the Coast Guard, a branch of the armed forces, with broad law enforcement responsibilities.[2053] Second, over time it has enacted a fairly

---

For a discussion of instances when the emergency, "immediate response authority" has been used see, Winthorp, The Oklahoma City Bombing: Immediate Response Authority and Other Military Assistance to Civil Authority (MAC), ARMY LAWYER 3 (July, 1997).

[2052] Whoever, except in cases and under circumstances expressly authorized by the Constitution or Act of Congress, willfully uses any part of the Army or the Air Force as a posse comitatus or otherwise to execute the laws shall be fined under this title or imprisoned not more than two years, or both. 18 U.S.C. 1385 (emphasis added).

[2053] "The Coast Guard shall enforce or assist in the enforcement of all applicable Federal laws on, under, and over the high seas and waters subject to the jurisdiction of the United states; shall engage in maritime air surveillance or interdiction to enforce or assist in the enforcement of the laws of the United States; shall administer laws and promulgate and enforce regulations for the promotion of safety of life and property on and under the high seas and waters subject to the jurisdiction of the United States covering all matters not specifically delegated by law to some other executive department; shall develop, establish, maintain and operate with due regard to the requirements of national defense, aids to maritime navigation, icebreaking facilities, and rescue facilities for the promotion of safety on, under, and over the high seas and waters subject to the jurisdiction of the United States; shall, pursuant to international agreements, develop, establish, maintain, and operate icebreaking facilities on, under, and over the waters other than the high seas and waters subject to the jurisdiction of the Untied States; shall engage in oceanographic research on the high seas and in waters subject to the jurisdiction of the United Stats; and shall maintain a state of readiness to function as a specialized service in the Navy in time of war, including the fulfillment of Maritime Defense Zone command responsibilities, 14 U.S.C. 2. Coast Guard personnel are also considered customs officers for purpose of custom law enforcement, 19 U.S.C. 1401(i)("When used in this subtitle [relating to administrative provisions concerning customs duties] or in part I of subtitle II of this chapter [relating to the miscellaneous provisions of the Tariff Act of 1930] . . . (i) The terms `officer of the customs' and `customs officer' mean . . . any commissioned, warrant, or petty officer of the Coast Guard. . ."). See generally, The United States Coast Guard's Law Enforcement Authority Under 14 U.S.C. §89: Smugglers' Blues or Boaters' Nightmare? 34 WILLIAM & MARY LAW REVIEW 933 (1993); Not Fit for Sea Duty: The

extensive array of particularized statutes, like those authorizing the President to call out the armed forces in times of insurrection and domestic violence, 10 U.S.C. 331-335.[2054] Finally, it has passed general legislation permitting the armed

---

Posse Comitatus Act, the United States Navy, and Federal Law Enforcement at Sea, 31 WILLIAM & MARY LAW REVIEW 445 (1990).

[2054] 5 U.S.C. App. (Inspector General Act of 1978) 8(g) (Department of Defense Inspector General is not limited by the Posse Comitatus Act (18 U.S.C. 1385) in carrying out audits and investigations under the Act); 10 U.S.C. 331-335 (President may use the militia and armed forces to suppress insurrection and enforce federal authority in the face of rebellion or other forms of domestic violence);

10 U.S.C. 374 note (§1004 of the National Defense Authorization Act for 1991, as amended)(during fiscal years 1991 through 2002, the Secretary of Defense may provide counter-drug activity assistance upon request of federal or state law enforcement agencies);

10 U.S.C. 382 (the Secretary of Defense may provide assistance to the Department of Justice in emergency situations involving chemical or biological weapons of mass destruction);

10 U.S.C. 382 note (§1023 of the National Defense Authorization Act for Fiscal Year 2000) (during fiscal years 2000 through 2004, the Secretary of Defense may provide assistance to federal and state law enforcement agencies to respond to terrorism or threats of terrorism);

16 U.S.C. 23 (Secretary of the Army may detail troops to protect Yellowstone National Park upon the request of the Secretary of the Interior);

16 U.S.C. 78 (Secretary of the Army may detail troops to protect Sequoia and Yosemite National Parks upon the request of the Secretary of the Interior);

16 U.S.C. 593 (President may use the land and naval forces of the United States to prevent destruction of federal timber in Florida);

16 U.S.C. 1861(a) (Secretary of Transportation (or the Secretary of the Navy in time of war) may entering into agreements for the use of personnel and resources of other federal or state agencies -- including those of the Department of Defense -- for the enforcement of the Magnuson Fishery Conservation and Management Act);

18 U.S.C. 112, 1116 (Attorney General may request the assistance of federal or state agencies -- including the Army, Navy and Air Force -- to protect foreign dignitaries from assault, manslaughter and murder);

18 U.S.C. 351 (FBI may request the assistance of any federal or state agency -- including the Army, Navy and Air Force -- in its investigations of the assassination, kidnapping or assault of a Member of Congress);

18 U.S.C. 831 (Attorney General may request assistance from the Secretary of Defense for enforcement of the proscriptions against criminal transactions in nuclear materials)(18 U.S.C. 175a, 229E, and 2332e cross reference to the Attorney General's authority under 10 U.S.C. 381 to request assistance from the Secretary in an emergency involving biological weapons, chemical weapons, and weapons of mass destruction respective);

forces to share information and equipment with civilian law enforcement agencies, 10 U.S.C. 371-381.

How explicit must a statutory exception be? If one believes the word "expressly" should be ignored with respect to the constitutionally based exception, consistency might suggest no more is required than that Congress authorize a thing to be done. To those so inclined, the position is further fortified when the statute authorizes executive branch action and the President's faithful execution

---

18 U.S.C. 1751 (FBI may request the assistance of any federal or state agency -- including the Army, Navy and Air Force -- in its investigations of the assassination, kidnapping or assault of the President);

18 U.S.C. 3056 (Director of the Secret Service may request assistance from the Department of Defense and other federal agencies to protect the President);

22 U.S.C. 408 (President may use the land and naval forces of the United States to enforce Title IV of the Espionage Act of 1917 (22 U.S.C. 401-408));

22 U.S.C. 461 (President may use the land and naval forces and militia of the United States to seize or detain ships used in violation of the Neutrality Act);

22 U.S.C. 462 (President may use the land and naval forces and militia of the United States to detain or compel departure of foreign ships under the provisions of the Neutrality Act);

25 U.S.C. 180 (President may use military force to remove trespassers from Indian treaty lands); 42 U.S.C. 98 (Secretary of the Navy at the request of the Public Health Service may make vessels or hulks available to quarantine authority at various U.S. ports);

42 U.S.C. 1989 (magistrates issuing arrest warrants for civil rights violations may authorize those serving the warrants to call for assistance from bystanders, the posse comitatus, or the land or naval forces or militia of the United States;

42 U.S.C. 5170b (Governor of state in which a major disaster has occurred may request the President to direct the Secretary of Defense to permit the use of DoD personnel for emergency work necessary for the preservation of life and property); 43 U.S.C. 1065 (President may use military force to remove unlawful enclosures from the public lands);

48 U.S.C. 1418 (President may use the land and naval forces of the United States to protect the rights of owners in guano islands);

48 U.S.C. 1422 (Governor of Guam may request assistance of senior military or naval commander of the armed forces of the United States in cases of disaster, invasion, insurrection, rebellion or imminent danger thereof, or of lawless violence);

48 U.S.C. 1591 (Governor of the Virgin Islands may request assistance of senior military or naval commander of the armed forces of the United States in the Virgin Islands or Puerto Rico in cases of disaster, invasion, insurrection, rebellion or imminent danger thereof, or of lawless violence); 50 U.S.C. 220 (President may use the Army, Navy or militia to prevent the unlawful removal of vessels or cargoes from customs areas during times of insurrection).

responsibility[2055] and the administrative housekeeping statute[2056] can be called into play. In this rarely espoused view if an agency has statutory authority to perform a task, the military may be asked to help.

Others maintain that statutes which authorize assistance from federal agencies and departments generally in order to accomplish a particular task qualify as exceptions even if they do not mention the Department of Defense or any part of the military establishment by name.[2057] On the one hand, such legislation has ordinarily come into being after the Posse Comitatus Act and thus would ordinarily be thought to amend any conflicting earlier law. On the other hand, the use of military force in civilian affairs is such an extraordinary thing that perhaps it ought not be presumed and only found were Congress has so stated in hoc verba.

The final and more commonly accepted proposition is that the phrase "in cases and under circumstances expressly authorized by . . . Act of Congress" demands statutory exception specifically refer to some form of military assistance.[2058]

Information and Equipment

In 1981, Congress enacted general law enforcement exceptions to the Posse Comitatus Act prohibitions in order to resolve questions raised by the so-called Wounded Knee cases.[2059] The cases grew out of events beginning late in February of 1973, when an armed crowd broke into and looted a trading post in the village of Wounded Knee on the Pine Ridge Reservation in South Dakota. FBI agents, U.S. marshals, and Bureau of Indian Affairs police surrounded the village and

---

[2055] U.S.Const. Art.II, §3, cl.3 ("he [the President] shall take care that the laws be faithfully executed."

[2056] 5 U.S.C. 301 ("The head of an Executive department or military department may prescribe regulations for the government of his department, the conduct of its employees, the distribution and performance of its business, and the custody, use, and preservation of its records, papers, and property. . . .").

[2057] E.g., 21 U.S.C. 873(b)("[w]hen requested by the Attorney General, it shall be the duty of any agency or instrumentality of the Federal Government to furnish assistance, including technical advice, to him for carrying out his functions under this subchapter; except that no such agency or instrumentality shall be required to furnish the name of, or other identifying information about, a patient or research subject whose identity it has undertaken to keep confidential").

[2058] The Department of Defense Directive, for example, lists only the military-aid-specific statutes in its inventory of statutory exceptions, DoD Dir.No. 5525.5 (Encl.4) A.2.e.

[2059] H.R.Rep.No. 97-71, pt.2, 5-6, reprinted in 1981 UNITED STATES CODE, CONGRESSIONAL AND ADMINISTRATIVE NEWS 1785, 1788 ("Although the military activities challenged in each case were identical, the courts in Banks and Jaramillo found those activities to be in violation of the [Posse Comitatus] Act, while the lower court in Red Feather found those activities to be permissible").

besieged the group almost immediately. The take-over and events which occurred during the siege led to four cases[2060] involving a series of federal criminal charges including obstructing a law enforcement officer in the lawful performance of his duties during the course of a civil disturbance.[2061] Military assistance provided federal authorities at Wounded Knee undermined the prospects of a conviction under 18 U.S.C. 231(a)(3).[2062]

The 1981 legislation contains both explicit grants of authority and restrictions on the use of that authority for military assistance to the police -- federal, state and local -- particularly in the form of information and equipment, 10 U.S.C. 371-381.

Information: Spies, Advisers, and Undercover Agents

The Wounded Knee cases spawned uncertainty as to the extent to which military authorities might share technical advice, the results of reconnaissance flights or any other forms of information with civilian law enforcement authorities. Section 371 specifically permits the armed forces to share information acquired during military operations and in fact encourages the armed forces to plan their activities with an eye to the production of incidental civilian benefits.[2063] The

---

[2060] United States v. Jaramillo, 380 F.Supp. 1375 (D.Neb. 1974), app.dism'd, 510 F.2d 808 (8th Cir. 1975); United States v. Banks, 383 F.Supp. 368 (D.S.D. 1974); United States v. Red Feather, 381 F.Supp. 916 (D.S.D. 1975); United States v. McArthur, 419 F.Supp. 186 (D.N.D. 1976), aff'd sub nom., United States v. Casper, 541 F.2d 1275 (8th Cir. 1976).

[2061] 18 U.S.C. 231(a)(3)(1970 ed.)("Whoever commits or attempts to commit any act to obstruct, impede, or interfere with any fireman or law enforcement officer lawfully engaged in the lawful performance of his official duties incident to and during the commission of a civil disorder which in any way or degree obstructs, delays, or adversely affects commerce or the movement of any article or commodity in commerce or the conduct or performance of any federally protected function --shall be fined not more than $10,000 or imprisoned not more than five years, or both").

[2062] "The evidence of military involvement contained in the transcripts [of the Wounded Knee trial cases], in essence, falls into the following categories: use by federal civil law enforcement officers of material and equipment furnished by the United States Army and the South Dakota National Guard; the presence of United States Army personnel who were ordered to Wounded Knee to observe and report to the President through the Department of Defense the necessity of calling in federal troops; the drafting by military personnel of contingency plans to be used by the United States Army in the event that federal military intervention was ordered by the President; aerial photographic reconnaissance service provided by the United States Air Force and the Nebraska National Guard; the advice, urging and counsel given by the United States Army personnel to Department of Justice personnel on the subjects of negotiations, logistics and rules of engagement; and the maintenance of military vehicles performed by members of the Nebraska National Guard," United States v. McArthur, 419 F.Supp. at 193 n.3.

[2063] "(a) The Secretary of Defense may in accordance with other applicable law, provide to Federal, State or local civilian law enforcement officials any information collected during the normal course of military training or operations that may be relevant to a violation of any Federal or State law within the jurisdiction of such officials.

section allows the use of military undercover agents and the collection of intelligence concerning civilian activities only where there is a nexus to an underlying military purpose.[2064]

"(b) The needs of civilian law enforcement officials for information shall, to the maximum extent practicable, be taken into account in the planning and execution of military training or operations.

"(c) The Secretary of Defense shall ensure, to the extent consistent with national security, that intelligence information held by the Department of Defense and relevant to drug interdiction or other civilian law enforcement matters is provided promptly to appropriate civilian law enforcement officials," 10 U.S.C. 371.

"The phrase `in accordance with other applicable law' as used in section 371 is meant to continue the application of the Privacy Act to this type of intelligence sharing. . . . [Congress did] not intend the military to engage in the routine collection of intelligence information about United States residents. . . [and] noting in this section [was] intended to modify in any way existing law with respect to the military's authority (or lack thereof) to collect and disseminate intelligence information about American citizens and residents here and abroad. See e.g., Executive Order 12036," H.R.Rep.No.97-71 pt.2, 8, reprinted in 1981 UNITED STATES CODE, CONGRESSIONAL AND ADMINISTRATIVE NEWS 1785, 1791.

[2064] "The Committee adopted the view of the Department of Justice that the weight of authority on the Posse Comitatus Act `prohibits the use of miliary personnel as informants, undercover agents, or non-custodial interrogators in a civilian criminal investigation that does not involve potential military defendants or is not intended to lead to any official action by the armed forces.' . . . [W]hen military personnel become aware of violations of civilian laws as an incidental result of other militaryoperations, such information may be voluntarily disclosed.

"Examples of this type of information sharing include situations such as investigations of military and non-military coconspirators and the observation by military personnel of illegal conduct during a routine military mission or training operation.

"The Committee anticipates, however, that an increased sensitivity to the needs of civilian law enforcement officials, particularly in drug enforcement, will permit more compatible mission planning and execution. For example, the scheduling of routine training missions can easily accommodate the need for improved intelligence information concerning drug trafficking in the Caribbean. The committee does not intend the military to engage in the routine collection of intelligence information about United States residents. Thus, the legislation creates no risk that the military will return to the abuses exposed in previous Congressional hearings. See Hearings on Federal Data Banks, Computers and the Bill of Rights before the Committee on Constitutional Rights, Committee on the Judiciary, United States Senate, 92nd Cong., 1st sess." H.R.Rep.No. 91-71, 8 & 8 n.1.

The staff report following the Federal Data Banks hearings noted that, "the U.S. Army had for several years maintained a close and pervasive watch over most civilian protest activity throughout the United States. At its height during the lat 1960's, the monitoring drew upon the part-time services of at least 1,500 plainclothes agents of the Army Intelligence Command, and an unspecified number of agents from the Continental Army Command. Their reports, which described the nonviolent political activities of thousands of individuals and organizations unaffiliated with the armed forces were amassed in scores of data centers. . . . The picture is that of a runaway intelligence bureaucracy unwatched by its civilian superiors, eagerly grasping for information about political dissenters of all kinds and totally oblivious to the impact its spying

---

Section 373 permits military personnel to train civilian police on "the operation and maintenance of equipment" and to provide them with "expert advice."[2065] The section was originally limited to equipment provided by the armed forces,[2066] but was expanded in 1988 to include training on any equipment regardless of its origin.[2067]

---

could have on the constitutional liberties it had sworn to defend." Military Surveillance of Civilian Politics: A Report of the Subcommittee on Constitutional Rights of the Senate Committee on the Judiciary, 93d Cong., 1st Sess. 10 (1973)(Comm.Print).

For a more contemporary examination of the issues associated with military surveillance of off-base political protests see, Peterson, Civilian Demonstrations Near the Military Installation: Restraints on Military Surveillance and Other Activities, 140 MILITARY LAW REVIEW 113 (Spring, 1993).

[2065] "The Secretary of Defense may, in accordance with other applicable law, make Department of Defense personnel available -- (1) to train Federal, State, and local civilian law enforcement officials in the operation and maintenance of equipment, including equipment made available under section 372 of this title; and (2) to provide such law enforcement officials with expert advice relevant to the purposes of this chapter," 10 U.S.C. 373.

[2066] "Nothing in this section contemplates the creation of large scale or elaborate training programs . . . . [This section would not authorize the routine use of a Green Beret training course for urban SWAT teams.] . . . Rather this section anticipates the continuing need for the military to train civilians in the operation and maintenance of the equipment lent under proposed section 372," H.R.Rep.No. 97-71, at 10, reprinted in 1981 UNITED STATES CODE, CONGRESSIONAL AND ADMINISTRATIVE NEWS 1785, 1792-793 (footnote 2 of the report in brackets).

[2067] "Paragraph (1) clarifies current law to provide that the Secretary of Defense, in accordance with applicable law, may make Department of Defense personnel available to train Federal, State, and local civilian law enforcement officials in the operation of maintenance of equipment, including equipment made available under section 372," H.R.Rep.No. 100-989, 451, reprinted in 1988 United States Code Congressional and Administrative News 2503, 2579. See also, DoD Dir.No. 5525.5 (Encl.4) A.4., "a. The Military Departments and Defense Agencies may provide training to Federal, State, and local civilian law enforcement officials, Such assistance may including training in the operation and maintenance of equipment made available under section A. of enclosure 3. This does not permit large scale or elaborate training, and does not permit regular or direct involvement of military personnel in activities that are fundamentally civilian law enforcement operations, except as other wise authorized in this enclosure.

"b. Training of Federal, State, and local civilian law enforcement officials shall be provided under the following guidance:

"(1) This assistance shall be limited to situations when the use of non-DoD personnel would be unfeasible or impractical form a cost or time perspective and would not otherwise compromise national security or military preparedness concerns.

"(2) Such assistance may not involve DoD personnel in a direct role in a law enforcement operation, except as otherwise authorized by law.

The explanation of what might constitute "expert advice" is limited, but Congress clearly did not use the phrase as a euphemism for active military participation in civilian police activity.[2068]

Equipment and Facilities

Abstractly it might seem that even civilian use -against Americans within the United States -- of tanks, missiles, fighter planes, aircraft carriers and other implements of war offends the Posse Comitatus Act even if use can be accomplished without the direct involvement of military personnel. The arsenal of American military weapons and equipment are "part of the Army and Air Force" even when turned over to civilian authorities before use for civilian purposes. Even if the Posse Comitatus Act were read to apply only to the use of personnel, would the use of military personnel to maintain equipment loaned to civilian authorities violate the Act's proscription? The Wounded Knee cases provided conflicting answers.

The 1981 provisions make it clear that the Defense Department may provide civilian police with military equipment[2069] and under some circumstances,

---

"(3) Except as otherwise authorized by law, the performance of such assistance by DoD personnel shall be at a location where there is not a reasonable likelihood of a law enforcement confrontation."

[2068] "Neither does the authority to provide expert advice create a loophole to allow regular or direct involvement of military personnel in what are fundamentally civilian law enforcement operations," H.R.Rep.No. 97-71, at 10, reprinted in 1981 UNITED STATES CODE, CONGRESSIONAL AND ADMINISTRATIVE NEWS 1785, 1792.

"Paragraph (2) restates current law permitting advice. Such training and expert advice may extend to instruction in the operation of equipment, scientific analysis, translations, and assistance in strategic planning, but may not extend to direct, active involvement in specific law enforcement operations," H.R.Rep.No. 100-989, 451, reprinted in 1988 United States Code Congressional and Administrative News 2503, 2579. See also, DoD Dir.No. 5525.5 (Encl.4) A.5., "Military Departments and Defense Agencies may provide expert advice to Federal, State, or local law enforcement in accordance with 10 U.S.C. §§371-378 (reference (d)). This does not permit regular or direct involvement of military personnel in activities that are fundamentally civilian law enforcement operations, except as otherwise authorized in this enclosure."

[2069] "The Secretary of Defense may, in accordance with other applicable law, make available any equipment (including associated supplies or spare parts), base facility, or research facility of the Department of Defense to any Federal, State, or local civilian law enforcement official for law enforcement purposes," 10 U.S.C. 372.

See also 10 U.S.C. 381:

"(a) The Secretary of Defense, in cooperation with the Attorney General, shall conduct an annual briefing of law enforcement personnel of each State (including law enforcement personnel of the political subdivisions of each State) regarding information, training, technical support, and

---

particularly in drug cases, may also supply military personnel to operate and maintain such equipment.[2070] The provisions also include extraordinary authority to use Navy ships to support Coast Guard drug interdiction on the high seas.[2071]

---

equipment and facilities available to civilian law enforcement personnel from the Department of Defense.

"(b) Each briefing conducted under subsection (a) shall include the following: (1) An explanation of the procedures for civilian law enforcement officials --(A) to obtain information, equipment, training, expert advice, and other personnel support under this chapter; and (B) to obtain surplus military equipment. (2) A description of the types of information, equipment and facilities, and training and advice available to civilian law enforcement officials from the Department of Defense. (3) A current, comprehensive list of military equipment which is suitable for law enforcement officials form the Department of Defense and available as surplus property from the Administrator of General Services.

"(c) The Attorney General and the Administrator of General Services shall --(1) establish or designate an appropriate office or offices to maintain the list described in subsection (b)(3) and to furnish information to civilian law enforcement officials on the availability of surplus military equipment; and (2) make available to civilian law enforcement personnel nationwide, tollfree telephone communication with such office or offices."

[2070] "(a) The Secretary of Defense may, in accordance with other applicable law, make Department of Defense personnel available for the maintenance of equipment for Federal, State, and local civilian law enforcement officials, including equipment made available under section 372 of this title.

"(b)(1) Subject to paragraph (2) and in accordance with other applicable law, the Secretary of Defense may, upon request from the head of a Federal law enforcement agency, make Department of Defense personnel available to operate equipment (including equipment made available under section 372 of this title) with respect to -- (A) a criminal violation of a provision of law specified in paragraph (4)(A); or (B) assistance that such agency is authorized to furnish to a State, local, or foreign government which is involved in the enforcement of similar laws. (2) Department of Defense personnel made available to a civilian law enforcement agency under this subsection may operate equipment for the following purposes:

"(A) Detection, monitoring, and communication of the movement of air and sea traffic.

"(B) Detection, monitoring, an communication of the movement of surface traffic outside the geographic boundary of the United States and within the United States not to exceed 25 miles of the boundary if the initial detection occurred outside the boundary.

"(C) Aerial reconnaissance.

"(D) Interception of vessels or aircraft detected outside the land area of the United States for the purposes of communicating with such vessel and aircraft to direct such vessels and aircraft to go to a location designated by appropriate civilian officials.

"(E) Operation of equipment to facilitate communications in connection with law enforcement programs specified in paragraph (4)(A).

"(F) Subject to joint approval by the Secretary of Defense and the Attorney General (and the Secretary of State in the case of a law enforcement operation outside the land area of the United

States) -- (i) the transportation of civilian law enforcement personnel; and (ii) the operation of a base of operations for civilian law enforcement personnel.

"(3) Department of Defense personnel made available to operate equipment for the purpose stated in paragraph (2)(D) may continue to operate such equipment into the land area of the United States in cases involving the pursuit of vessels or aircraft where the detection began outside such land area.

"(4) In this subsection: (A) The term `Federal law enforcement agency' means an agency with jurisdiction to enforce any of the following: (i) The Controlled Substances Act (21 U.S.C. 801 et seq.) or the Controlled Substances Import and Export Act (21 U.S.C. 951 et seq.). (ii) Any of sections 274 through 278 of the Immigration and Nationality Act (8 U.S.C. 1324-1328). (iii) A law relating to the arrival or departure of merchandise (as defined in section 401 of the Tariff Act of 1930 (19 U.S.C. 1401) into or out of the customs territory of the United states (as defined in general note 2 of the Harmonized Tariff Schedules of the United States) or any other territory or possession of the United States. (iv) The Maritime Drug Law Enforcement Act (46 U.S.C. 1001 et seq.).

"(B) The term `land area of the United States' includes the land area of any territory, commonwealth, or possession of the United States.

"(c) The Secretary of Defense may, in accordance with other applicable law, make Department of Defense personnel available to any Federal, State, or local civilian law enforcement agency to operate equipment for purposes other than described in subsection (b)(2) only to the extent that such support does not involve direct participation by such personnel in a civilian law enforcement operation unless such direct participation is otherwise authorized by law," 10 U.S.C. 374.

"(a) Procedures. (1) The Secretary of Defense shall establish procedures in accordance with this subsection under which States and units of local government may purchase law enforcement equipment suitable for counter-drug activities through the Department of Defense. The procedures shall require the following: (A) Each State desiring to participate in a procurement of equipment suitable for counter-drug activities through the Department of Defense shall submit to the Department, in such form and manner and at such times as the Secretary prescribes, the following: (i) a request for law enforcement equipment. (ii) Advance payment for such equipment, in an amount determined by the Secretary based on estimated or actual costs of the equipment and administrative costs incurred by the Department. (B) A State may include in a request submitted under subparagraph (A) only the type of equipment listed in the catalog produced under subsection (c). (C) A request for law enforcement equipment shall consist of an enumeration of the law enforcement equipment that is desired by the State and units of local government within the State. The Governor of a State may establish such procedures as the Governor considers appropriate for administering and coordinating requests for law enforcement equipment from units of local government within the State. (D) A State requesting law enforcement equipment shall be responsible for arranging and paying for shipment of the equipment to the State and localities within the State. (2) In establishing the procedures, the Secretary of Defense shall coordinate with the General Services Administration and other Federal agencies for purposes of avoiding duplication of effort.

"(b) Reimbursement of Administrative Costs. -- In the case of any purchase made by a State or unit of local government under the procedures established under subsection (a), the Secretary of Defense shall require the State or unit of local government to reimburse the Department of Defense for the administrative costs to the Department of such purchase.

Limitations: Military Preparedness, Reimbursement, and Direct Use

The authority granted in sections 371-381 is subject to three general caveats. It may not be used to undermine the military capability of the United States.[2072]

"(c) GSA Catalog. -- The Administrator of General Services, in coordination with the Secretary of Defense shall produce and maintain a catalog of law enforcement equipment suitable e for counter-drug activities for purchase by States and units of local government under the procedures established by the Secretary under this section.

"(d) Definitions. -- In this section: (1) The term `State' includes the District of Columbia, the Commonwealth of Puerto Rico, the Commonwealth of the Northern Mariana Islands, and any territory or possession of the United States. (2) The term `unit of local government' means any city, county, township, town, borough, parish, village, or other general purpose political subdivision of a State; an Indian tribe which performs law enforcement functions as determined by the Secretary of the Interior; or any agency of the District of Columbia government or the United States Government performing law enforcement functions in and for the District of Columbia or the Trust Territory of the Pacific Islands. (3) The term `law enforcement equipment suitable for counter-drug activities' has the meaning given such term in regulations prescribed by the Secretary of Defense. In prescribing the meaning of the term, the Secretary may not include any equipment that the Department of Defense does not procure for its own purposes" 10 U.S.C. 381.

[2071] "(a) The Secretary of Defense and the Secretary of Transportation shall provide that there be assigned on board every appropriate surface naval vessel at sea in a drug-interdiction area members of the Coast Guard who are trained in law enforcement and have powers of the Coast Guard under title 14, including the power to make arrests and to carry out searches and seizures.

"(b) Members of the Coast Guard assigned to duty on board naval vessels under this section shall perform such law enforcement functions (including drug-interdiction functions) -- (1) as may be agreed upon by the Secretary of Defense and the Secretary of Transportation; and (2) as are otherwise within the jurisdiction of the Coast Guard.

"(c) No fewer than 500 active duty personnel of the Coast Guard shall be assigned each fiscal year to duty under this section. However, if at any time the Secretary of Transportation, after consultation with the Secretary of Defense, determines that there are insufficient naval vessels available for purposes of this section, such personnel may be assigned other duty involving enforcement of laws listed in section 374(b)(4)(A) of this title.

"(d) In this section, the term `drug-interdiction area' means an area outside the land area of the United States (as defined in section 374(b)(4)(B) of this title) in which the Secretary of Defense (in consultation with the Attorney General) determines that activities involving smuggling of drugs into the United States are ongoing," 10 U.S.C. 379.

[2072] "Support (including the provision of any equipment or facility or the assignment or detail of any personnel) may not be provided to any civilian law enforcement official under this chapter if the provision of such support will adversely affect the military preparedness of the United States. The Secretary of Defense shall prescribe such regulations as may be necessary to ensure that the provision of any such support does not adversely affect the military preparedness of the United States," 10 U.S.C. 376.

The civilian beneficiaries of military aid must pay for the assistance.[2073] And the Secretary of Defense must issue regulations to ensure that the authority of sections 371 to 381 does not result in use of the armed forces to make arrests or conduct searches and seizures solely for the benefit of civilian law enforcement.[2074]

For several years, the regulations called for by section 375 appeared in parallel form in the Code of Federal Regulations[2075] and in a Defense Department Directive.[2076] The heart of the regulations appeared in subsection 213.10(a)(3), "Except as otherwise provided in this enclosure, the prohibition on use of military personnel `as a posse comitatus or otherwise to execute the laws' prohibits the following forms of direct assistance: (i) Interdiction of a vehicle, vessel, aircraft or other similar activity. (ii) A search or seizure. (iii) An arrest, stop and frisk, or similar activity. (iv) Use of military personnel for surveillance or pursuit of individuals, or as informants, undercover agents, investigators, or interrogators," 32 CFR §213.10(a)(3)(July 1, 1992). Although the provisions have been removed from the CFR, the Directive remains in effect.[2077]

[2073] "(a) To the extent otherwise required by section 1535 of title 31 (popularly known as the `Economy Act') or other applicable law the Secretary of Defense shall require a civilian law enforcement agency to which support is provided under this chapter to reimburse the Department of Defense for that support.

"(b) An agency to which support is provided under this chapter is not required to reimburse the Department of Defense for such support if such support -- (1) is provided in the normal course of military training or operations; or (2) results in a benefit to the element of the Department of Defense providing the support that is substantially equivalent to that which would otherwise be obtained from military operations or training," 10 U.S.C. 377.

[2074] "Secretary of Defense shall prescribe such regulations as may be necessary to ensure that any activity (including the provision of any equipment or facility or the assignment or detail of any personnel) under this chapter does not include or permit direct participation by a member of the Army, Navy, Air Force, or Marine Corps in a search, seizure, arrest, or other similar activity unless participation in such activity by such member is otherwise authorized by law," 10 U.S.C. 375.

[2075] 47 Fed.Reg. 14899 (April 7, 1982), codified at, 32 CFR pt.213, removed, 58 Fed.Reg. 25776 (April 28, 1993).

[2076] Department of Defense Directive No. 5525.5 (January 15, 1986), as amended December 12, 1989, hereafter referred to as DoD Dir.No. 5525.5. Prior to enactment of 10 U.S.C. 371381, the Navy had operated under a Navy Department Instruction of similar import, SECNAVINST 5400.12 (January 17, 1969), see United States v. Walden, 490 F.2d 372, 37374 (4th Cir. 1974).

[2077] The provision in DoD Dir. No. 5525.5 (Encl.4) reads, "Except as otherwise provided in this enclosure, the prohibition on the use of military personnel `as a posse comitatus or otherwise to execute the laws' prohibits the following forms of direct assistance: a. Interdiction of a vehicle, vessel, aircraft, or other similar activity. b. A search or seizure. c. An arrest, apprehension, stop and frisk, or similar activity. d. Use of military personnel for surveillance or pursuit of individuals, or as undercover agents, informants, investigators, or interrogators," DoD Dir. No. 5525.5 (Encl.4) §A.3.

Military Purpose

The armed forces, when in performance of their military responsibilities, are beyond the reach of the Posse Comitatus Act and its statutory and regulatory supplements. Analysis of constitutional or statutory exceptions is unnecessary in such cases. The original debates make it clear that the Act was designed to prevent use of the armed forces to execute civilian law. Congress did not intend to limit the authority of the Army to perform its military duties. The legislative history, however, does not resolve the question of whether the Act prohibits the Army from performing its military duties in a manner which affords incidental benefits to civilian law enforcement officers.

The courts and commentators believe that it does not.[2078] As long as the primary purpose of an activity is to address a military purpose, the activity need not be abandoned simply because it also assists civilian law enforcement efforts. Courts appear to view the location of the activity as particular indicative of primary purpose; as one court noted, "the power to maintain order, security, and discipline on a military facility is necessary for military operations."[2079]

The courts have concluded that, consistent with this legitimate military purpose to maintain order on military installations, military personnel may, without violating the Posse Comitatus Act, may turn over to civilian law enforcement authorities armed felons arrested when they flee onto a military base, Harker v. State, 663 P.2d 932, 936 (Alaska 1983), or drunk drivers arrested on a military base,[2080] or firearms stolen from a military installation, United States v. Griley, 814 F.2d 967, 976 (4th Cir. 1987). The courts have likewise found no violation of the Act when military personnel arrest civilians on military facilities for crimes committed there, United States v. Banks, 539 F.2d 14, 16 (9th Cir. 1976), or when military authorities assist a civilian police investigation conducted on a military

---

[2078] Logic might suggest that the military purpose doctrine is simply the largest of the statutory exceptions, that is, that the doctrine merely encompasses the military authority vested in the armed forces under the Code of Military Justice and the other statutes which grant them military authority. Neither the commentators nor the courts have ordinarily clearly limit their analyses in such terms, see e.g., Meeks, Illegal Law Enforcement: Aiding Civil Authorities in Violation of the Posse Comitatus Act, 70 MILITARY LAW REVIEW 83, 124-26 (Fall, 1975); Rice, New Laws and Insights Encircle the Posse Comitatus Act, 104 MILITARY LAW REVIEW 109, 128-35 (Spring, 1984); Hayes v. Hawes, 921 F.2d 100, 103 (7th Cir. 1990); Taylor v. State, 640 So.2d 1127, 1136 (Fla.App. 1994); State v. Pattioay, 78 Haw. 455, 459-62, 896 P.2d 911, 915-18 (1995).

[2079] Eggleston v. Dept. of Revenue, 895 P.2d 1169, 1170 (Colo.App. 1995), citing Cafeteria & Restaurant Workers Union Local v. McElroy, 367 U.S. 886 (1961).

[2080] Eggleston v. Dept. of Revenue, 895 P.2d 1169 (Colo.App. 1995)(military police also administered breath test and provided local law enforcement officers with the results); McNeil v. State, 787 P.2d 1036, 1037 (Alaska App. 1990); Anchorage v. King, 754 P.2d 283, 286 (Alaska App. 1988).

facility.[2081] The military purpose doctrine likewise permits military law enforcement personnel to investigate the off-base conduct of military personnel.[2082] The DoD Directive evidences a comparable understanding.[2083]

[2081] People v. Caviano, 148 Misc.2d 426, 560 N.Y.S.2d 932, 936-37 (N.Y.S.Ct. 1990)(Navy personnel made a sailor available for questioning at naval station facilities; the interrogation was conducted by civilian police who subsequently arrested the sailor for an out of state robbery); United States v. Hartley, 678 F.2d 961, 978 (11th Cir. 1982)(military inspectors who discovered evidence of fraudulent conduct by defense contractors "aided the civilian employee in charge of the investigation only to the extent of activities normally performed in the ordinary course of their [military] duties"); State v. Trueblood, 265 S.E.2d 662, 664 (N.C.App. 1980)(military search (with consent) of on-base quarters in connection with a civilian investigation of off-base drug dealing by military personnel); State v. Nelson, 298 N.C. 573, 260 S.E.2d 629 (1979)(military inventory of personal effects of AWOL soldier were conducted primarily for a military purpose pursuant to a regulation designed to safeguard private property and protect service against claims); Commonwealth v. Shadron, 370 A.2d 697, 699 (Pa. 1977)(military police acting within the scope their authority did not violate the Act by making a soldier available, at the Air Force base where he was stationed, to civilian investigators for interrogation by the civilian officers and by permitted the civilians to search the defendant's possessions with his consent).

[2082] United States v. Griley, 814 F.2d 967, 976 (4th Cir. 1987)(off-base military investigation of concerning property stolen on-base by military personnel); Applewhite v. United States, 995 F.2d 997, 1001 (10th Cir. 1993)(military police off-base drug sting targeting military personnel); State v. Hayes, 102 N.C.App. 777, 404 S.E.2d 12 (1991)(off-base purchase of drugs by a military undercover agent from an AWOL soldier); State v. Poe, 755 S.W.2d 41 (Tenn. 1988)(military investigation of the off-base murder of a soldier by other soldiers).

[2083] 2. Permissible direct assistance. The following activities are not restricted by reference

(v) [the Posse Comitatus Act, 18 U.S.C. 1385].

a. Actions that are taken for the primary purpose of furthering a military or foreign affairs function of the United States, regardless of incidental benefits to civilian authorities. This provisions must be used with caution, and does not include actions taken for the primary purpose of aiding civilian law enforcement officials or otherwise serving as a subterfuge to avoid the restrictions of reference (v). Actions under this provision may include the following, depending on the nature of the DoD interest and the authority governing the specific action in question:

(1) Investigations and other actions related to enforcement of the Uniform Code of Military Justice (UCMJ)(reference (d)).

(2) Investigations and other actions that are likely to result in administrative proceedings by the Department of Defense, regardless of whether there is a related civil or criminal proceeding. See DoD Directive 5525.7 (reference (w)) with respect to matters in which the Departments of Defense and Justice both have an interest.

(3) Investigations and other actions related to the commander's inherent authority to maintain law and order on a military installation or facility.

(4) Protection of classified military information or equipment.

(5) Protection of DoD personnel, DoD equipment, and official guests of the Department of Defense.

Cases called to apply the military purpose doctrine in cooperative police activities occurring off-base are the most difficult to reconcile. Some seem to require no more than a logical military nexus,[2084] others demand a very clear, specific

---

(6) Such other actions that are undertaken primarily for a military or foreign affairs purpose, DoD Dir.No. 5525.5 (Encl. 4) A.2.a. (32 CFR §213.10(2)(i)(July 1, 1992) was identical except for styles used to designate subsections, paragraphs and subparagraphs and that the CFR contained no cross reference citations except to the Code of Military Justice).

[2084] State v. Sanders, 303 N.C. 608, 613, 281 S.E.2d 7, 10 (1981)("military policeman Lambert's duty [during joint patrol with civilian police off-base] was not to execute civilian law but to assist the police department in returning apprehended military personnel to Fort Bragg"); State v. Short, 113 Wash.2d 35, 36-7 & 39, 775 P.2d 458, 458-59 & 460 (1989)("the Naval Investigative Services (NIS) instigated a joint drug operation with local law enforcement agencies . . . . NIS brought in Agent Jerry Kramer, a civilian Navy employee, to work undercover. . . . Kramer became employed as a bouncer at Noodles, a local restaurant where drug contacts were made. In this position, Kramer checked the ID of persons entering the bar and determine that about 80 percent of those entering Noodles were military personnel. While employed at Noodles Kramer met James Corso and, later, the defendant Larry K. Short. . . . Corso indicated that Kramer could buy more cocaine through Short. Kramer and Corso waited at Noodles until Short arrived. After a brief discussion, Kramer gave Short $250 to get some cocaine. Corso and Short left Noodles together and returned an hour later. Corso entered the bar and delivered a foil package to Kramer. Kramer delivered the alleged cocaine along with information about Corso and Short, to his immediate supervisor, Agent Kocina. A Washington State Patrol Crime Laboratory analysis revealed that the substance was not cocaine. . . . Kramer still undercover complained to Short about the counterfeit and demanded reimbursement. Short promised to replace the fake cocaine with real cocaine [but did not]. Short was arrest later by local authorities and convicted . . . for selling a substitute substance in lieu of a controlled substance [to Kramer]. . . . Case law discloses that the use of equipment, personnel, and information is generally not considered direct participation under 10 U.S.C. §371 or under the posse comitatus act. . . . Here, Kramer did not arrest Short, and any personnel, equipment, and information provided to local law enforcement did not constitute direct participation"); People v. Wells,175 Cal. 876, 878, 221 Cal.Rptr. 273, 273-74 (1985)("with the goal of taking illegal drug dealers off the streets of the City of Oceanside and thus minimizing the flow of drugs into nearby Camp Pendleton, the Naval Investigative Service (N.I.S.) initiated what N.I.S. calls an Initiative Criminal Investigative Operation by soliciting the assistance of the Oceanside Police Department (O.P.D.). . . . The operational plan called for the N.I.S. agents, all military policemen, to be used as confidential informants immediately under the supervision and surveillance of a particular O.P.D. officer. Solicitation for drugs was to be done by N.I.S. agents. Any detention or arrest of a suspect was to be handled by an O.P.D. officer. The N.I.S. agent always was accompanied within a matter of feet or yards by an O.P.D. officer. On most occasions, the N.I.S. agent was equipped with a concealed transmitter. O.P.D. furnished prerecorded money to N.I.S. agents to make drug purchases and, once a purchase was completed by an N.I.S. agent, the suspected drugs were turned over to an O.P.D. officer to be impounded and analyzed. O.P.D. paid nothing to N.I.S. for its assistance. Several operations were carried out according to the plan. . . . In light of the language, background and apparent purposes of the Posse Comitatus Act to stop state use of the federal militia, particularly in policing state elections and to prevent the subjugation of citizens to the exercise of military power of a regulatory, prescriptive or compulsory nature, we find no violation of the act in the facts of this case").

---

military connection before they will concede the presence of a military purpose,[2085] and still others seem to seek a middle ground.[2086]

[2085] In Walden, for example, where a Treasury agent was found to have used Marines as undercover agents to secure evidence against civilian firearms offenders, the court found a breach of the Posse Comitatus requirements without even acknowledging the government's military purpose argument, United States v. Walden, 490 F.2d 372 (4th Cir. 1974); Meeks, Illegal Law Enforcement: Aiding Civil Authorities in Violation of the Posse Comitatus Act, 70 MILITARY LAW REVIEW 83, 115 (Fall, 1975)("the Government argued [in Walden] that the Act had not been violated because the investigation was `related directly to the maintenance of order and security` on the base and that such undercover assistance to civilian authorities does not constitute `execution of the law'"); Rice, New Laws and Insights Encircle the Posse Comitatus Act, 104 MILITARY LAW REVIEW 109, 129 (Spring, 1984)("[i]f the court considered the government's argument that the activities of the Marines were related to the maintenance, order and security of the base, it had rejected it. However, the sale of the weapons occurred immediately off the base in the town of Quantico. If the base authorities were aware of this fact and that the illegally sold weapons were being purchased by Marines and being brought on the base, then what may they do to insure order and discipline? Clearly, they can notify local authorities. But would the purchase in question by an undercover Marine be for the primary purpose of furthering a military function? Order, discipline, and security of a base is a military function"); State v. Pattioay, 78 Haw. 455, 464-65, 896 P.2d 911, 920-21 (1995)("[w]here the target of a military investigation is a civilian and there is no verified connection to military personnel, the PCA prohibits military participation in activities designed to execute civilian laws. People v. Tyler (Tyler I), 854 P.2d 1366 (Colo.App. 1993), rev'd on other grounds, 874 P.2d 1037 (Colo. 1994) (Tyler II). . . . In fact, the apparent justification for the military involvement in the instant case was to facilitate the enforcement of civilian laws. In Tyler I, the Colorado Court of Appeals stated: `before the military may directly participate in an undercover investigation of these civilians and their off-base activities, the state carries the burden of demonstrating that there exists a nexus between drug sales off base by civilians to military personnel and the military base at which the purchasers are stationed. . . . Hence, the prosecution has the duty to present evidence to show that, when a military investigation was undertaken, the targeted drug transactions involved military personnel or were connected to sales conducted on a military installation.' 854 P.2d at 1369 [emphasis of the Pattioay court]; see also Moon [v. State, 785 P.2d 45,] 46-47 [(Alaska App. 1991),]. Furthermore, we agree with the observation in Chief Justice Rabinowitz's dissent in Kim v. State, supra [817 P.2d 467 (Alaska 1991)]; he observed that an independent military interest in the health and safety of its personnel does not establish a `military function' or `primary [military] purpose' under 32 CFR §213.10(a)(2)(1). 817 P.2d at 471 & 471 n.10. That the military has a valid interest in ferreting out those who supply drugs to military personnel, does not automatically qualify its aid to civilian drug law enforcement as having the `primary purpose of furthering a military . . . function'").

[2086] Moon v. State, 785 P.2d 45, 48 (Alaska App. 1990)("[I]t seems to us that the army had a valid military purpose in preventing illicit drug transactions involving active duty personnel even if the transaction took place off base. The investigation was not begun until the military was satisfied that drug dealers at the Palace Hotel had targeted military personnel as a market. It was also reasonable to infer that a substantial quantity of illicit drugs was finding its way onto the base"); State v. Maxwell, 328 S.E.2d 507, 509 (W.Va. 1985)(same); State v. Presgraves, 328 S.E.2d (W.Va. 1985)(same); Hayes v. Hawes, 921 F.2d 100, 103-104 (7th Cir. 1990)(no violation where Navy undercover agent, who had "received information" a that a sailor had purchased drugs at an off-base arcade, with several other military agents joined local police for surveillance of the arcade, made a drug buy in cooperation with local police who made the arrest and conducted the search of civilian).

Willfully Execute the Laws

Willful

The Act is limited to "willful" misuse of the Army or Air Force.[2087] The Senate version of the original Act would have limited proscription to "willful and knowing" violations, 7 Cong.Rec. 4302 (1878); the House version had no limitation, 7 Cong.Rec. 4181 (1878). The compromise which emerged from conference opted to forbid only willful violations but neither the statements of the managers nor statements elsewhere in the debate explain what the limitation means. And the scattered statements found in the case law under the Act are somewhat conflicting and not particularly helpful,[2088] although it seems unlikely that a court would convict for anything less than a deliberate disregard of the law's requirements.

Execute the Law

[2087] Whoever, except in cases and under circumstances expressly authorized by the Constitution or Act of Congress, willfully uses any part of the Army or the Air Force as a posse comitatus or otherwise to execute the laws shall be fined under this title or imprisoned not more than two years, or both. 18 U.S.C. 1385 (emphasis added).

[2088] United States v. Walden, 490 F.2d 372, 276 (4th Cir. 1974)("there is totally lacking any evidence that there was a conscious, deliberate or willful intent on the part of the Marines or the . . . Special Investigator to violate the Instruction or the spirit of the Posse Comitatus Act. From all that appears, the Special Investigator acted innocently albeit ill-advisedly"); State v. Danko, 219 Kan. 490, 548 P.2d 819, 822 (1976)("the statute is limited to deliberate use of armed force for the primary purpose of executing civilian laws")(quoting Furman, Restrictions Upon Use of the Army Imposed by the Posse Comitatus Act, 7 MILITARY LAW REVIEW 85, 128 (1960)); Kim v. State, 817 P.2d 467, 469 n.2 (Alaska, 1991)(Rabinowitz, J. dissenting)("A will to violate the Act is not required, but only the wilful use of military personnel").

In other instances, Congress has used the term "willful" in a number of different ways and the term "has been construed by the courts in a variety of ways, often inconsistent and contradictory. The courts have defined a `willful' act as an act done voluntarily as distinguished from accidentally, an act doe with specific intent to violate the law, an act done with bad purpose, an act done without justifiable excuse, an act done stubbornly, an act done without grounds for believing it is lawful, and an act done with careless disregard whether or not one has the right so to act," S.Rep.No. 307, 97th Cong., 1st Sess. 64 (1981).

Recent Supreme Court cases seem to caution against a broad interpretation of the term "willful" or any of the other state-of-mind elements in federal criminal statute, Bryan v. United States, 524 U.S. 184, 191-92 (1998)(“The word willfully is sometimes said to be a word of many meanings whose construction is often dependent on the context in which it appears. . . . As a general matter, when used in the criminal context, a willful act is one undertaken with a bad purpose. In other words, in order to establish a willful violation of a statute, the Government must prove that the defendant acted with knowledge that his conduct was unlawful”)(citing Ratzlaf v. United States, 510 U.S. 135, 137 (1994)).

When has the Army or Air Force been used "to execute the laws"? The language of the Act by itself seems very sweeping.[2089] It is comparable to the instruction of the Constitution that the President "take care that the laws are faithfully executed," U.S. Const. Art.II, §3. Without more, it would seem to prohibit the use of the Army or the Air Force to implement the command or authorization of all state or federal law. It might apply with equal force to delivering the mail or making an arrest.

Existing case law and commentary indicate that "execution of the law" in violation of the Posse Comitatus Act occurs (a) when the armed forces perform tasks ordinarily assigned not to them but to an organ of civil government, or (b) when the armed forces perform tasks assigned to them solely for purposes of civilian government.

While inquiries may surface in other contexts such as the use of the armed forces to fight forest fires or to provide assistance in the case of other natural disasters,[2090] Posse Comitatus Act questions arise most often when the armed forces assist civilian police. This is perhaps not surprising since it is the use that

---

[2089] Whoever, except in cases and under circumstances expressly authorized by the Constitution or Act of Congress, willfully uses any part of the Army or the Air Force as a posse comitatus or otherwise to execute the laws shall be fined under this title or imprisoned not more than two years, or both. 18 U.S.C. 1385 (emphasis added).

[2090] See e.g., Copeland & Lamb, Disaster Law and Hurricane Andrew: Government Lawyers Leading the Way to Recovery, 27 URBAN LAWYER 1 (1995); Delzompo, Warriors on the Fire Line: The Deployment of Service Members to Fight Fire in the United States, 1995 ARMY LAWYER 51 (April, 1995); Federal Disaster Assistance: Report of the Senate Task Force on Funding Disaster Relief, SEN. DOC.104-4 (1995).

Congress has recently established provisions which at first glance might appear to be a blanket statutory exception of military assistance to civil authorities for any purpose other than police activities ("[t]he Secretary of Defense shall establish a program to be known as the `Civil-Military Cooperative Action Program.' Under the program, the Secretary may, in accordance with other applicable law, use the skills, capabilities, and resources of the armed forces to assist civilian efforts to meet the domestic needs of the United States," 10 U.S.C. 410(a)). Upon closer examination, however, it becomes clear that legislation seeks to encourage activity that would not previously have violated the Posse Comitatus Act or its supplementary statutory and regulatory provisions ("The programs shall have the following objectives: (1) To enhance individual and unit training and morale in the armed forces through meaningful community involvement of the armed forces. (2) To encourage cooperation between civilian and military sectors of society in addressing domestic needs. (3) To advance equal opportunity. (4) To enrich the civilian economy of the United states through education, training, and transfer of technological advances. (5) To improve the environment and economic and social conditions. (6) To provide opportunities for disadvantaged citizens of the United States. . . . Nothing in this section shall be construed as authorizing -- (1) the use of the armed forces for civilian law enforcement purposes; or (2) the use of Department of Defense personnel or resources for any program, project, or activity that is prohibited by law," 10 U.S.C. 410(b),(e)); S.Rep.No. 102-352, 278-82 (1992); H.R.Rep.No. 102-966, 762, reprinted in 1992 UNITED STATES CODE, CONGRESSIONAL AND ADMINISTRATIVE NEWS 1769, 1853.

stimulated passage of the Act. During the debate, Members complained of various ways in which the Army had been used, essentially as a police force, to break up labor disputes, to collect taxes, to execute search and arrest warrants, and to maintain order at the polls and during state legislative sessions.[2091]

At least when suggested that the armed forces have been improperly used as a police force, the tests used by most contemporary courts to determine whether such military activity violates the Posse Comitatus Act were developed out of disturbances at Wounded Knee on the Pine Ridge Indian Reservation in South Dakota and inquiry:

(1) whether civilian law enforcement officials made a "direct active use" of military investigators to "execute the law";
(2) whether the use of the military "pervaded the activities" of the civilian officials; or
(3) whether the military was used so as to subject "citizens to the exercise of military power which was regulatory, prescriptive, or compulsory in nature." *Taylor v. State*, 640 So.2d 1127, 1136 (Fla.App. 1994).[2092]

The vast majority of cases called upon to apply these tests have found that the assistance provided civilian law enforcement did not constitute "execution of the law" in violation of Posse Comitatus Act requirements.[2093] Those most likely to

---

[2091] 5 Cong.Rec. 2113 (1877); 6 Cong.Rec. 294-307, 322; 7 Cong.Rec. 3538, 3581-582, 3850, 4245 (1878).

[2092] See also, United States v. Kahn, 35 F.3d 426, 431 (9th Cir. 1994); United States v. Yunis, 924 F.2d 1086, 1094 (D.C.Cir. 1991); Hayes v. Hawes, 921 F.2d 100, 104 (7th Cir. 1990); United States v. Gerena, 649 F.Supp. 1179, 1182 (D.Conn. 1986); United States v. Hartley, 678 F.2d 961, 978 n.24 (8th Cir. 1982); note the similarity to the tests used in the Wounded Knee Cases, United States v. Jaramillo, 380 F.Supp. 1375, 1379-380 (D.Neb. 1974), appeal dismissed, 510 F.2d 808 (8th Cir. 1975)(whether the use of military personnel affected or materially contributed to the activities of civilian law enforcement officials); United States v. Banks, 383 F.Supp. 368, 375 (D.S.D. 1974)(whether there was active participation of military personnel in civilian law enforcement activities); United States v. Red Feather, 392 F.Supp. 916, 921 (D.S.D. 1975)(whether there was direct active use of military personnel by civilian law enforcement officers); United States v. McArthur, 419 F.Supp. 186 (D.N.D. 1976), aff'd sub nom., United States v. Casper, 541 F.2d 1275, 1278 (8th Cir. 1976)(whether "Army or Air Force personnel [were] used by the civilian law enforcement officers in such manner that the military personnel subjected the citizens to the exercise of military power which was regulatory, prescriptive, or compulsory in nature, either presently or prospectively").

[2093] United States v. Yunis, 924 F.2d 1086, 1094 (D.C.Cir. 1991)(Navy transportation of prisoner in the custody the FBI); Hall v. State, 557 N.E.2d 3, 4-5 (Ind.App. 1990)(the [Air Force] Office of Special Investigations (OSI) asked Arthur Biles and Darryl Ivery, Air Force personnel, if they would be undercover agents to assist the Kokomo Police Department in drug investigations. . . . Biles and Ivery met with an OSI agent and Kokomo police officers to prepare for a controlled buy of cocaine. The police placed a body transmitter on Biles . . .. Hall met Biles and told him he could get him anything he wanted. . . . Biles gave [Hall sixty dollars ($60.00) to purchase one-half gram

fail the tests seem to be those where the activities appear to have a colorable military purpose but the government fails to make a convincing showing.[2094]

Military Coverage

---

of cocaine. Hall walked to his sister's car . . . and returned with the cocaine. Biles negotiated to buy two more bags of cocaine for one-hundred ten dollars. [Biles and Ivery testified at Hall's subsequent trial for dealing cocaine.] . . . Adopting the standard in [United States v.] McArthur, [419 F.Supp. 186 (D.N.D. 1975), aff'd, 541 F.2d 1275 (8th Cir. 1976)], we do not find that the acts of Biles and Ivery display the unauthorized exercise of military power that is `regulatory, prescriptive, or compulsory in nature); United States v. Bacon, 851 F.2d 1312 (11th Cir. 1988)("an active-duty army investigator assumed an undercover role in working jointlywith the . . . Sheriff's Department to ferret out a source of some of the cocaine being supplied to [the area for] both civilians and army personnel. . . . Army funds were used for some of the undercover drug `buys.' State and local funds were used for others. All drugs and other evidence gathered by Army Investigator Perkins were turned over to the state and local investigators for evidence in the prosecution of drug distributor Joe Bacon. . . . There was no `military permeation of civilian law enforcement.' In this case the limited military participation was nothing more than a case of assistance to civilian law enforcement efforts by military personnel and resources. This does not violate the statutory prohibition of the Posse Comitatus Act")[note that the courts do not seem to have accepted the proposition that military undercover participation without a primary military purpose is a per se violation of the Posse Comitatus Act or at least of DoD Dir. No. 5525.5 (Encl.4) A.3. ("except as otherwise provided in this enclosure, [e.g., when done primarily for a military purpose], the prohibition on the use of military personnel `as a posse comitatus or otherwise to execute the laws prohibits . . . d. Use of military personnel for surveillance. . . or as undercover agents. . . ."]);United States v. Hartley, 796 F.2d 112, 115 (5th Cir. 1986)(Air Force assistance to a customs agent tracking an aircraft suspected of smuggling marijuana into the United States);United States v. Gerena, 649 F.Supp. 1179, 1182 (D.Conn. 1986)(military transport of prisoner in the custody of the Marshals Service);Airway Heights v. Dilley, 45 Wash.App. 87, 92, 724 P.2d 407, 410 (1986)(use of Air Force technician and equipment to administer breathalyzer test).

[2094] E.g., Accord, Taylor v. State, 645 P.2d 522, 525 (Okla.Crim.[App.] 1982). See also, United States v. Walden, 490 F.2d 372 (4th Cir. 1974); Taylor v. State, 640 So.2d 1127, 1136 (Fla.App. 1994)("[m]ilitary participation in civilian law enforcement activities is restricted by the Federal Posse Comitatus Act, 18 U.S.C. 1385, and by 10 U.S.C. §375. Cases addressing this issue have ruled that where military involvement is limited and there is an independent military purpose, `the coordination of military police efforts with those of civilian law enforcement officials does not violate either [section 1385 or section 375].' Hayes v. Hawes, 921 F.2d 100, 103 (7th Cir. 1990). . . . In this case, the activities of the NIS [Naval Investigative Service] agents permeated the initial stages of the homicide investigation. Upon ascertaining that appellant [a sailor subsequently convicted in state court on two counts of first degree murder] purchased a one-way ticket to Virginia, the NIS agents obtained authorization form his commanding officer enabling them to arrest appellant on grounds of desertion for unauthorized absence. They agents traveled to Virginia, where they interviewed appellant's family members and kept them under surveillance. When appellant was found and taken into custody, the NIS agents questioned him about the homicides, obtained oral and written statements from him, and seized his clothing and other personal effects. The NIS agents then transported appellant to Jacksonville, where they turned him over to the civilian authorities. . . . [T]he NIS agent stated candidly that his primary purpose in traveling to Virginia was to question appellant about the homicides. We conclude the nature of the military involvement in the investigation may have constituted a violation of the federal Act. . .").

The Posse Comitatus Act proscribes use of the Army or the Air Force to execute the law.[2095] It says nothing about the Navy, the Marine Corps, the Coast Guard, or the National Guard. The amendment first offered to the Army appropriation bill in 1878 to enact the Posse Comitatus provisions would have prohibited use of "any part of the land or naval forces of the United States" to execute the law, 7 Cong.Rec. 3586 (1878). Some commentators believe that sponsors subsequently limited the posse comitatus amendment to the Army appropriation bill in order to avoid challenges on grounds of germaneness.[2096] The courts have generally held that the Posse Comitatus Act by itself does not apply to the Navy or the Marine Corps.[2097] They maintain, however, that those forces are covered by similarly confining administrative and legislative supplements,[2098] the most currently applicable of which appear in the DoD Directive.[2099]

[2095] Whoever, except in cases and under circumstances expressly authorized by the Constitution or Act of Congress, willfully uses any part of the Army or the Air Force as a posse comitatus or otherwise to execute the laws shall be fined under this title or imprisoned not more than two years, or both. 18 U.S.C. 1385 (emphasis added).

[2096] The Navy's Role in Interdicting Narcotics Traffic: War on Drugs or Ambush of the Constitution? 75 GEORGETOWN LAW JOURNAL 1947, 1955 (1987); Meeks, Illegal Law Enforcement: Aiding Civil Authorities in Violation of the Posse Comitatus Act, 70 MILITARY LAW REVIEW 83, 101 (Fall, 1975). Under long standing rules of the House, an amendment that deals with a subject different from those contained in the bill which it seeks to amend is nongermane and subject to challenge. If the posse comitatus amendment sponsors adjusted their amendment solely for reasons of germaneness, one would expect to find a comparable amendment in the Navy appropriation bill before the Congress at the same time. So such amendment was offered to the Navy bill, 46 Stat. 48 (1878).

[2097] United States v. Mendoza-Cecelia, 963 F.2d 1467, 1477 (11th Cir. 1992); United States v. Yunis, 924 F.2d 1086, 1093 (D.C.Cir. 1991); State v. Short, 113 Wash.2d 35, 38, 775 P.2d 458, 459 (1989); United States v. Ahumedo-Avendano, 872 F.2d 367, 372 n.6 (11th Cir. 1989); Schowengerdt v. General Dynamics Corp., 823 F.2d 1328, 1339-340 (9th Cir. 1987); United States v. Roberts, 779 F.2d 565, 567 (9th Cir. 1986); United States v. Walden, 490 F.2d 372, 374 (4th Cir. 1974).

[2098] United States v. Kahn, 35 F.3d 426, 431 (9th Cir. 1994)("[t]hus the Posse Comitatus Act applies to the Navy through section 375 [of title 10 of the United States Code] and 32 C.F.R. §213.10"); Taylor v. State, 640 So.2d 1127, 1136 (Fla.App. 1994)("[m]ilitary participation in civilian law enforcement activities is restricted by the federal Posse Comitatus Act, 18 U.S.C. §1385, and by 10 U.S.C. §375"); United States v. Yunis, 924 F.2d 1086, 1094 (D.C.Cir. 1991)) ("[r]egulations issued under 10 U.S.C. §375 require Navy compliance with the restrictions of the Posse Comitatus Act. . ."); Hayes v. Hawes, 921 F.2d 100, 102-103 (7th Cir. 1990)(". . .10 U.S.C. §375 and the regulations promulgated thereunder at 32 C.F.R. §§213.1-213.11 make the proscriptions of [18 U.S.C.] §1385 applicable to the Navy and serve to limit its involvement with civilian law enforcement officials"); State v. Short, 113 Wash.2d 35, 39, 775 P.2d 458, 460 (1989)("[b]ecause the limitations on the use of the armed services contained in 10 U.S.C. §375 correspond closely with those in the posse comitatus act, the same analysis should apply"); United States v. Ahumedo-Avendano, 872 F.2d 367, 372 n.6 (11th Cir. 1989)("[t]he Posse Comitatus Act does not expressly regulate the use of naval forces as a posse comitatus; the courts of appeal that have considered this question, however, have concluded that the prohibition embodied in the Act applies to naval forces, either by implication or by virtue of executive act"); United States v.

Coast Guard

The Posse Comitatus Act likewise says nothing about the Coast Guard. The Coast Guard was formed by merging two civilian agencies, the revenue cutter service and the lifesaving service. Although created and used for law enforcement purposes, the cutter service had already been used as part of the military forces of the United States by the time the Posse Comitatus Act was enacted.[2100]

Roberts, 779 F.2d 565, 568 (9th Cir. 1986)(" . . .the Posse Comitatus Act and sections 371-378 of Title 10 embody similar proscriptions against military involvement in civil law enforcement. . . "); United States v. Del Prado-Montero, 740 F.2d 113, 116 (1st Cir. 1984)("18 U.S.C. 1385 prohibits the use of the Army and the Air Force to enforce the laws of the United States, a proscription that has been extended by executive act to the Navy"); United States v. Chaparro-Almeida, 679 F.2d 423, 425 (5th Cir. 1982)(dicta in case involving the Coast Guard); United States v. Walden, 490 F.2d 372, 373-74 (4th Cir. 1974)("[t]he use of Marines as undercover investigators by the Treasury Department is counter to a Navy military regulation proscribing the use of military personnel to enforce civilian laws. . . . Thus, though by its terms the Posse Comitatus Act does not make criminal the use of Marines to enforce federal laws, the Navy has adopted the restriction by self-imposed administrative regulation").

As an examination of the cases listed above and in the previous footnote demonstrate, although in basic agreement subsequent courts have sometime described their views as in conflict. In fact, one camp will cite Walden for the proposition that the Posse Comitatus Act does not apply to the Navy or Marines although its requirements have been adopted by administrative and/or legislative supplements, while the other camp will cite Walden for the assertedly contrary proposition that the Posse Comitatus Act requirements apply to the Navy and Marines by way of regulation and/or legislative supplement. A third group takes an abbreviate route to the same destination by simply citing Walden for the principle that the Posse Comitatus Act applies to Navy and the Marines, see e.g., People v. Caviano, 148 Misc.2d 426, 560 N.Y.S.2d 932, 936 n.1 (1990); State v. Presgraves, 328 S.E.2d 699, 701 n.3 (W.,Va. 1985); State v. Maxwell, 328 S.E.2d 506, 509 n.4 (W.Va. 1985); People v. Wells, 175 Cal.App.3d 876, 879, 221 Cal.Rprt. 273, 275 (1985); People v. Blend, 121 Cal.App.3d 215, 222, 175 Cal.Rprt. 263, 267 (1981).

[2099] "A. REISSUANCE AND PURPOSE

This Directive reissues reference (a) [DoD Directive No. 5525.5 (March 22, 1982)] to update uniform DoD policies and procedures to be followed with respect to support provided to Federal, State, and local civilian law enforcement efforts. . . .

"APPLICABILITY AND SCOPE

1. This Directive applies to the Office of the Secretary of Defense (OSD), the Military Departments, the Organization of the Joint Chiefs of Staff (OJS), the Unified and Specified Commands, and the Defense Agencies (hereafter referred to collectively as DoD Components). The term `Military Service,' as used herein, refers to the Army, Navy, Air Force, and Marine Corps."

[2100] See 46 Stat. 316 (1878), directing the Secretary of the Treasury to issue three months extra pay to those who had engaged in the military service of the United States during the war with Mexico and listing the cutter service as one source of possibly qualifying service.

The Coast Guard is now a branch of the armed forces, located within the Department of Transportation, 14 U.S.C. 1, but relocated within the Navy in time of war or upon the order of the President, 14 U.S.C. 3. The Act does apply to the Coast Guard while it remains part of the Department of Transportation.[2101] While part of the Navy, it is subject to the orders of the Secretary of the Navy, 14 U.S.C. 3, and consequently to any generally applicable directives or instructions issued under the Department of Defense or the Navy.

As a practical matter, however, the Coast Guard is statutorily authorized to perform law enforcement functions, 14 U.S.C. 2. Even while part of the Navy its law enforcement activities would come within the statutory exception to the posse comitatus restrictions, and the restrictions applicable to components of the Department of Defense would only apply to activities beyond those authorized.

National Guard

The Act is silent as to what constitutes "part" of the Army or Air Force for purposes of proscription. There is little commentary or case law to resolve questions concerning the coverage of the National Guard, the Civil Air Patrol, civilian employees of the armed forces, or regular members of the armed forces while off duty.

Strictly speaking, the Posse Comitatus Act predates the National Guard only in name for the Guard "is the modern Militia reserved to the States by Art.I, §8, cls.15, 16, of the Constitution" which has become "an organized force, capable of being assimilated with ease into the regular military establishment of the United States," Maryland v. United States, 381 U.S. 41, 46 (1965). There seems every reason to consider the National Guard part of the Army or Air Force, for purposes of the Posse Comitatus Act, when in federal service.[2102] When not in federal service, historical reflection might suggest that it is likewise covered. Recall that it was the state militia, called to the aid of the marshal enforcing the Fugitive Slave Act, which triggered Attorney General Cushing's famous opinion. And that the Posse Comitatus Act's reference to "posse comitatus or otherwise" is a "they-are-covered-no-matterwhat-you-call-them" response to the assertion derived from Cushing's opinion that troops could be used to execute the law as long as they were acting as citizens and not soldiers when they did so.

On the other hand, the National Guard is creature of both state and federal law, a condition which as the militia it has enjoyed since the days of the Articles of

---

[2101] United States v. Chaparro-Almedia, 679 F.2d 423, 425 (5th Cir. 1982); Jackson v. State, 572 P.2d 87, 93 (Alaska, 1977).

[2102] Meeks, Illegal Law Enforcement: Aiding Civil Authorities in Violation of the Posse Comitatus Act, 70 MILITARY LAW REVIEW 83, 96-9 (Fall, 1975); Furman, Restrictions Upon Use of the Army Imposed by the Posse Comitatus Act, 7 MILITARY LAW REVIEW 85, 101 (January, 1960).

Confederation.[2103] And the courts have said that members of the National Guard when not in federal service are not covered by the Posse Comitatus Act.[2104] Similarly, the DoD directive is only applicable to members of the National Guard when they are in federal service.[2105]

[2103] The status of the District of Columbia National Guard is somewhat different since it is a creature entirely of federal creation. This being the case it might be thought that the D.C. National Guard should be considered perpetually "in federal service" or that the Posse Comitatus Act would apply to it at all times even though the treatment of the National Guard in the various states might be different. This, however, is not the view of the Department of Justice which has concluded the Posse Comitatus Act applies to the D.C. National Guard only when it is called into federal service as a state National Guard might be. The Department has also determined that even if this were not the case the Posse Comitatus Act permits the D.C. National Guard to "to support the drug law enforcement efforts" of the D.C. police because of the authority granted by Congress in D.C. Code 39-104 (declaring that the D.C. National Guard shall not be subject to any duty except when called into federal service or to "aid civil authorities in the execution of the laws or suppression of riots"[D.C.Code §39-603 authorizes D.C. officials, in times of tumult, riot, or mob violence, to request the President to call out the D.C. National Guard to aid "in suppressing such violence and enforcing the laws"]) and D.C.Code §39-602 (authorizing the Commanding General of the D.C.National Guard to order "such drills, inspections, parades, escort, or other duties, as he may deem proper")(emphasis added), Use of the National Guard to Support Drug Interdiction Efforts in the District of Columbia, 13 OP.OFF. LEGAL COUNSEL 110 (1989).

[2104] Gilbert v. United States, 165 F.3d 470, 473 (6th Cir. 1999); United States v. Hutchings, 127 F.3d 1255, 1258 (10th Cir. 1997); United States v. Benish, 5 F.3d 20, 25-6 (3d Cir. 1993); United States v. Kyllo, 809 F.Supp. 787, 792-93 (D.Ore. 1992); Wallace v. State, 933 P.2d 1157, 1160 (Alaska App. 1997); accord, Rich, The National Guard, Drug Interdiction and Counterdrug Activities, and the Posse Comitatus Act: The Meaning and Implications of `In Federal Service', 1994 ARMY LAWYER 35, 42-3 (June, 1994); but in two Wounded Knee cases, in which National Guard involvement in the civilian law enforcement efforts helped doom federal prosecution, the courts made no effort to determine whether the Guard had been called into federal service, suggesting to some that the Guard was covered in any event. United States v. Banks, 383 F.Supp. 368, 376 (D.S.D. 1974); United States v. Jaramillo, 380 F.Supp. 1375, 1380-381 (D.Neb. 1974); see also, United States v. McArthur, 419 F.Supp. 186, 193 n.3 (D.N.D. 1976)(a third Wounded Knee case listing "use by federal civil law enforcement officers of material and equipment furnished by . . . the South Dakota National Guard. . . aerial photographic reconnaissance provided by . . . the Nebraska National Guard . . . and the maintenance of military vehicles performed by members of the Nebraska National Guard" as "evidence of military involvement"); Meeks, Illegal Law Enforcement: Aiding Civil Authorities in Violation of the Posse Comitatus Act, 70 MILITARY LAW REVIEW 83, 96-8 (Fall, 1975).

Kyllo suggests that 32 U.S.C. §112 (which permits the Secretary of Defense to provide funds for the drug interdiction activities conducted by various state National Guards when not in federal service) authorizes such Guards to assist in civilian law enforcement efforts, 809 F.Supp. at 793.

The legislative history of earlier efforts to involve the National Guard (while in state service) in drug interdiction indicates that the Congress believed that "[w]hen not in federal service, the National Guard is not subject to the Posse Comitatus Act," H.R.Rep.No.100989, 455, reprinted in 1988 UNITED STATES CODE CONGRESSIONAL AND ADMINISTRATIVE NEWS 2503, 2583.

[2105] "The restrictions of section A. above [the Directive's posse comitatus proscriptions], do not apply to the following persons . . . . 2. A member of the National Guard when not in Federal Service," DoD Directive No. 5525.5.b.2.

Off Duty, Acting as Citizens & Civilian Employees

The historical perspective fares little better on the question of whether the Posse Comitatus Act extends to soldiers who assist civilian law enforcement officials in a manner which any other citizen would be permitted to provide assistance, particularly if they do so while off duty.

Congress passed the Act in response to cases where members of the military had been used based on their civic obligations to respond to the call as the posse comitatus. The debate in the Senate, however, suggests that the Act was not intended to strip members of the military of all civilian rights and obligations.[2106]

Some of the cases, particularly the earlier ones, occasionally citing debate in the Senate, held that a soldier who does no more than any other citizen might do to assist civilian law enforcement has not been used in violation of the Posse Comitatus Act.[2107] The more recent decisions under similar facts, with the

---

[2106] "If a soldier sees a man assaulting me with a view to take my life, he is not going to stand by and see him do it, he comes to my relief not as a soldier, but as a human being, a man with a soul in his body, and as a citizen. . . . The soldier standing by would have interposed if he had been a man, but not as a soldier. He could not have gone down in pursuance of an order form a colonel or a captain, but he would have done it as a man." 7 Cong.Rec. 4245 (1878)(remarks of Sen. Merriman).

The weight afforded remarks in the Senate should perhaps reflect the fact that the Act was the work of a Democratic House, forced upon a reluctant Republican Senate.

[2107] People v. Taliferro, 116 Ill.App.3d 861, 520 N.E.2d 1047, 1051 (1988)(an airman acted as an undercover agent for local drug enforcement officers; "Ferguson participated in a controlled drug purchase in exactly the same manner as any other citizen would participate in such transaction"); Burkhart v. State, 727 P.2d 971, 972 (Okla.Crim.App. 1986)(military undercover agent investigating drugs sold to military personnel purchased some from the defendant and testified against him; "the agent `did not assume any greater authority than that of a private citizen in purchasing the marijuana'"); People v. Burden, 411 Mich. 56, 303 N.W.2d 444, 446-47 (1981)(airman agreed to serve undercover after being charged with drug sales by civilian authorities; "[i]n cooperating with and assisting the civilian police agency, Hall was not acting as a member of the military. He was acting only as a civilian. His military status was merely incidental to and not essential to his involvement with the civilian authorities. He was not in military uniform. He was not acting under military orders. He did not exercise either explicitly or implicitly any military authority. Moreover, Hall was not a regular law enforcement agent of the military, * * * nor does the record suggest that Hall's usefulness to civilian authorities was in any way enhanced by virtue of his being a military man. . . . [T]he assistance rendered by Hall was in no way different from the cooperation which would have been given by a private citizen offered the same opportunity to avoid criminal prosecution"); People v. Blend, 121 Cal.App.3d 215, 227, 175 Cal.Rptr. 263, 270 (1981)(a Navy wave caught by civilian authorities in violating the drug laws, agreed to serve undercover for the civilian police; "the [posse comitatus] act does not apply to military personnel who are acting clearly on their own initiative as private citizens"); Lee v. State, 513 P.2d 125, 126 (Okla.Crim.App. 1973)(military undercover agent in cooperation with local police purchases drugs off-base from a civilian; "agent Smith did not assume any greater

endorsement of the commentators,[2108] have focused on the nature of the assistance provided and whether the assistance is incidental to action taken primarily for a military purpose.[2109]

---

authority than that of a private citizen in purchasing the marijuana in the instant case"); Hildebrandt v. State, 507 P.2d 1323, 1325 (Okla.Crim.App. 1973)(military undercover investigators traced the source of drugs sold to military personnel to the defendant; the "soldier led the agents to a location outside the scope of their military jurisdiction, at which time the gents assumed no greater authority than that of a private citizen"); Hubert v. State, 504 P.2d 1245, 1246-247 (Okla.Crim.App. 1972)(same).

[2108] Meeks, Illegal Law Enforcement: Aiding Civil Authorities in Violation of the Posse Comitatus Act, 70 MILITARY LAW REVIEW 83, 126-27 (Fall, 1975) ("Military personnel are all private citizens as well as members of the federal military. The prohibitions of the Posse Comitatus Act do not apply to military personnel who are performing the normal duties of a citizen such as reporting crimes and suspicious activities, making citizens' arrests where allowed by local law and otherwise cooperating with civil police. It is not sufficient for military personnel to be `volunteers,' they must clearly be acting on their own initiative and in a purely unofficial and individual capacity. Commanders must be careful to insure that activities which are in violation of the act are not being carried on under the labels of `individual' or `unofficial' assistance. Some factors which may signal a violation of the Act include aid given during duty hours, aid prompted or suggested by a military superior or aid given with the knowledge or acquiescence of a military superior. Other considerations include the manner in which the civil authorities contacted the military person, whether that person regularly performs military law enforcement functions, and whether or not the individual's usefulness to civil authorities is related to his military status"); Rice, New Laws and Insights Encircle the Posse Comitatus Act, 194 MILITARY LAW REVIEW 109, 128-33 (Spring, 1984)(also noting that the catalyst for some the difficult stemmed from the holding in O'Callahan v. Parker, 395 U.S. 258 (1969)(since overturned) limiting military jurisdiction over crimes committed by military personnel to those which were service connected).

[2109] Fox v. State, 908 P.2d 1053, 1057 (Alaska App. 1995)("In civilian prosecutions stemming from joint military-civilian investigations into off-base drug sales, courts have interpreted these regulations to require the government to demonstrate a military purpose – that is a nexus between the targeted off-base sales and military personnel; this purpose must be shown to have been the primary purpose of the m ilitary's participation. In the absence of a nexus between the targeted off-base drug sales and military personnel, courts have condemned joint investigations as violations of the Posse Comitatus Act "); State v. Gunter, 902 S.W.2d 172, 175 (Tex.App. 1995)(after quoting the private citizen language in Burkhardt, supra, the court declared, "[a] majority of courts have also noted that where military involvement is limited and where there is an independent military purpose of preventing illicit drug transactions to support the military involvement, the coordination of military police efforts with those of civilian law enforcement does not violate the Act. Where the military participation in an investigation odes not pervade the activities of civilian officials, and does not subject the citizenry to the regulatory exercise of military power, it doe snot violate the Act"); State v. Pattioay, 78 Haw. 455, 466, 896 P.2d 911, 922 (1995)("Absent evidence to support the prosecution's claim of a primary military purpose, we must uphold the circuit court's conclusion that the joint civilian-military [undercover drug] investigation violated the PCA, 10 U.S.C. §375, and relevant federal regulations"); Taylor v. State, 640 So.2d 1127, 1136 (Fla.App. 1994) ("[m]ilitary participation in civilian law enforcement activities is restricted by the federal Posse Comitatus Act and by 10 U.S.C. §375. Cases addressing this issue have ruled that where military involvement is limited and there is an independent military purpose, `the coordination of military police efforts with those of civilian law enforcement officials does not violate either section 1385 or section 375.' Hayes v. Hawes, 921 F.2d 100, 103 (7th Cir. 1990). The test for violation of the federal law is (1) whether civilian law enforcement officials made a direct active use of military investigators to execute the laws; (2)

Some have questioned whether civilian employees of the armed forces should come within the proscription of the Act,[2110] but most, frequently without comment, seem to consider them "part" of the armed forces for purposes of the Posse Comitatus Act.[2111] The current Defense Department Directive expressly includes civilian employees "under the direct command and control of a military officer" within its Posse Comitatus Act policy restrictions.[2112]

Geographical Application

It seems unlikely that the Posse Comitatus Act, by itself, applies beyond the confines of the United States, its territories and possessions.[2113] As a general rule, Acts of Congress are presumed to apply only within the United States, its territories and possessions unless Congress has provided otherwise or unless the purpose of Congress in enacting the legislation evidences an intent that the legislation enjoy extraterritorial application.[2114]

The Posse Comitatus Act contains no expression of extraterritorial application. Congress enacted it in response to problems occurring within the United States and its territories, problems associated with the American political process and military usurpation of civilian law enforcement responsibilities over Americans.

---

whether the use of the military pervaded the activities of the civilian officials; or (3) whether the military was used so as to subject citizens to the exercise of military power which was regulatory, proscriptive, or compulsory in nature").

[2110] State v. Short, 113 Wash.2d 35, 39-40, 775 P.2d 458, 460 (1989); State v. Morris, 522 A.2d 220, 221 (R.I. 1987); People v. Hayes, 144 Ill.App. 3d 696, 494 N.E.2d 1238, 1240 (1986); see also, Furman, Restrictions Upon Use of the Army Imposed by the Posse Comitatus Act, 7 MILITARY LAW REVIEW 85, 101 (1960).

[2111] See e.g., Hayes v. Hawes, 921 F.2d 100 (7th Cir. 1990); People v. Wells, 175 Cal.App.3d 878, 221 Cal.Rprt. 273 (1988); State v. Maxwell, 328 S.E.2d 506 (W.Va. 1985); State v. Presgraves, 328 S.E.2d 699 (W.Va. 1985); United States v. Hartley, 486 F.Supp. 1348 (M.D.Fla. 1980), aff'd, 678 F.2d 961 (11th Cir. 1982); Meeks, Illegal Law Enforcement: Aiding Civil Authorities in Violation of the Posse Comitatus Act, 70 MILITARY LAW REVIEW 83 (Fall, 1975)("civilian investigators operate under the immediate supervision of military officers who are prohibited by the Act from aiding local authorities. Holding that the civilian subordinates are not also prohibited allows a principal to accomplish things through his agent that he could not otherwise lawfully do himself. It is foolhardy to assume that it is only the sight of the man in military uniform aiding the sheriff that tends to offend the civilian community").

[2112] DoD Dir. No. 5525.5 (Encl.4) §B.3, a comparable provision appeared in 32 CFR §213.10(b)(3)(July 1, 1992 ed.).

[2113] Extraterritorial Effect of the Posse Comitatus Act, 13 OP. OFF. LEGAL COUNSEL 387 (1989); Siemer & Effron, Military Participation in United States Law Enforcement Activities Overseas: The Extraterritorial Effect of the Posse Comitatus Act, 54 ST.JOHN'S LAW REVIEW 1 (1979).

[2114] United States v. Bowman, 260 U.S. 94, 98 (1922); Blackmer v. United States, 284 U.S. 421 (1932); United States v. Yunis, 924 F.2d 1086, 1090-91 (D.C.Cir. 1991).

It seems unlikely that its extraterritorial application was either anticipated or intended.

The first court to consider the question agreed, but it arose in occupied territory overseas in which an American military government had temporarily displaced civil authorities, *Chandler v. United States*, 171 F.2d 921, 936 (1st Cir. 1948). For some time subsequent decisions either declined to resolve the issue or ignored it.[2115]

Congress does appear to have intended the authority and restrictions contained in 10 U.S.C. 371-381 to apply both in the United States and beyond its borders. Certainly, the provisions directing the placement of members of the Coast Guard on Navy ships for drug interdiction purposes, 10 U.S.C. 379, evidence an understanding that the Posse Comitatus Act's statutory shadow, 10 U.S.C. 375, applies at least on the high seas.[2116] In fact, in some instances it initially contemplated that various provisions would only apply overseas.[2117]

The regulations implementing 10 U.S.C. 375 address only assistance to law enforcement officials of the several states, the United States, or its territories or possessions, DoD Dir. No. 5525.5, §3, without any explicit declaration that the ban applies only within this country. In the case of assistance provided overseas to foreign law enforcement officials, the so-called Mansfield Amendment, 22 U.S.C. 2291(c), creates something of an overseas version of the Posse Comitatus Act, at least for drug enforcement purposes.[2118]

[2115] Gillars v. United States, 182 F.2d 962, 973 (D.C.Cir. 1950); D'Aquino v. United States, 192 F.2d 338, 351 (9th Cir. 1951); United States v. Cotton, 471 F.2d 744, 748-49 (9th Cir. 1973).

[2116] Cf., United States v. Klimavicius-Viloria, 144 F.3d 1249, 1259 (9th Cir. 1998); United Sstates v. Khan, 35 F.3d 426, 431-32 (9th Cir. 1994)(both determining that the particular activities of Navy personnel on the high seas in aid of law enforcement officials did not violate 10 U.S.C. 375).

[2117] "The Committee considered and narrowly rejected a suggestion that the assistance permitted by this section be made available only outside the United States," H.R.Rep.No. 97-71, pt.2, 12 n.3, reprinted in 1981 UNITED STATES CODE, CONGRESSIONAL AND ADMINISTRATIVE NEWS 1785, 1795.

[2118] "(c) Participation in foreign police actions

"(1) Prohibition on effecting an arrest

"No officer or employee of the United States may directly effect an arrest in any foreign country as part of any foreign police action with respect to narcotics control efforts, notwithstanding any other provisions of law.

"(2) Participation in arrest actions

Consequences of Violation

Prosecution

The Posse Comitatus Act is a criminal statute under which there has apparently never been a prosecution.[2119] It has been invoked with varying degrees of success,

---

"Paragraph (1) does not prohibit an officer or employee of the United States, with the approval of the United States chief of mission, from being present when foreign officers are effecting an arrest or from assisting foreign officers who are effecting an arrest.

"(3) Exception for exigent, threatening circumstances

"Paragraph (1) does not prohibit an officer or employee from taking direct action to protect life or safety if exigent circumstances arise which are unanticipated and which pose an immediate threat to United States officers or employees, officers or employees of a foreign government, or members of the public.

"(4) Exception for maritime law enforcement

"With the agreement of a foreign country, paragraph (1) does not apply with respect to maritime law enforcement operations in the territorial sea or archipelagic waters of that country.

"(5) Interrogations

"No officer or employee of the United States may interrogate or be present during the interrogation of any United States person arrested in any foreign country with respect to narcotics control efforts without the written consent of such person.

"(6) Exception for status of forces arrangements

"This subsection does not apply to the activities of the United States Armed Forces in carrying out their responsibilities under applicable Status of Forces arrangements." 22 U.S.C. 2291(c).

In the course of its opinion concerning the extraterritorial application of the Posse Comitatus Act, the Office of Legal Counsel characterized an earlier version of the Mansfield Amendment as applicable only in the case of American involvement "in the internal enforcement activities of foreign countries" and not applicable to the overseas enforcement of American law, Extraterritorial Effect of the Posse Comitatus Act, 13 OP. OFF. LEGAL COUNSEL 387, 410-11 n.16 (1989)(citing dicta in United States v. Green, 671 F.2d 46, 53 n.9 (1st Cir. 1982), for the proposition that the Mansfield Amendment "was only intended to `insure that U.S. personnel do not become involved in sensitive, internal law enforcement operations which could adversely affect U.S. relations with that country'" and inferring that U.S. enforcement of its laws within the territory of another nation for misconduct within that nation would not similarly adversely affect relations and was intended to be covered). However tenable that position may once have been, it seems to have been undermined by the inclusion of subparagraph (4) making the Amendment inapplicable in cases where the foreign country has agreed to the application of American drug laws within its territorial waters.

[2119] Gilligan, Opening the Gate? An Analysis of Military Law Enforcement Authority Over Civilian Lawbreakers On and Off the Federal Installation, 161 MILITARY LAW REVIEW 1, 11 (1999); State

---

however, to challenge the jurisdiction of the courts, as a defense in criminal prosecutions for other offenses, as a ground for the suppression of evidence, as the grounds for, or a defense against, civil liability, and as an impediment to proposed actions by the armed forces.

Exclusion of Evidence

Allegations that the Posse Comitatus Act has been violated are made most often by defendants seeking to exclude related testimony or physical evidence. The case law begins with *United States v. Walden*, 490 F.2d 372 (4th Cir. 1974), where the court found that the Treasury Department's use of three Marines as undercover agents in an investigation of firearms offenses violated Navy regulations which made the Act applicable to use of the Marines, but declined to order the exclusion of evidence obtained by the Marines.

The court found no "conscious, deliberate or willful intent on the part of the Marines or the Treasury Department's Special Investigator to violate" the regulation or the Act, 490 F.2d at 376. It also noted that the regulation contained no enforcement mechanism and the Posse Comitatus Act provided only for criminal prosecution, and that case before lacked the elements which had lead to the adoption of the Fourth Amendment exclusionary rule. Finally, the court felt the use of the Marines had been aberrational, that subsequent similar transgressions were unlikely, and that the regulation would be amended to provide an enforcement component. But the court warned, "should there be evidence of widespread or repeated violations in any future case, or ineffectiveness of enforcement by the military, we will consider ourselves free to consider whether adoption of an exclusionary rile is required as a future deterrent," 490 F.2d at 377.

Later defendants have focused upon the warning; later courts upon the refusal to adopt an exclusionary rule. Most cases note the absence of an exclusionary rule either to avoid unnecessary posse comitatus act analysis or as the final step in the analysis.[2120] Three states cases, two of them recent, have required the suppression

---

v. Pattioay, 78 Haw. 455, 467, 896 P.2d 911, 923 (1995); Moon v. State, 785 P.2d 45, 48 (Alaska App. 1990).

[2120] E.g., United States v. Wolffs, 594 F.2d 77, 85 (5th Cir. 1979)("We pretermit discussion of whether there was a violation of the statute or regulation. We need not decide that complex and difficult issue because assuming without deciding that there was a violation application of an exclusionary rule is not warranted"); People v. Hayes, 144 Ill.App.3d 696, 494 N.E.2d 1238, 1240 (1986)("numerous decisions with facts similar to those presented here have found that no violation of the Act occurs if the aid is not characterized as military and the investigation merely coordinates with civilian police. More importantly, with few exceptions, the courts have uniformly held that the exclusionary rule does not apply to evidence seized in violation the Posse Comitatus Act"); other cases include, United States v. Mullin, 178 F.3d 334, 342-43 (5th Cir. 1999); United States v. Al-Talib, 55 F.3d 923 (4th Cir. 1995); State v. Gunter, 902 S.W.2d 172 (Tex.App. 1995); Taylor v. State, 640 So.2d 1127 (Fla.App. 1994)(finding a violation but declining to exclude

of evidence resulting from the use of military undercover agents to target civilian drug dealing without establishing any connection to activities on a military installation or sales to military personnel other than the undercover agents.[2121]

Jurisdiction & Criminal Defenses

The first criminal defendants to seek refuge in the Posse Comitatus Act claimed unsuccessfully that use of the military to transport them back to the United States for trial violated the Posse Comitatus Act and vitiated the jurisdiction of American courts to try them. Ordinarily, criminal trials are not barred simply because the defendant was unlawfully seized and carried into the jurisdiction of the trial court.[2122] There are indications that the same rule applies when the defendant challenges the court's jurisdiction on the grounds of Posse Comitatus Act violations. In the early posse comitatus cases, the defendants' arguments were further undermined by the fact that the countries from which they were returned, Germany and Japan, were under American military rule at the time.[2123] In later cases some of which began beyond the territorial confines of the United States although none in occupied territory, the courts noted that dismissal would not be an appropriate remedy for a posse comitatus violation.[2124]

---

evidence); State v. Valdobinos, 122 Wash.2d 270, 858 P.2d 199 (1993); United States v. Mendoza-Cecelia, 963 F.2d 1467 (11th Cir. 1992); McPherson v. State 800 P.2d 928 (Alaska App. 1990); People v. Caviano, 148 Misc.2d 426, 560 N.Y.S.2d 932 (N.Y.S.Ct. 1990); Moon v. State, 785 P.2d 45 (Alaska App. 1990); Badoino v. State, 785 P.2d 39 (Alaska App. 1990); Hayes v. Hawes, 921 F.2d 100 (7th Cir. 1990); State v. Short, 113 Wash.2d 35, 775 P.2d 458 (1989); State v. Poe, 755 S.W.2d 41 (Tenn. 1988); United States v. Bacon, 851 F.2d 1312 (11th Cir. 1988); United States v. Griley, 814 F.2d 967 (4th Cir. 1987); State v. Morris, 522 A.2d 220 (R.I. 1987); United States v. Hartley, 796 F.2d 112 (5th Cir. 1986); United States v. Roberts, 779 F.2d 565 (9th Cir. 1986) (found violation but declined to find application of the exclusionary rule appropriate); Burkhart v. State, 727 P.2d 971 (Okla.Crim.App. 1986); People v. Wells, 175 Cal.App.3d 876, 221 Cal.Rptr. 273 (1985); State v. Maxwell, 328 S.E.2d 506 (W.Va. 1985); Unites States v. Chaparro-Almeida, 679 F.2d 423 (5th Cir. 1982); People v. Burden, 411 Mich.56, 303 N.W.2d 444 (1981); State v. Sanders, 303 N.C. 608, 281 S.E.2d 7 (N.C. 1981); State v. Trueblood, 46 N.C.App. 541, 265 S.E.2d 662 (N.C.App. 1980); State v. Nelson, 298 N.C. 573, 260 S.E.2d 629 (1979); State v. Danko, 219 Kan. 490, 548 P.2d 819 (9176); Hubert v. State, 504 P.2d 1245 (Okla.Crim.App. 1972).

[2121] State v. Pattioay, 78 Haw. 455, 896 P.2d 911 (1995); People v. Tyler, 854 P.2d 1366 (Colo.App. 1993), rev'd on other grounds, 874 P.2d 1037 (Colo. 1994); Taylor v. State, 645 P.2d 522 (Okla.Crim.App. 1982).

[2122] Ker v. Illinois 119 U.S. 436 (1886); Frisbie v. Collins,342 U.S. 519 (1952); United States v. Alvarez-Machain, 504 U.S. 655 (1992).

[2123] Chandler v. United States 171 F.2d 921 (1st Cir. 1949); Gillars v. United States, 182 F.2d 962 (D.C.Cir. 1950); D'Aquino v. United States, 192 F.2d 338 (9th Cir. 1951).

[2124] United States v. Mendoza-Cecelia, 963 F.2d 1467, 1478 n.9 (11th Cir. 1992); United States v. Yunis, 924 F.2d 1086, 1093-94 (D.C.Cir. 1991); State v. Morris, 522 A.2d 220, 221 (R.I. 1987); United States v. Roberts, 779 F.2d 565, 568 (9th Cir. 1986); United States v. Cotton, 471 F.2d 744, 749 (9th Cir. 1973).

Defendants have found the Act more helpful in prosecutions where the government must establish the lawfulness of its conduct as one of the elements of the offense charged. Thus, several defendants at Wounded Knee were able to persuade the court that evidence of possible Posse Comitatus Act violations precluded their convictions for obstructing law enforcement officials "lawfully engaged" in the performance of their duties.[2125]

Civil Liability

Almost a decade ago, the Eighth Circuit found that a violation of the Act might constitute an unreasonable search and seizure for purposes of the Fourth Amendment thereby giving rise to a Bivens cause of action against offending federal officers or employees.[2126] A Posse Comitatus Act violation, however, also provides the government with a defense to a claim under the Federal Tort Claims Act since the government is not liable under that Act for injuries inflicted by federal officers or employees acting outside the scope of their authority.[2127] On balance, however, the Posse Comitatus Act is only rarely placed in issue in civil cases.

Compliance

The most significant impact of the Posse Comitatus Act is attributable to compliance by the armed forces. As administrative adoption of the Act for the Navy and Marines demonstrates, the military has a long standing practice of avoiding involvement in civilian affairs which it believes are contrary to the Act.[2128]

[2125] United States v. Banks, 383 F.Supp. 368, 374-77 (D.S.D. 1974); United States v. Jaramillo, 380 F.Supp. 1375, 1378-381 (D.Neb. 1974).

[2126] Bissonette v. Haig, 800 F.2d 812 (8th Cir. 1986), aff'd as if by an equally divided court for want of a quorum , 485 U.S. 264 (1988); see also, Applewhite v. United States, 995 F.2d 997 (10th Cir. 1993). Bivens v. Six Unknown Named Agents of the Federal Bureau of Narcotics, 403 U.S. 388 (1971), recognized a private cause of action in tort for injuries suffered as a result of a constitutional violation.

[2127] Wrynn v. United States, 200 F.Supp. 457 (E.D.N.Y. 1961); Rice, New Laws and Insights Encircle the Posse Comitatus Act, 104 MILITARY LAW REVIEW 109, 115 (Spring, 1984).

[2128] Furman, Restrictions Upon Use of the Army Imposed by the Posse Comitatus Act, 7 MILITARY LAW REVIEW 85, 85-86 (January, 1960); Meeks, Illegal law Enforcement: Aiding Civil Authorities in Violation of the Posse Comitatus Act, 70 MILITARY LAW REVIEW 83 (Fall, 1975)(both citing extensively to internal instructions, directives and opinions advising members of the military to refrain from conduct understood to be contrary to the Posse Comitatus Act); Peterson, Civilian Demonstrations Near the Military Installation: Restraints on Military Surveillance and Other Activities, 140 MILITARY LAW REVIEW 113, 145 n.165 (Spring, 1993)("when the Army believes the Posse Comitatus Act actually applies, the Army interprets the prohibitions of the Act broadly"); cf.,Rice, New Laws and Insights Encircle the Posse Comitatus Act, 104 MILITARY LAW REVIEW 109, 118 & 118 n.55 (Spring, 1984)("Unexpected decisions

Selected Bibliography

Books & Articles

Bell, The Third Amendment, Forgotten But Not Gone, 2 WILLIAM & MARY BILL OF RIGHTS JOURNAL 117 (1993)

Blackstone, I COMMENTARIES ON THE LAWS OF ENGLAND (1765 ed.)

Bowen, MIRACLE AT PHILADELPHIA: THE STORY OF THE CONSTITUTIONAL CONVENTION MAY TO SEPTEMBER 1787 (1966)

Boyd, THE WHISKEY REBELLION: PAST AND PRESENT PERSPECTIVES (1985)

Coke, I THE SECOND PART OF THE INSTITUTES OF THE LAWS OF ENGLAND (1797 ed.)

Collier & Collier, DECISION IN PHILADELPHIA: THE CONSTITUTIONAL CONVENTION OF 1787 (1986)

Corwin, THE PRESIDENT: OFFICE AND POWERS, 1787-1984 (5th ed. 1984)

Davis, Swords Into Plowshares the Dangerous Politicization of the Military in the Post-Cold War Era, 33 VALPARAISO UNIVERSITY LAW REVIEW 61 (1998)

Dowell, MILITARY AID TO THE CIVIL POWER (1925)

Engdahl, Foundations for Military Intervention in the United States, 7 UNIVERSITY OF PUGET SOUND LAW REVIEW 1 (1983)

, The Legal Background and Aftermath of the Kent State Tragedy, 22 CLEVELAND STATE LAW REVIEW 3 (1973)

, Soldiers, Riots and Revolution: The Law and History of Military Troops in Civil Disorders, 57 IOWA LAW JOURNAL 1 (1971)

Faust, The President's Use of Troops to Enforce Federal Law, 7 CLEVELANDMARSHALL LAW REVIEW 362 (1958)

---

cause ripples in the steady flow of jurisprudence. Consequently, the notoriety of the Banks case [one of the Wounded Knee quartet of cases] should not be surprising. It also caused hesitancy on the part of the Department of Defense.* *During the Hanafi Muslem hostage situation in Washington, D.C., the Justice Department had requested grenades in case the gunmen began to kill their hostages. There was a delay in responding to the request")(footnote 55 of the article is quoted following the asterisks).

Fields & Hardy, The Third Amendment and the Issue of the Maintenance of Standing Armies: A Legal History, 35 AMERICAN JOURNAL OF LEGAL HISTORY 393 (1991)

Fields, The Third Amendment: Constitutional Protection From the Involuntary Quartering of Soldiers, 124 MILITARY LAW REVIEW 195 (Spring, 1989)

Furman, Restrictions Upon Use of the Army Imposed by the Posse Comitatus Act, 7 MILITARY LAW REVIEW 85 (January, 1960)

Gilligan, Opening the Gate? An Analysis of Military Law Enforcement Authority Over Civilian Lawbreakers On and Off the Federal Installation, 161 MILITARY LAW REVIEW 1 (September, 1999)

Hale, THE HISTORY OF THE COMMON LAW OF ENGLAND (1716 ed.)

Herz, Gun Crazy: Constitutional False Consciousness and Dereliction of Dialogic Responsibility, 75 BOSTON UNIVERSITY LAW REVIEW 57 (1995)

Kopel & Blackman, Can Soldiers Be Peace Officers" The Waco Disaster and the Militarization of American Law Enforcement, 30 AKRON LAW REVIEW 619 (1997)

Lieber, THE USE OF THE ARMY IN AID OF THE CIVIL POWER (1898)

Lorence, The Constitutionality of the Posse Comitatus Act, 8 UNIVERSITY OF KANSAS CITY LAW REVIEW 164 (1940)

Meeks, Illegal Law Enforcement: Aiding Civil Authorities in Violation of the Posse Comitatus Act, 70 MILITARY LAW REVIEW 83 (Fall, 1975)

Moore, Posse Comitatus Revisited: The Use of the Military in Civil Law Enforcement 15 JOURNAL OF CRIMINAL JUSTICE 375 (1987)

Morison, Commager, & Leuchtenburg, I THE GROWTH OF THE AMERICAN REPUBLIC (7th ed. 1980)

Pollitt, Presidential Use of Troops to Execute the Laws: A Brief History, 36 NORTH CAROLINA LAW REVIEW 117 (1958)

Porto, Construction and Application of the Posse Comitatus Act (18 USCS §1385), and Similar Predecessor Provisions, Restricting Use of United States Army and Air Force to Execute Laws, 141 ALR FED. 271 (1997 & 1999 Supp.)

Rice, New Laws and Insights Encircle the Posse Comitatus Act, 104 MILITARY LAW REVIEW 109 (Spring, 1984)

Rich, The National Guard, Drug Interdiction and Counterdrug Activities, and Posse Comitatus: The Meaning and Implications of "In Federal Service", ARMY LAWYER 35 (June, 1994)

Rich, PRESIDENTS AND CIVIL DISORDER (1941)

Sanchez, The "Drug War": The U.S. Miliary and National Security, 34 AIR FORCE LAW REVIEW 109 (1991)

Siemer & Effron, Military Participation in United States Law Enforcement Activities Overseas: The Extraterritorial Effect of the Posse Comitatus Act, 54 ST.JOHN'S LAW REVIEW 1 (1979)

Slaughter, THE WHISKEY REBELLION: FRONTIER EPILOGUE TO THE AMERICAN REVOLUTION (1986)

Stubbs, SELECT CHARTERS AND OTHER ILLUSTRATIONS OF ENGLISH CONSTITUTIONAL HISTORY FROM THE EARLIEST TIMES TO THE REIGN OF EDWARD THE FIRST (8th ed. 1895)

Swindler, MAGNA CARTA: LEGEND AND LEGACY (1965)

Thompson, MAGNA CARTA: ITS ROLE IN THE MAKING OF THE ENGLISH CONSTITUTION 1300-1629 (1948)

United States Congress, Activities of Federal Law Enforcement Agencies Toward the Branch Davidians: Joint Hearings Before the Subcomm. on Crime of the House Comm. on the Judiciary and the Subcomm. on National Security, International Affairs and Criminal Justice of the House Comm. on Government Reform and Oversight, 104th Cong., 1st Sess. (1995)

, Federal Aid in Domestic Disturbances: 1787-1903, S.DOC.NO. 209, 57th Cong., 2d Sess. (1903)

, Materials Related to the Investigation Into the Activities of Federal Law Enforcement Agencies Toward the Branch Davidians: Comm.Print by the House Comm. On the Judiciary in Conjunction with the House Comm. On Government Reform and Oversight, 104th Cong., 2d Sess. (1996)

, Military Role in Drug Interdiction: Hearing Before the House Comm. on Armed Services, Investigations Subcomm., 101st Cong., 1st Sess. (1989)

, Military Cooperation with Civilian Law Enforcement: Hearings Before the House Comm. on the Judiciary, Subcomm. on Crime, 99th Cong., 1st Sess.(1986)

, Military Cooperation with Civilian Law Enforcement: Hearings Before the House Comm. on the Judiciary, Subcomm. on Crime, 98th Cong., 1st Sess.(1985)

, Posse Comitatus Act: Hearings Before the House Comm. on the Judiciary, Subcomm. on Crime, 97th Cong., 1st Sess.(1983)

Van Alstyne, The Second Amendment and the Personal Right to Bear Arms, 43 DUKE LAW JOURNAL 1236 (1994)

Zobel, THE BOSTON MASSACRE (1987)

Notes & Comments

Airborne Drug Trafficking Deterrence: Can A Shootdown Policy Fly? 38 UCLA LAW REVIEW 1258 (1991)

A Comprehensive Study of the Use of Military Troops in Civil Disorders with Proposals for Legislative Reform, 43 UNIVERSITY OF COLORADO LAW REVIEW 399 (1972)

Don't Call Out the Marines: An Assessment of the Posse Comitatus Act, 13 TEXAS TECH LAW REVIEW 1467 (1982)

Fourth Amendment and the Posse Comitatus Act Restrictions on Military Involvement in Civil Law Enforcement, 54 GEORGE WASHINGTON LAW REVIEW 404 (1986)

Honored in the Breach: Presidential Authority to Execute the Laws With Military Force, 83 YALE LAW JOURNAL 130 (1973)

The Legality of United States Military Operations Along the United States-Mexico Border, 5 SOUTHWESTERN JOURNAL OF LAW AND TRADE IN THE AMERICAS 453 (1998)

Locked and Loaded: Taking Aim at the Growing Use of The American Military in Civilian Law Enforcement Operations, 26 LOYOLA OF LOS ANGELES LAW REVIEW 1291 (1993)

The Navy's Role in Interdicting Narcotics Traffic: War on Drugs or Ambush of the Constitution?, 75 GEORGETOWN LAW JOURNAL 1947 (1987)

Not Fit for Sea Duty: The Posse Comitatus Act, the United States Navy, and Federal Law Enforcement at Sea, 31 WILLIAM & MARY LAW REVIEW 445 (1990)

The Posse Comitatus Act: A Principle in Need of Renewal, 75 WASHINGTON UNIVERSITY LAW QUARTERLY 953 (1997)

The Posse Comitatus Act: Reconstruction Politics Reconsidered, 13 AMERICAN CRIMINAL LAW REVIEW 703 (1976)

The Posse Comitatus Act as an Exclusionary Rule: Is the Criminal to Go Free Because the Soldier Has Blundered?, 61 NORTH DAKOTA LAW REVIEW 107 (1985)

The Third Amendment's Protection Against Unwanted Military Intrusion: Engblom v. Carey, 49 BROOKLYN LAW REVIEW 857 (1983)

The United States Coast Guard's Law Enforcement Authority Under 14 U.S.C. §89: Smugglers' Blues or Boaters' Nightmare?, 34 WILLIAM & MARY LAW REVIEW 933 (1993)

United States v. Juda: Fifth Amendment Due Process and Stateless Vessels on the High Seas, 73 BOSTON UNIVERSITY LAW REVIEW 477 (1993)

United States v. Yunis: The D.C.Circuit's Dubious Approval of U.S. Long-Arm Jurisdiction Over Extraterritorial Crimes, 87 NORTHWESTERN UNIVERSITY LAW REVIEW 697 (1993)

Use of Troops to Enforce Federal Laws, 56 MICHIGAN LAW REVIEW 249 (1957).

18 U.S.C. CHAPTER 73: OBSTRUCTION OF JUSTICE (18 U.S.C. §§ 1501-1521)

Government Cover-Ups of Intelligence Crimes and Other Misconduct

Obstruction of Justice: An Abridged Overview of Related Federal Criminal Laws, RS 22783 (December 27, 2007).

CHARLES DOYLE, CONG. RESEARCH SERV., OBSTRUCTION OF JUSTICE: AN ABRIDGED OVERVIEW OF RELATED FEDERAL CRIMINAL LAWS (2007), *available at* http://www.intelligencelaw.com/library/secondary/crs/pdf/RS22783_12-27-2007.pdf.

Charles Doyle
Senior Specialist
American Law Division

Summary

Obstruction of justice is the frustration of governmental purposes by violence, corruption, destruction of evidence, or deceit. It is a federal crime. In fact, it is several crimes. Obstruction prosecutions regularly involve charges under several statutory provisions. Federal obstruction of justice laws are legion; too many for even passing reference to all of them in a single report.

The general obstruction of justice provisions are six: 18 U.S.C. 1512 (tampering with federal witnesses), 1513 (retaliating against federal witnesses), 1503 (obstruction of pending federal court proceedings), 1505 (obstruction of pending Congressional or federal administrative proceedings), 371 (conspiracy), and contempt. In addition to these, there are a host of other statutes that penalize obstruction by violence, corruption, destruction of evidence, or deceit.

This is an abridged version of CRS Report RL34303, Obstruction of Justice: An Overview of Some of the Federal Laws that Prohibit Interference with Judicial, Executive or Legislative Activities, without the footnotes, quotations, or citations to authority found in the longer report.

Witness Tampering (18 U.S.C. 1512)

Section 1512 applies to the obstruction of federal proceedings – judicial, congressional, or executive. It consists of four somewhat overlapping crimes: use of force or the threat of the use of force to prevent the production of evidence (18 U.S.C. 1512(a)); use of deception or corruption or intimidation to prevent the production of evidence (18 U.S.C. 1512(b)); destruction or concealment of evidence or attempts to do so (18 U.S.C. 1512(c)); and witness harassment to prevent the production of evidence (18 U.S.C. 1512(d)).

Obstruction by Violence (18 U.S.C. 1512(a))

Subsection 1512(a) has slightly different elements depending upon whether the offense involves a killing or attempted killing – 18 U.S.C. 1512(a)(1) or some other use of physical force or a threat – 18 U.S.C. 1512(a)(2). In essence, it condemns the use of violence to prevent a witness from testifying or producing evidence for an investigation and sets its penalties according to whether the obstructive violence was a homicide, an assault or a threat.

Auxiliary Offenses and Liability

Subsection 1512(k) makes conspiracy to violate Section 1512 a separate offense subject to the same penalties as the underlying offense. The section serves as an alternative to a prosecution under 18 U.S.C. 371 that outlaws conspiracy to violate any federal criminal statute. Section 371 is punishable by imprisonment for not more than 5 years and conviction requires the government to prove the commission of an overt act in furtherance of the scheme by one of the conspirators. Subsection 1512(k) has no specific overt act element, and the courts have generally declined to imply one under such circumstances. Regardless of which section is invoked, conspirators are criminally liable under the Pinkerton doctrine for any crime committed in the foreseeable furtherance of the conspiracy.

Accomplices to a violation of subsection 1512(a) may incur criminal liability by operation of 18 U.S.C. 2, 3, 4, or 373 as well. Section 2 treats accomplices before the fact as principals, that is, it declares that those who command, procure or aid and abet in the commission of a federal crime by another, are to be sentenced as if they committed the offense themselves.[2129] As a general rule, in order to aid and abet another to commit a crime it is necessary that a defendant in some way associate himself with the venture, that he participate in it as in something he wishes to bring about, that he seek by his action to make it succeed. It is also necessary to prove that someone else committed the underlying offense. Section 3 outlaws acting as an accessory after the fact, which occurs when one knowing

---

[2129] 18 U.S.C. 2 ("(a) Whoever commits an offense against the United States or aids, abets, counsels, commands, induces or procures its commission, is punishable as a principal. (b) Whoever willfully causes an act to be done which if directly performed by him or another would be an offense against the United States, is punishable as a principal").

that an offense has been committed, receives, relieves, comforts or assists the offender in order to hinder his or her apprehension, trial, or punishment. Prosecution requires the commission of an underlying federal crime by someone else. Offenders face sentences set at one half of the sentence attached to the underlying offense, or if the underlying offense is punishable by life imprisonment or death, by imprisonment for not more than 15 years (and a fine of not more than $250,000). The elements of misprision of felony under 18 U.S.C. 4 are (1) the principal committed and completed the felony alleged; (2) the defendant had full knowledge of that fact; (3) the defendant failed to notify the authorities; and (4) defendant took steps to conceal the crime. The offense is punishable by imprisonment for not more than 3 years and/or a fine of not more than $250,000. Solicitation to commit an offense under subsection 1512(a), or any other crime of violence, is proscribed in 18 U.S.C. 373. To establish solicitation under §373, the Government must demonstrate that the defendant (1) had the intent for another to commit a crime of violence and (2) solicited, commanded, induced or otherwise endeavored to persuade such other person to commit the crime of violence under circumstances that strongly corroborate evidence of that intent. Section 373 provides an affirmative statutory defense for one who prevents the commission of the solicited offense.[2130] Offenders face penalties set at one half of the sanctions for the underlying offense, but imprisonment for not more than 20 years, if the solicited crime of violence is punishable by death or imprisonment for life. A subsection 1512(a) violation opens up the prospect of prosecution for other crimes for which a violation of subsection 1512(a) may serve as an element. The federal money laundering and racketeering statutes are perhaps the most prominent examples of these. The racketeering statutes (RICO) outlaw acquiring or conducting the affairs of an interstate enterprise through a pattern of predicate offenses. Section 1512 offenses are RICO predicate offenses. RICO violations are punishable by imprisonment for not more that 20 years (or imprisonment for life if the predicate offense carries such a penalty), a fine of not more than $250,000 and the confiscation of related property. The money laundering provisions, among other things, prohibit financial transactions involving the proceeds of a predicate offense. RICO predicate offenses are by definition money laundering predicate offenses. Money laundering is punishable by imprisonment for not more than 20 years, a fine, and the confiscation of related property.

[2130] 18 U.S.C. 373(b), (c)("(b) It is an affirmative defense to a prosecution under this section that, under circumstances manifesting a voluntary and complete renunciation of his criminal intent, the defendant prevented the commission of the crime solicited. A renunciation is not "voluntary and complete" if it is motivated in whole or in part by a decision to postpone the commission of the crime until another time or to substitute another victim or another but similar objective. If the defendant raises the affirmative defense at trial, the defendant has the burden of proving the defense by a preponderance of the evidence. (c) It is not a defense to a prosecution under this section that the person solicited could not be convicted of the crime because he lacked the state of mind required for its commission, because he was incompetent or irresponsible, or because he is immune from prosecution or is not subject to prosecution.").

Obstruction by Intimidation, Threats, Persuasion, or Deception (18 U.S.C. 1512(b)

The second group of offenses within Section 1512 outlaws obstruction of federal Congressional, judicial, or administrative activities by intimidation, threat, corrupt persuasion or deception. In more general terms, subsection 1512(b) bans (1) knowingly, (2) using one of the prohibited forms of persuasion (intimidation, threat, misleading or corrupt persuasion), (3) with the intent to prevent a witness's testimony or physical evidence from being truthfully presented at official federal proceedings or with the intent to prevent a witness from cooperating with authorities in a matter relating to a federal offense. It also bans any attempt to so intimidate, threaten, or corruptly persuade. The conspiracy, accomplice, RICO and money laundering attributes are equally applicable to subsection 1512(b) offenses.

Obstruction by Destruction of Evidence or Harassment (18 U.S.C. 1512(c), 1512(d))

Subsection 1512(c) proscribes obstruction of official proceedings by destruction of evidence and is punishable by imprisonment for not more than 20 years. Subsection 1512(d) outlaws harassing federal witnesses and is a misdemeanor punishable by imprisonment for not more than one year. Both enjoy the conspiracy, accomplice, RICO and money laundering attributes that to apply to all Section 1512 offenses.

Obstructing Federal Courts (18 U.S.C. 1503): The Omnibus Provision

Unlike Section 1512, Section 1503 does not to apply to the obstruction of Congressional or administrative proceedings. It condemns obstructing pending judicial proceedings. For conviction, the government must prove beyond a reasonable doubt: (1) that there was a pending judicial proceeding, (2) that the defendant knew this proceeding was pending, and (3) that the defendant then corruptly endeavored to influence, obstruct, or impede the due administration of justice. Offenders are punished according to the nature of obstruction: murder and manslaughter are punished as those crimes are punished when committed in violation of sections 1111 and 1112; attempted murder, attempted manslaughter, or any violation involving a juror called to hear a case relating to a class A or B felony is punishable by imprisonment for not more than 20 years; and all other offenses by imprisonment for not more than 10 years. Conspiracy to violate Section 1503 can only be prosecuted under the general conspiracy statute. Section 1503 offenses are RICO predicate offenses and consequently money laundering predicate offenses. Those who aid and abet a Section 1503 offense are liable as principals and are punishable as if they committed the offense themselves. An individual who knows that another has committed a Section 1503 offense and nevertheless assists the offender in order to hinder his capture, trial or punishment is in turn punishable as an accessory after the fact. And an

individual who affirmatively conceals the commission of a Section 1503 by another is guilty of misprision.

Retaliating Against Federal Witnesses (18 U.S.C. 1513)

Section 1513 prohibits witness or informant retaliation in the form of killing, attempting to kill, inflicting or threatening to inflict bodily injury, damaging or threatening to damage property, and conspiracies to do so. It also prohibits economic retaliation against federal witnesses, but only witnesses in court proceedings and only on criminal cases. Its penalty structure is comparable to that of Section 1503. Section 1513 offenses are RICO predicate offenses and money laundering predicate offenses, and the provisions for conspirators and accomplices apply as well.

Obstructing Congressional or Administrative Proceedings (18 U.S.C. 1505)

Section 1505 outlaws obstructing Congressional or federal administrative proceedings, a crime punishable by imprisonment not more than 5 years (not more than 8 years if the offense involves domestic or international terrorism). The crime has three essential elements. First, there must be a proceeding pending before a department or agency of the United States. Second, the defendant must be aware of the pending proceeding. Third, the defendant must have intentionally endeavored corruptly to influence, obstruct or impede the pending proceeding. Section 1505 offenses are not RICO or money laundering predicate offenses. Conspiracy to obstruct administrative or Congressional proceedings may be prosecuted under 18 U.S.C. 371, and the general aiding and abetting, accessory after the fact, and misprision statutes are likely to apply with equal force in the case of obstruction of an administrative or Congressional proceeding.

Conspiracy to Obstruct to Defraud (18 U.S.C. 371)

Section 371 contains both a general conspiracy prohibition and a specific obstruction conspiracy prohibition in the form of a conspiracy to defraud proscription. The elements of conspiracy to defraud the United States are: (1) an agreement of two more individuals; (2) to defraud the United States; and (3) an overt act by one of the conspirators in furtherance of the scheme. The fraud covered by the statute reaches any conspiracy for the purpose of impairing, obstructing or defeating the lawful functions of any department of Government by deceit, craft or trickery, or at least by means that are dishonest. The scheme may be designed to deprive the United States of money or property, but it need not be so; a plot calculated to frustrate the functions of a governmental entity will suffice.

Criminal Contempt of Court

The final and oldest of the general obstruction provisions is contempt. Contemporary federal contempt derives from statute, rule and inherent or auxiliary authority. Criminal contempt comes in two forms, direct and indirect. Direct contempt involves misconduct in the presence of the court and is punished

to ensure the decorum of the court and the dignity of the bench. Indirect contempt consists of those obstructions committed outside the presence of the court. Direct contempt may be summarily punished; indirect contempt may not. A court may punish as criminal contempt disobedience or resistance to its lawful writ, process, order, rule, decree, or command. Criminal contempt may be punished by imprisonment or by a fine or both. The Sixth Amendment right to a jury trial limits the term of imprisonment which a court may summarily impose to a maximum of six months.

Contempt of Congress

Contempt of Congress is punishable by statute and under the inherent powers of Congress. Congress has not exercised its inherent contempt power for some time. The statutory contempt of Congress provision, 2 U.S.C. 192, outlaws the failure to obey a Congressional subpoena or the refusal to answer questioning at a Congressional hearing. The offense is punishable by imprisonment for not more than one year and a fine of up to $100,000.

Obstruction of Justice by Violence or Threat

Several other federal statutes outlaw use of threats or violence to obstruct federal government activities. One, 18 U.S.C. 115, prohibits acts of violence against judges, jurors, officials, former officials, and their families in order to impede or retaliate for the performance of their duties. It makes assault, kidnaping, murder, and attempts and conspiracies to commit such offenses in violation of the section subject to the penalties imposed for those crimes elsewhere in the Code. It makes threats to commit an assault punishable by imprisonment for not more than 6 years and threats to commit any of the other offenses under the section punishable by imprisonment for not more than 10 years. Another, 18 U.S.C. 1114, protects federal officers and employees as well as those assisting them, from murder, manslaughter, and attempted murder and manslaughter committed during or account of the performance of their duties. The section's coverage extends to government witnesses. Other provisions protect federal officers and employees from kidnaping and assault committed during or on account of the performance of their duties, but their coverage of those assisting them is less clear. Beyond these general prohibitions, federal law proscribes the murder, kidnaping, or assault of Members of Congress, Supreme Court Justices, or Cabinet Secretaries; and a number of statutes outlaw assaults on federal officers and employees responsible for the enforcement of particular federal statutes and programs.

Obstruction of Justice by Bribery: 18 U.S.C. 201

Section 201 outlaws offering or soliciting bribes or illegal gratuities in connection with judicial, congressional and administrative proceedings. Bribery is a quid pro quo offense. It condemns invitations and solicitations to corruption. The penalty structure for bribery is fairly distinctive: imprisonment for not more than 15 years; a fine of the greater of three times the amount of the bribe or $250,000;

and disqualification from holding any federal position of honor or trust thereafter.

Mail and Wire Fraud

The mail fraud and wire fraud statutes have been written and constructed with such sweep that they cover among other things, obstruction of government activities by corruption. They reach any scheme to obstruct the lawful functioning in the judicial, legislative or executive branch of government that involves (1) the deprivation of money, property or honest services, and (2) the use of the mail or wire communications as an integral part of scheme. Congress expanded the scope of the mail and wire fraud statutes with the passage of 18 U.S.C. 1346 which defines the "scheme to defraud" element in the fraud statutes to include a scheme "to deprive another of the intangible right of honest services." Some courts have said that honest services fraud in the public sector typically occurs in either of two situations: (1) bribery, where a public official was paid for a particular decision or action; or (2) failure to disclose a conflict of interest resulting in personal gain. Prosecutors may favor a mail or wire fraud charge over or in addition to bribery charge if for no the reason than that under both fraud sections offenders face imprisonment for not more than 20 years rather than the 15-year maximum found in Section 201.

Obstruction by Extortion Under Color of Official Right (18 U.S.C. 1951)

Extortion under color of official right occurs when a public official receives a payment to which he is not entitled, knowing it is being provided in exchange for the performance of an official act. Liability may be incurred by public officers and employees, those in the process of becoming public officers or employees, those who hold themselves out to be public officers or employees, their coconspirators, or those who aid and abet public officers or employees in extortion under color or official right. The payment need not have been solicited, nor need the official act for which it is exchanged have been committed. The prosecution must establish that the extortion obstructed, delayed, or affected interstate or foreign commerce, but the impact need not have actually occurred nor been even potentially severe. Violations are punishable by imprisonment for not more than 20 years.

Obstruction of Justice by Destruction of Evidence

Other than subsection 1512(c), there are three federal statutes which expressly outlaw the destruction of evidence in order to obstruct justice: 18 U.S.C. 1519 prohibits destruction of evidence in connection with federal investigation or bankruptcy proceedings, 18 U.S.C. 1520 prohibits destruction of corporate audit records, and 18 U.S.C. 2232(a) prohibits the destruction of property to prevent the government from searching or seizing it.

OBSTRUCTION OF JUSTICE BY DECEPTION

In addition to the obstruction of justice provisions of 18 U.S.C. 1503 and 1512, there are four other general statutes that outlaw obstructing the government's business by deception. Three involve perjury: 18 U.S.C. 1623 that outlaws false swearing before federal courts and grand juries; 18 U.S.C. 1621 the older and more general prohibition that proscribes false swearing in federal official matters (judicial, legislative, or administrative); and 18 U.S.C. 1622 that condemns subornation, that is, inducing another to commit perjury. The fourth, 18 U.S.C. 1001, proscribes material false statements concerning any matter within the jurisdiction of a federal executive branch agency, and to a somewhat more limited extent with the jurisdiction of the federal courts or a Congressional entity.

The State Secrets Privilege

The State Secrets Privilege: Limits on Litigation Involving Classified Information, R40603 (May 28, 2009).

EDWARD C. LIU, CONGRESSIONAL RESEARCH SERV., THE STATE SECRETS PRIVILEGE: LIMITS ON LITIGATION INVOLVING CLASSIFIED INFORMATION (2009), *available at* http://www.intelligencelaw.com/library/secondary/crs/pdf/R40603_5-28-2009.pdf.

Edward C. Liu
Legislative Attorney
eliu@crs.loc.gov, 7-9166

May 28, 2009

Summary

The state secrets privilege is a judicially created evidentiary privilege that allows the government to resist court-ordered disclosure of information during litigation, if there is a reasonable danger that such disclosure would harm the national security of the United States. The Supreme Court first described the modern analytical framework of the state secrets privilege in the 1953 case of *United States v. Reynolds*. In its opinion, the Court laid out a two-step procedure to be used when evaluating a claim of privilege to protect state secrets. First, there must be a formal claim of privilege, lodged by the head of the department which has control over the matter, after actual personal consideration by that officer. Second, a court must independently determine whether the circumstances are appropriate for the claim of privilege, and yet do so without forcing a disclosure of the very thing the privilege is designed to protect. If the privilege is appropriately invoked, it is absolute and the disclosure of the underlying information cannot be compelled by the court.

The Classified Information Procedures Act (CIPA) provides pretrial procedures that permit a trial judge to rule on questions of admissibility involving classified information before introduction of the evidence in open court. The use of classified evidence may also implicate criminal defendants' rights to exculpatory information and witnesses' statements held by the prosecution, or their right to confront witnesses under the Sixth Amendment.

Congressional action may affect the operation or coverage of the state secrets privilege. In 2008, a federal district court held that the Foreign Intelligence Surveillance Act supplanted the state secrets privilege with respect to civil claims of unlawful electronic surveillance. In the 111th Congress, House and Senate versions of bills entitled "the State Secrets Protection Act," H.R. 984 and S. 417,

have been introduced to codify the privilege. The bills would additionally limit the privilege to cases where significant harm to national security was presented, require judicial review of the actual information claimed to be privileged, and require the Attorney General to report to Congress within 30 days of any invocation of the state secrets privilege.

Introduction

The state secrets privilege, derived from common law, is an evidentiary privilege that allows the government to resist court-ordered disclosure of information during litigation if there is a reasonable danger that such disclosure would harm the national security of the United States.[2131] In recent years, some have suggested that this privilege has been overused by the executive branch to prevent disclosure of its questionable conduct, particularly with respect to the "war on terror."[2132] Both the Bush and Obama administrations have asserted the state secrets privilege in suits brought by private litigants alleging unlawful electronic surveillance[2133] and extraordinary rendition.[2134]

This report is intended to provide an overview of the protections afforded by the state secrets privilege. Although it is primarily a construct of the judiciary,[2135] Congress has previously enacted and continues to consider legislation that may affect its operation. In 1980, Congress enacted the Classified Information Procedures Act to provide uniform procedures to be used in federal criminal

---

[2131] For a common law discussion of the privilege, see 8 Wigmore Evidence §§ 2367-2379 (J. McNaughton rev. 1961); for a more recent description, see EDWARD J. IMWINKELREID, THE NEWWIGMORE: ATREATISE ON EVIDENCE: EVIDENTIARY PRIVILEGES, ch. 8 (2002). It has also been argued that the privilege is derived "from the President's authority over national security, and thus is imbued with 'constitutional overtones.'" Amanda Frost, The State Secrets Privilege And Separation Of Powers, 75 FORDHAM L. REV. 1931, 1935 (Mar. 2007).

[2132] Editorial, Securing Lawsuits, WASH. POST, May 11, 2009, at A16; Editorial, Unraveling Injustice, N.Y. TIMES, Feb. 5, 2009, at 30; Louis Fisher, Examining the State Secrets Privilege: Protecting National Security While Preserving Accountability, Statement Before the Senate Judiciary Committee, Feb. 13, 2008, at 3, available at http://loc.gov/law/help/usconlaw/pdf/ssp_senatejudiciary.pdf; Editorial, Revisit the State Secrets Privilege, PITTSBURGH POST-GAZETTE, Oct. 15, 2007, at B7.

[2133] See, e.g., Al-Haramain Islamic Found., Inc. v. Bush, 507 F.3d 1190, 1204-1205 (9th Cir. 2007); Carrie Johnson, Handling of State Secrets at Issue; Like Predecessor, New Justice Dept. Claiming Privilege, WASH. POST, at Mar. 25, 2009, at A1.

[2134] See, e.g., El-Masri v. U.S., 479 F.3d 296 (4th Cir. 2007) and Carrie Johnson, Handling of State Secrets, supra note 3 ("Six weeks ago, Attorney General Eric H. Holder Jr. disappointed civil libertarians by invoking the state-secrets claim in a case against a Boeing Co. subsidiary accused of transporting five terrorism suspects to countries where they were tortured").

[2135] See FED. R. EVID. 501.

litigation involving classified information.[2136] In 2008, a federal district court held that portions of the Foreign Intelligence Surveillance Act (FISA) superseded the state secrets privilege, at least with respect to civil claims alleging unlawful electronic surveillance under FISA.[2137] In the 111th Congress, different versions of the State Secrets Protection Act have been introduced in both the House of Representatives[2138] and the Senate.[2139]

After reviewing the case law that defines the current state secrets privilege, this report will discuss both enacted and proposed legislation that may affect the scope or function of the state secrets privilege.

United States v. Reynolds: The Seminal Case

The Supreme Court first articulated the modern analytical framework of the state secrets privilege in 1953, when it decided *United States v. Reynolds*.[2140] That case involved multiple wrongful death claims brought by the widows of three civilians who died aboard a military aircraft that crashed while testing secret electronic equipment. The plaintiffs had sought discovery of the official post-incident report and survivors' statements that were in the possession of the Air Force. The Air Force opposed disclosure of those documents as the aircraft and its occupants were engaged in a "highly secret mission of the Air Force" at the time of the crash.[2141] The federal district court ordered the Air Force to produce the documents so that it could independently determine whether they contained privileged information. When the Air Force refused to provide the documents to the court, the district court ruled in favor of the plaintiffs on the issue of negligence; the court of appeals subsequently affirmed the district court's ruling.[2142]

The Supreme Court reversed. In its opinion, the Court laid out a two-step procedure to be used when evaluating a claim of privilege to protect state secrets. First, "there must be a formal claim of privilege, lodged by the head of the department which has control over the matter, after actual personal

---

[2136] P.L. 96-456.

[2137] In re NSA Telcoms. Records Litig., 564 F. Supp. 2d 1109, 1119 (N.D. Cal. 2008).

[2138] H.R. 984.

[2139] S. 417.

[2140] U.S. v. Reynolds, 345 U.S. 1 (1953).

[2141] Id. at 5. The Air Force did offer to make the surviving crew available for examination by the plaintiffs. Id.

[2142] Reynolds v. U.S., 192 F.2d 987 (3d Cir. 1951).

consideration by that officer."[2143] Second, "the court itself must determine whether the circumstances are appropriate for the claim of privilege, and yet do so without forcing a disclosure of the very thing the privilege is designed to protect."[2144]

Asserting the Privilege

The first requirement identified by the Court, the assertion of the privilege, is a largely procedural hurdle to assure that the privilege is "not to be lightly invoked."[2145] Nevertheless this requirement is readily met through the written assertion of the privilege by the head of the department in control of the information in question. The lack of a formal assertion has been excused because strict adherence to the requirement would have had little or no benefit.[2146]

Evaluating the Validity of the Privilege

In contrast, "the latter requirement is the only one which presents real difficulty."[2147] For example, although the Supreme Court's holding in Reynolds recognized that it is the role of the judiciary to evaluate the validity of claims of privilege, the Court declined to require courts to automatically require inspection of the underlying information. As the Court noted in Reynolds, "too much judicial inquiry into the claim of privilege would force disclosure of the thing the privilege was meant to protect, while a complete abandonment of judicial control would lead to intolerable abuses."[2148] In light of this dilemma, the Court chose to chart a middle course, employing a "formula of compromise" to balance the competing

---

[2143] Id. at 8.

[2144] Id. With respect to the facts at hand, the Court noted that the Secretary of the Air Force had filed a formal assertion of the privilege, and that there was a reasonable danger "that the accident investigation report would contain references to the secret electronic equipment which was the primary concern of the mission." Id. at 10. Furthermore, it was "apparent that these electronic devices must be kept secret if their full military advantage is to be exploited in the national interests." Id. Thus, the Court upheld the government's assertion of the state secrets privilege and barred discovery of the requested documents by the plaintiffs.

[2145] Id. at 7.

[2146] But see Clift v. U.S., 597 F.2d 826, 828-9 (2d Cir. 1979) (preventing discovery of documents in a patent infringement suit brought by the inventor of a cryptographic device against the government where the Director of the NSA had submitted an affidavit stating that disclosing the contents of the documents would be a criminal violation, but had not formally asserted the state secrets privilege; the court reasoned that imposition of the formal requirement would have had little or no benefit in this circumstance).

[2147] Reynolds, 345 U.S. at 8.

[2148] Id.

interests of oversight by the judiciary and national security interests.[2149] Under this scheme, the privilege should be found valid when the court is satisfied that there is a reasonable danger that disclosure "will expose military matters which, in the interest of national security, should not be divulged."[2150] Once the court is satisfied that the privilege is valid, it should not further "jeopardize the security which the privilege is meant to protect by insisting upon an examination of the evidence, even by the judge alone, in chambers."[2151]

Whether a court can be satisfied without examining the underlying information may be affected by the amount of deference afforded to the government's representations regarding the information. In Reynolds, the Court noted that the necessity of the underlying information to the litigation will determine "how far the court should probe in satisfying itself that the occasion for invoking the privilege is appropriate."[2152] In the case of Reynolds, the Court noted that the Air Force had offered to make the surviving crew members available for examination by the plaintiffs.[2153] Because of this alternative avenue of information, the Court was satisfied that the privilege was valid based primarily upon representations made by the government regarding the contents of the documents.[2154] Conversely, less deference to the government's representations may be warranted where a private litigant has a strong need for the information.[2155]

The Effect of a Valid Privilege

If the privilege is appropriately invoked, it is absolute and the disclosure of the underlying information cannot be compelled by the court. Although a private litigant's need for the information may be relevant to the amount of deference afforded to the government, "even the most compelling necessity cannot overcome the claim of privilege if the court is ultimately satisfied" that the privilege is appropriate.[2156]

[2149] Id. at 9.

[2150] Id. at 10.

[2151] Id.

[2152] Id. at 11.

[2153] Id. at 5.

[2154] Id. at 11.

[2155] See, e.g., Molerio v. FBI, 749 F.2d 815, 822 (D.C. Cir. 1984) (in camera examination of classified information was appropriate where it was central to litigation); Al-Haramain Islamic Found., Inc. v. Bush, 507 F.3d at 1203-1204 ("We reviewed the Sealed Document in camera because of [plaintiff's] admittedly substantial need for the document to establish its case").

[2156] Id.

In some circumstances, the exclusion of the protected information can be fatal to the litigation. In *Halkin v. Helms*, the D.C. Circuit was confronted with a claim of privilege regarding the National Security Agency's alleged interception of international communications to and from persons who had been targeted by the Central Intelligence Agency.[2157] After deciding that the claim of privilege was valid, the D.C. Circuit affirmed the protection of that information from discovery.[2158] Although some non-privileged evidence that the plaintiffs were targeted by the Central Intelligence Agency (CIA) existed, the court dismissed the suit after deciding that without the privileged information, the plaintiffs would not be able to establish a prima facie case of unlawful electronic surveillance.

A similar result may occur if the state secrets privilege requires the exclusion of evidence central to a litigant's defense. In *Molerio v. Federal Bureau of Investigation*, a job seeker alleged that the Federal Bureau of Investigation (FBI) had disqualified him based upon his father's political ties to socialist organizations in violation of the applicant and his father's First Amendment rights.[2159] In response, the FBI asserted that it had a lawful reason to disqualify the plaintiff, but claimed that its reason was protected by the state secrets privilege. After reviewing the FBI's claim *in camera*, the D.C. Circuit agreed that the evidence of a nondiscriminatory reason was protected and that its exclusion would deprive the FBI of a valid defense. Therefore, the dismissal of that action was required once the privilege was determined to be valid.[2160]

Whether the assertion of the state secrets privilege is fatal to a particular suit, or merely excludes privileged evidence from further litigation, is a question that is highly dependent upon the specific facts of a case. Two recent cases from the Fourth and Ninth Circuits, dealing with the federal government's rendition practices,[2161] can be viewed as exemplifying the varied conclusions courts have reached in ostensibly similar cases. In *El-Masri v. United States*, the plaintiff brought a civil suit against various government officials and private transportation companies alleging that he had been unlawfully rendered to a

---

[2157] Halkin v. Helms, 690 F.2d 977 (D.C. Cir. 1982).

[2158] The other evidence of CIA targeting was never claimed to be privileged by the government. Id. at 997.

[2159] Molerio v. FBI, 749 F. 2d at 824-825.

[2160] Id. at 825.

[2161] These suits involve controversies in which the United States allegedly rendered suspected terrorists to states known to practice torture. See CRS Report RL32890, Renditions: Constraints Imposed by Laws on Torture, by Michael John Garcia.

secret CIA detention site.[2162] Similarly, in *Mohamed v. Jeppesen Dataplan*, a subsidiary of the Boeing Company was sued for allegedly transporting the plaintiffs to countries that engaged in torture.[2163] In both cases, the government asserted the state secrets privilege and argued that the suits should be dismissed because the issues involved in the lawsuits could not be litigated without risking disclosure of privileged information.[2164] Both trial courts held that the privilege was properly invoked and dismissed both complaints at the pleadings stage. However, upon appeal the respective circuits reached markedly different conclusions.

In El-*Masri*, the Fourth Circuit agreed with the trial court and affirmed the dismissal of the case. According to the Fourth Circuit's opinion, any attempt to prove or disprove the allegations in the complaint would necessarily involve disclosing the internal organization and procedures of the CIA, as well as secret contracts with the transportation companies. Therefore, because "the very subject matter of [the] action is a state secret,"[2165] the court was required to dismiss the suit upon the successful invocation of the privilege by the government.[2166]

In contrast, the Ninth Circuit held that the state secrets privilege only excluded privileged evidence from discovery or admission at trial, and did not require the dismissal of the complaint at the pleadings stage.[2167] While the exclusion of privileged evidence from discovery might ultimately be fatal to the litigation, because it prevents the plaintiffs from establishing a prima facie case or denies the defendant a valid defense, the Jeppesen court held that dismissal of a suit on the pleadings because of the "very subject matter" of the privileged information is

---

[2162] El-Masri v. U.S., 479 F.3d 296 (4th Cir. 2007).

[2163] Mohamed v. Jeppesen Dataplan, 2009 U.S. App. LEXIS 8978 (9th Cir. Apr. 28, 2009).

[2164] El-Masri v. U.S., 479 F.3d at 301. In Jeppesen, the federal government was not initially a defendant, but intervened in the case to assert the privilege and simultaneously moved to dismiss. Mohamed v. Jeppesen Dataplan, 539 F. Supp. 2d 1128, 1132-1133 (N.D. Cal. 2008).

[2165] El-Masri, 479 F.3d at 310 (quoting Kasza v. Browner, 133 F.3d 1159, 1170 (9th Cir. 1998) (upholding summary judgment for defendant Air Force in suit alleging unlawful handling of hazardous waste after government successfully asserted state secrets privilege in response to almost all of plaintiff's discovery requests)).

[2166] El-Masri, 479 F.3d at 311 (citing Sterling v. Tenet, 416 F.3d 338, 341 (4th Cir. 2005) (Title VII claim brought by covert employee of the CIA cannot be litigated without disclosing privileged information)).

[2167] Mohamed, 2009 U.S. App. LEXIS 8978, at 27-28. The court also held that the Totten rule, which requires the immediate dismissal of suits involving espionage contracts and is discussed in the next section, was not applicable here. See infra notes 39-44 and accompanying text.

not warranted,[2168] except in the special case of contracts for espionage discussed below.

Totten v. United States: The Special Case of Nonjusticiable Contracts for Espionage

Although courts may reach different results when considering the effect of an assertion of the state secrets privilege, there is one category of cases involving state secrets that courts have generally held to be nonjusticiable: specifically, cases brought against the federal government to enforce contracts for espionage.

This rule was first enunciated in Totten v. United States, in which the Supreme Court dismissed a breach of contract claim brought against the government by the estate of a former Civil War spy for the Union.[2169] The Court dismissed the claim noting that "public policy forbids the maintenance of any suit in a court of justice, the trial of which would inevitably lead to the disclosure of matters which the law itself regards as confidential."[2170]

In *Tenet v. Doe*, the Supreme Court reaffirmed the central holding of Totten, which stated that controversies over espionage contracts are not justiciable.[2171] Prior to that decision, the relevance of the *Totten* rule in light of the Court's intervening decision in *Reynolds* was unclear. For example, in the lower court proceedings leading up to the Supreme Court's opinion in *Tenet*, the Ninth Circuit had held that the immediate dismissal doctrine required in *Totten* was, in modern times, only appropriate once the state secrets privilege had been properly asserted and evaluated pursuant to *Reynolds* and its progeny.[2172]

Ultimately in *Tenet*, the Supreme Court held that the *Totten* rule had not been "reduced to an example of the state secrets privilege," and that "the state secrets privilege and the more frequent use of in camera judicial proceedings simply cannot provide the absolute protection we found necessary in enunciating the *Totten* rule."[2173] Therefore disputes over contracts for espionage appear to remain

---

[2168] Id. at 18. Therefore, the appellate court reversed the trial court's dismissal and remanded the case for further proceedings. Id. at 38-40.

[2169] Totten v. U.S., 92 U.S. 105 (1876).

[2170] Id. at 107.

[2171] Tenet v. Doe, 544 U.S. 1 (2005).

[2172] Doe v. Tenet, 329 F.3d 1135 (9th Cir. 2003) (rev'd by Tenet v. Doe, 544 U.S. at 1).

[2173] Tenet v. Doe, 544 U.S. at 10-11.

a special category of cases which the courts have no jurisdiction over, even without any invocation of the state secrets privilege by the government.[2174]

The Classified Information Procedures Act and Secret Evidence in Criminal Litigation

Although the cases discussed thus far have dealt only with civil litigation, the government enjoys a similar privilege with respect to the use of classified information in criminal litigation. In practice, this privilege operates differently in the criminal context as the government is simultaneously responsible for prosecution and the protection of national security. Therefore, when classified information is part of the prosecution's case-in-chief, the government may resolve these competing interests before any judicial proceedings are necessary.

However, once criminal proceedings have been instigated, the Sixth Amendment provides a criminal defendant with the right to have a public trial, to be confronted with the witnesses against him, and to present relevant evidence in his defense.[2175] In some prosecutions, particularly those conducted as part of the "global war on terror," the defendant's presentation of evidence in a public trial could also present risks to the national security of the United States. Additionally, in situations known colloquially as "graymail," the defendant may be seeking to introduce tangentially related classified information solely to force the prosecution to dismiss the charges against him.[2176]

This dilemma was one factor leading to Congress's enactment of the Classified Information Procedures Act (CIPA),[2177] which "provides pretrial procedures that will permit the trial judge to rule on questions of admissibility involving classified information before introduction of the evidence in open court."[2178] These procedures, which are summarized in **Appendix A**, are intended to provide a means for the court to distinguish instances of graymail from cases in which classified information is actually material to the defense.

Importantly, the text of CIPA contains no standards for a court to apply to evaluate whether a claim of privilege is valid. As the Second Circuit has noted, CIPA "presupposes a governmental privilege against disclosing classified

---

[2174] Id. at 11 ("requiring the Government to invoke the privilege on a case-by-case basis risks the perception that it is either confirming or denying relationships with individual plaintiffs").

[2175] U.S. CONST. amend. VI.

[2176] See S.REPT. 96-823 at 1-4 (part of the legislative history of CIPA).

[2177] P.L. 96-456, codified at 18 U.S.C. app. 3 § 1-16.

[2178] S.REPT. 96-823, at 1.

information" in criminal matters.[2179] Other courts have agreed that CIPA does not create any new privilege against the disclosure of classified information,[2180] but merely establishes uniform procedures to determine the materiality of classified information to the defense in a criminal proceeding.[2181] Under CIPA, if the government objects to disclosure of classified information that is material to the defense, the court is required to accept that assertion without scrutiny, and impose nondisclosure orders upon the defendant.[2182] However, in such cases the court is also empowered to dismiss the indictment against the defendant, or impose other sanctions that are appropriate.[2183] Therefore, once classified information has been determined through the procedures under CIPA to be material, it falls to the government to elect between permitting the disclosure of that information or the sanctions the court may impose.

Prosecutions implicating classified information can be factually varied, but an important distinction that may be made among them is from whom information is being kept. In cases where the defendant is already privy to some classified information, the government may be seeking to prevent disclosure to the general public. However, in the case of terrorism prosecutions, the more typical situation is likely to be the introduction of classified information as part of the prosecution's case against the defendant. In these cases, protective orders preventing disclosure to the defendant, as well as to the public, may be sought by the government. Constitutional issues related to withholding classified information from a criminal defendant arise during two distinct phases of criminal litigation. First, issues may arise during the discovery phase when the defendant requests and is entitled to classified information in the possession of the prosecution. Secondly, issues may arise during the trial phase, when classified information is sought to be presented to the trier-of-fact as evidence of the defendant's guilt. The issues implicated during both of these phases are discussed below.

[2179] U.S. v. Aref, 533 F.3d 72, 78-79 (2nd Cir. 2008) (holding that the state secrets privilege may be asserted in criminal prosecutions, subject to the procedures in CIPA, if the information is not relevant and helpful to the defense).

[2180] U.S. v. Meija, 448 F.3d 436, 455 (D.C. Cir. 2006). See also U.S. v. Yunis, 867 F.2d 617, 621 (D.C. Cir. 1989).

[2181] The legislative history of CIPA states that "it is well-settled that the common law state secrets privilege is not applicable in the criminal arena." H.REPT. 96-831 pt. 1, at n.12. But, see U.S. v. Aref, 533 F.3d 72 at 79 (observing that this statement in the legislative history "sweeps too broadly").

[2182] 18 U.S.C. app. 3, § 6(e)(1).

[2183] 18 U.S.C. app. 3, § 6(e)(2).

Withholding Classified Information During Discovery

The mechanics of discovery in federal criminal litigation are governed primarily by the Federal Rules of Criminal Procedure (FED. R. CRIM. P.). These rules provide the means by which defendants may request information and evidence in the possession of the prosecution, in many cases prior to trial. There are two important classes of information that the prosecution must provide, if requested by the defendant: specifically *Brady* material and Jencks material.

Brady material, named after the seminal Supreme Court case *Brady v. Maryland*,[2184] refers to information in the prosecution's possession which is exculpatory, or tends to prove the innocence of the defendant. For example, statements by witnesses that contradict or are inconsistent with the prosecution's theory of the case must be provided to the defense, even if the prosecution does not intend to call those witnesses. Prosecutors are considered to have possession of information that is in the control of agencies that are "closely aligned with the prosecution,"[2185] but, whether information held exclusively by elements of the intelligence community could fall within this category does not appear to have been addressed.[2186]

Jencks material refers to written statements made by a prosecution witness who has testified or may testify. For example, this would include a report made by a witness called to testify against the defendant. In the Supreme Court's opinion in *Jencks v. United States*,[2187] the Court noted the high impeachment value a witness's prior statements can have, both to show inconsistency or incompleteness of the in-court testimony. Subsequently, this requirement was codified by the Jencks Act.[2188]

The operation of *Jencks* and *Brady* may differ significantly in the context of classified information. Under § 4 of CIPA, which deals with disclosure of

---

[2184] Brady v. Maryland, 373 U.S. 83 (1963) (holding that due process requires prosecution to turn over exculpatory evidence in its possession).

[2185] United States v. Brooks, 966 F.2d 1500, 1503 (1992).

[2186] But, see United States v. Libby, 429 F. Supp. 2d 1 (D.D.C. 2006) (in a prosecution involving the unauthorized disclosure of classified information, the CIA was closely aligned with special prosecutor for purposes of Brady based on the free flow of other documents between the CIA and the prosecutor).

[2187] Jencks v. U.S., 353 U.S. 657 (1957) (holding that, in a criminal prosecution, the government may not withhold documents relied upon by government witnesses, even where disclosure of those documents might damage national security interests).

[2188] Codified at 18 U.S.C. § 3500. The Jencks Act provides definitions for so-called "Jencks material" and requires disclosure of such material to the defense, but only after the witness has testified.

discoverable classified information, the prosecution may request to submit either a redacted version or a substitute of the classified information in order to prevent harm to national security.[2189] While the court may reject the redacted version or substitute as an insufficient proxy for the original, this decision is made ex parte without the defendant's input. Classified information that is also *Jencks* or *Brady* material is still subject to CIPA and may be provided in a redacted or substituted form.[2190]

In some cases, the issue may not be the disclosure of a document or statement, but whether to grant the defendant pre-trial access to government witnesses. In *United States v. Moussaoui*, one issue was the ability of the defendant to depose "enemy combatant" witnesses who were, at the time the deposition was ordered, considered intelligence assets by the United States.[2191] Under the FED. R. CRIM. P., a defendant may request a deposition in order to preserve testimony at trial.[2192] In *Moussaoui*, the court had determined that a deposition of the witnesses by the defendant was warranted because the witnesses had information that could have been exculpatory or could have disqualified the defendant for the death penalty.[2193] However, the government refused to produce the deponents citing national security concerns.[2194]

In light of this refusal, the Fourth Circuit, noting the conflict between the government's duty to comply with the court's discovery orders and the need to protect national security, considered whether the defendant could be provided with an adequate substitute for the depositions. The court also noted that substitutes would necessarily be different from depositions, and that these

---

[2189] 18 U.S.C. app. 3, § 4.

[2190] See United States v. O'Hara, 301 F.3d 563, 569 (7th Cir. 2002) (holding that in camera examination and redaction of purported Brady material by trial court was proper).

[2191] United States v. Moussaoui, 382 F.3d 453 (4th Cir. 2004). Moussaoui was prosecuted for his involvement in the conspiracy to commit the terrorist attacks of September 11, 2001. While the U.S. Court of Appeals for the Fourth Circuit held that CIPA did not apply to question of whether Moussaoui and his standby counsel would be allowed to depose to enemy combatant witnesses, United States v. Moussaoui, 333 F.3d 509, 514-15 (4th Cir. 2003), both the district court and the Fourth Circuit looked to CIPA for guidance when considering the question, see Moussaoui, supra, 382 F.3d at 471 n. 20 and accompanying text. Further litigation of these issues was rendered moot when Zacarias Moussaoui subsequently entered a guilty plea.

[2192] FED. R. CRIM. P. 15(a). The court should permit the deposition if there are exceptional circumstances and it is in the interest of justice.

[2193] Moussaoui, 382 F.3d at 458, 473-475.

[2194] Id. at 459.

differences should not automatically render the substitutes inadequate.[2195] Instead, the appropriate standard was whether the substitutes put the defendant in substantially the same position he would have been absent the government's national security concerns.[2196] Here, the Fourth Circuit seemed to indicate that government-produced summaries of the witnesses' statements, with some procedural modifications, could be adequate substitutes for depositions.[2197]

The Confrontation Clause and the Use of Secret Evidence At Trial

The use of secret evidence at trial also implicates constitutional concerns. As described above, there may be instances where disclosure of classified information to the defendant would be damaging to the national security. In these instances, the prosecution may seek to present evidence at trial in a manner that does not result in disclosure to the defendant. One proposed scenario might be the physical exclusion of the defendant from those portions of the trial, while allowing the defendant's counsel to remain present.[2198] However, such proceedings could be viewed as unconstitutionally infringing upon the defendant's Sixth Amendment right to confrontation.[2199]

Historically, defendants have had the right to be present during the presentation of evidence against them, and to participate in their defense.[2200] But other courts have approved of procedures which do not go so far as to require the defendant's physical presence. In *United States v. Abu Ali*, the Fourth Circuit permitted video conferences to allow the defendant to observe, and be observed by, witnesses who were being deposed in Riyadh, Saudi Arabia.[2201] The Fourth Circuit stated that

---

[2195] Id. at 477.

[2196] Id.

[2197] Id. at 479-483. The precise form of the deposition substitutes is unclear as significant portions of the Fourth Circuit's opinion dealing with the substitute were redacted.

[2198] See Hamdan v. Rumsfeld, 344 F. Supp. 2d 152, 168 (D.D.C. 2004) (describing potential procedures under military commissions established by Presidential order).

[2199] See Hamdan v. Rumsfeld, 548 U.S. 557, 634 (2006) (Stevens, J., plurality opinion) (stating that "an accused must, absent disruptive conduct or consent, be present for his trial and must be privy to the evidence against him").

[2200] See, e.g., id.; Crawford, 541 U.S. at 49, 124 S.Ct. 1354, 158 L.Ed.2d 177 (2004) ("It is a rule of the common law, founded on natural justice, that no man shall be prejudiced by evidence which he had not the liberty to cross examine") (internal citations omitted).

[2201] United States v. Abu Ali, 528 F.3d 210, 239-240 (4th Cir. 2008)(quoting Maryland v. Craig, 497 U.S. 836, 850 (1990)). In this case the defendant, while located in the Federal courthouse in Alexandria, Va., was able to communicate with his counsel in Riyadh via telephone during breaks in the deposition or upon the request of defense counsel.

these procedures satisfied the Confrontation Clause if "the denial of 'face-to-face confrontation' [was] 'necessary to further an important public policy,'" and sufficient procedural protections were in place to assure the reliability of the testimony.[2202] Here, the Fourth Circuit cited the protection of national security as satisfying the "important public policy" requirement. The cited procedural safeguards were the ability of the defendant and witness to mutually observe the other, the fact that testimony was given under oath in the Saudi criminal justice system, and the ability of defense counsel to cross examine the witnesses.[2203]

Arguments alleging that protective orders violate the Confrontation Clause because they do not allow the participation of the defendant may also be undercut in the classified information context because, in some cases, the excluded defendant is not believed to have knowledge of the information being presented.[2204] Therefore, his ability to provide his counsel with rebuttal information for cross examination purposes may be reduced. CIPA does not have any provisions which authorize the exclusion of defendants from any portion of trial based upon national security considerations. But, CIPA § 3 may authorize courts to issue protective orders preventing disclosure of classified information to the defendant by defense counsel.[2205]

Legislative Modification of the State Secrets Privilege

While CIPA may not appear to impose any limitations on the scope of the government's privilege against disclosing classified information, other pieces of legislation may affect the operation or coverage of the privilege. In 2008, a federal district court held that FISA supplanted the state secrets privilege with respect to civil claims of unlawful electronic surveillance. Two versions of the State Secrets Protection Act have also been introduced in the 111th Congress to codify and change aspects of the privilege in civil litigation. Each of these is discussed below.[2206]

[2202] Id. at 241-242 (citing Maryland v. Craig, 497 U.S. 836 (1990), in which one-way video testimony procedures were used in a prosecution for alleged child abuse).

[2203] Id. See, also, United States v. Bell, 464 F.2d 667 (2nd Cir. 1972) (holding that exclusion of the public and the defendant from proceedings in which testimony regarding a "hijacker profile" was presented was consistent with the Confrontation Clause).

[2204] Arguably, if the defendant is already aware of the information, the need to prevent disclosure to him is lessened.

[2205] See Brian Z. Tamanaha, A Critical Review of The Classified Information Procedures Act, 13 AM. J. CRIM. L. 277, 290, n.64, n.65 (1986).

[2206] Proposals like those in the Whistleblower Protection Enhancement Act, H.R. 1507 in the 111th Congress, that address the state secrets privilege in a more limited context are beyond the scope of this report.

The Foreign Intelligence Surveillance Act

FISA provides a statutory framework for government agencies to seek an order from the specialized Foreign Intelligence Surveillance Court (FISC) that authorizes the collection of foreign intelligence information via electronic surveillance[2207] or physical searches.[2208] FISA also provides procedures governing the use of pen registers and trap and trace devices,[2209] and access to certain business records for foreign intelligence collection.[2210]

FISA also provides a civil remedy for an "aggrieved person … who has been subjected to an electronic surveillance or about whom information obtained by electronic surveillance of such person has been disclosed or used" in violation of federal law.[2211] When evaluating the legality of a FISA order, the statute states that the court

> *shall, notwithstanding any other law, if the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States, review in camera and ex parte the application, order, and such other materials relating to the surveillance as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted. In making this determination, the court may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance only where such disclosure is necessary to make an accurate determination of the legality of the surveillance.*[2212]

The interaction between FISA and the state secrets privilege has been a central issue in some litigation regarding the Terrorist Surveillance Program instituted by the Bush Administration shortly after the terrorist attacks of September 11, 2001. In *In re National Security Agency Telecommunications Records Litigation*, plaintiffs sued federal officials for allegedly conducting unlawful

---

[2207] 50 U.S.C. §§ 1801-1808.

[2208] 50 U.S.C. §§ 1822-1826.

[2209] 50 U.S.C. §§ 1841-1846. Pen registers capture the numbers dialed on a telephone line; trap and trace devices identify the originating number of a call on a particular phone line. See 18 U.S.C. § 3127(3)-(4).

[2210] 50 U.S.C. §§ 1861-1862.

[2211] 50 U.S.C. § 1810.

[2212] 50 U.S.C. § 1806(f).

electronic surveillance of the plaintiffs.[2213] The plaintiffs sought discovery of records of the alleged electronic surveillance, portions of which had already been inadvertently disclosed to the plaintiffs by the government.[2214] The government attempted to prevent disclosure of these records by asserting the state secrets privilege and the Ninth Circuit, reviewing an interlocutory appeal, held that the records were initially protected by the state secrets privilege.[2215] However the Ninth Circuit remanded the case to the district court to address whether FISA superseded the state secrets privilege.[2216]

On remand, the Federal District Court for the Northern District of California held that the FISA procedures, which the court read as requiring judicial examination of the actual underlying information, superseded the judicially created state secrets privilege as it is described in *Reynolds*,[2217] but only if the plaintiffs could demonstrate that they had standing as "aggrieved persons" under FISA.[2218] In January of 2009, the court found that the plaintiffs had successfully met this burden using information that was not protected by the state secrets privilege.[2219]

The State Secrets Protection Act

H.R. 984 and S. 417, both entitled the State Secrets Protection Act, were introduced in the 111th Congress to codify the procedures and standards to be used in civil cases to evaluate a claim of the state secrets privilege by the government. Neither bill would address the operation of the state secrets privilege or CIPA in the context of criminal litigation. This section provides a general overview of the major changes proposed in each bill; a description of the individual provisions of each bill may be found in **Appendix B** and **Appendix C**, respectively.

Both bills would authorize the use of security measures provided under CIPA and provide all parties with a right of interlocutory appeal on any issue relating to the state secrets privilege. H.R. 984 would also impose a duty upon the Attorney General to report on cases in which the government had asserted the state secrets privilege to the congressional Intelligence Committees and the chairs and ranking

---

[2213] In re NSA Telecomms Records Litig., 564 F. Supp. 2d 1109, 1112 (N.D. Cal. 2008).

[2214] Id. at 1111.

[2215] Al-Haramain Islamic Found., Inc. v. Bush, 507 F.3d at 1204-1205.

[2216] Id. at 1206.

[2217] See, In re NSA Telecomms Records Litig., 564 F. Supp. 2d at 1119.

[2218] Id. at 1137. See also 50 U.S.C. § 1801(k) (defining "aggrieved persons" under FISA).

[2219] In re NSA Telcomms. Records Litig., 595 F. Supp. 2d 1077, 1086 (N.D. Cal. 2009).

members of the House and Senate Judiciary Committees. S. 417 would impose a similar duty, but would require reporting to the full membership of both committees and would also permit members of the respective committees to request access to the privileged information.

It would not be overstatement to say that both bills would impose more stringent judicial oversight of assertions of the state secrets privilege. Both bills would codify the common law requirement that the head of an agency formally assert the privilege after actual consideration by that officer, but would additionally require that official to provide an affidavit explaining the factual basis of the claim. The government would also be required to provide a public and unclassified version of this affidavit.

Both bills would also require a showing of "significant harm" before the privilege may apply.[2220] In contrast, courts applying Reynolds have generally not required that the harm to national security be "significant" in magnitude.[2221] Therefore, it is possible that both bills would require a higher threshold of harm to be demonstrated before the protection of the privilege could apply. It is also possible that some classified information would not be protected under either bill.[2222]

In a significant departure from the common law doctrine, both bills would require courts to examine the actual information for which the privilege is asserted to evaluate whether the claim of privilege is valid. This is in contrast to the procedures described under Reynolds, which do not automatically require courts to examine the underlying information in every case.

[2220] H.R. 984 limits the privilege to situations in which "public disclosure of the information ... would be reasonably likely to cause significant harm to the national defense or the diplomatic relations of the United States." Similarly, S. 417 defines a state secret as "any information that, if disclosed publicly, would be reasonably likely to cause significant harm to the national defense or foreign relations of the United States."

[2221] See Reynolds, 345 U.S. at 8 (requiring a risk of "injurious disclosure"); Ellsberg v. Mitchell, 709 F.2d 51, 59 (D.C. Cir. 1983) (upholding the privilege where "disclosure of the material would damage national security"); Molerio v. FBI, 749 F.2d 815, 822 (D.C. Cir. 1984) (upholding state secrets where disclosure of the secret "would impair national security"); Al-Haramain Islamic Foundation, Inc. v. Bush, 507 F..3d 1190, 1204 (9th Cir. 2007) (upholding privilege where disclosure "would undermine the government's intelligence capabilities and compromise national security"); Kasza v. Browner, 133 F.3d 1159, 1170 (9th Cir. 1998) (upholding privilege because "release of such information would reasonably endanger national security interests").

[2222] Pursuant to executive order, classified information falls into three levels: top secret, secret, and confidential. Confidential information, the lowest level, includes information that "could be expected to cause damage to the national security" if disclosed. Information may be classified as secret if there is a danger of "serious damage to the national security" of the United States. Information is top secret if exceptionally grave danger could occur. Exec. Order No. 12958, § 1.2(a) (as amended by Exec. Order No. 13292 (2003)).

Both bills would also authorize the court to order the government to provide alternative non-privileged substitutes for information that is found to be protected by the privilege in order to provide a private litigant with substantially the same opportunity to litigate the underlying issue of law or fact. A refusal by the government to provide a substitute could result in court imposed sanctions against the government.

Both bills appear intended to provide an alternative to the common law privileges described in both Reynolds and Totten. Although it has been argued that "any effort by Congress to regulate an exercise of the Executive's authority to protect national security through the state secrets privilege would plainly raise serious constitutional concerns,"[2223] at least one federal district court has recognized Congress's authority to enact legislation superseding the state secrets privilege.[2224]

S. 417, if enacted, would apply to all pending and future cases. H.R. 984 would similarly apply prospectively and would also have limited retroactive effect. Specifically, it would authorize federal courts to entertain timely motions to vacate final judgments that were based on the common law state secrets privilege and were entered after January 1, 2002, and involved claims against the federal government, or a government official in his official capacity.

This retroactivity provision may raise constitutional concerns. In *Plaut v. Spendthrift Farm*, the Supreme Court invalidated a legislative enactment that required federal courts to reopen final decisions as a violation of the separation of powers principle.[2225] It might be argued that the retroactivity provision in H.R. 984 also reopens final judgments in violation of the separation of powers principle. While a full analysis of this issue is beyond the scope of this report, it should be noted that the retroactivity provision of H.R. 984 may be distinguishable from the facts in *Plaut* for at least two reasons. First, unlike the statute in *Plaut*, H.R. 984 would not appear to compel courts to reopen such cases.[2226] Secondly, the Court found it important that *Plaut* reopened claims

---

[2223] Memorandum of Points and Authorities in Support of Defendants' Second Motion to Dismiss, Al-Haramain Islamic Foundation v. Bush, No. M:06-CV-1791 at 14 (Mar. 14, 2008) (arguing that the in camera procedures of FISA should not be read to supersede the state secrets privilege). See also Reynolds, 345 U.S. at n.9 (suggesting that the state secrets privilege is "an inherent executive power which is protected in the constitutional system of separation of power").

[2224] In re NSA Telecomms Records Litig., 564 F. Supp. 2d at 1119-20 (holding that FISA contains a clear expression of Congress's intent to abrogate the state secrets privilege).

[2225] Plaut v. Spendthrift Farm, 514 U.S. 211, 240 (1995) (invalidating statute that reopened final judgments in private civil actions under § 10(b) of the Securities Exchange Act of 1934).

[2226] H.R. 984, § 11 ("A court also may relieve a party ... from a final judgment, order, or proceeding") (emphasis added).

against private parties, while the retroactivity provisions in H.R. 984 would only be applicable to claims brought against the federal government.[2227]

Appendix A. Section-by-Section Summary of the Classified Information Procedures Act, 18 U.S.C. App. 3

Sec. 1. Provides definitions for both "classified information" and "national security" to be used in this act. Classified information means any information determined by the government pursuant to executive order, statute, or regulation to require protection for reasons of national security, and all data concerning (1) the design, manufacture, or utilization of atomic weapons; (2) the production of special nuclear material; or (3) the use of special nuclear material in the production of energy. National security means the national defense and foreign relations of the United States.

Sec. 2. Permits any party to request a pretrial conference to establish a schedule for discovery requests; the provision of notice if the defendant intends to disclose classified information; a hearing to determine the relevance, admissibility, and materiality of classified information; or any other matter which relates to classified information. No admission made by the defendant or his counsel at this pretrial conference may be used against the defendant unless it is made in writing and signed by the defendant and his counsel.

Sec. 3. Authorizes the court to issue protective orders prohibiting the further disclosure of any classified information disclosed to the defendant during the course of any federal criminal litigation.

Sec. 4. Authorizes the court to permit the government to redact classified information from discovery provided to the defendant. Alternatively the court may permit the government to summarize the classified information, or to admit relevant facts in lieu of providing discovery. The court may permit such procedures if the government submits a written statement explaining why the defendant is not entitled to the redacted information. The statement may be viewed by the court ex parte and in camera. If the government's request is granted, the written statement shall be preserved in the record, under seal, for appellate review.

Sec. 5. Imposes a continuing obligation on criminal defendants to notify, in writing and in a timely fashion, both the U.S. attorney and the court of their intent to disclose or cause the disclosure of classified information, along with a brief description of that information. The defendant may not disclose classified

---

[2227] See Id. at 230-1 (quoting U.S. v. Sioux Nation, 448 U.S. 371, 407) ("Congress' mere waiver of the res judicata effect of a prior judicial decision rejecting the validity of a legal claim against the United States does not violate the doctrine of separation of powers") (emphasis added).

information during litigation until notice has been provided, a hearing under this act has been held, and any interlocutory appeal has been heard.

Sec. 6. The government may request a hearing to determine the use, relevance, or admissibility of any classified information to be used at trial. This hearing may be conducted in camera if the Attorney General certifies that a public proceeding might result in disclosure of classified information. Before the hearing, the government may be required to give the defendant notice of what classified information is at issue and its relevancy to the charges against the defendant. If the court authorizes the disclosure of classified information, the government may request that a substitute for the information be used instead. After a hearing on the substitute, the court shall permit the substitute if it would give the defendant substantially the same ability to make his defense. This hearing may be held in camera at the request of the Attorney General, who may also submit an ex parte affidavit explaining the government's position. Disclosure of classified information may be prohibited if the Attorney General files an affidavit with the court objecting to disclosure. If the Attorney General files such an objection, the court may dismiss the indictment, find against the government on any pertinent issue, strike testimony, or take any other action as may be appropriate in the interests of justice.

Sec. 7. The government may take an interlocutory appeal from any order authorizing the disclosure of classified information, imposing sanctions for nondisclosure by the government, or refusing a protective order sought by the government. Appeals shall be expedited.

Sec. 8. Any material containing classified information may be admitted without changing the classification status of the information. The court may limit which parts of any material are admitted in order to prevent unnecessary disclosure of classified information, unless such limitations would be unfair. The government may object during any examination of a witness if classified information that has not yet been found admissible is likely to be elicited. The court will take whatever action is necessary to determine whether the response is admissible.

Sec. 9. Directs the Chief Justice of the United States, in consultation with the Attorney General, the Director of National Intelligence, and the Secretary of Defense, to establish procedures to protect classified information in the custody of federal courts.

Sec. 9A. Directs Department of Justice officials to provide briefings to senior officials of any other agency with respect to cases involving classified information that originated in that agency.

Sec. 10. In prosecutions where the government must prove that some material relates to the national security of the United States, such as prosecutions for espionage, the prosecution is required to notify the defendant of the portions of the material it will rely upon.

Sec. 11. Permits §§ 1-10 of this act to be amended pursuant to 28 U.S.C. § 2076. That provision described procedures to amend the Federal Rules of Evidence, but has since been repealed. Similar procedures for amending the Federal Rules of Evidence may now be found at 28 U.S.C. § 2072. It is not clear what effect the repeal of 28 U.S.C. § 2076 has had on this provision of CIPA.

Sec. 12. Directs the Attorney General to issue guidelines specifying the factors that should be used by the Department of Justice in determining whether to prosecute cases in which there is a risk of disclosing classified information. When a decision not to prosecute is made pursuant to these guidelines, an official of the Department of Justice shall prepare written findings regarding the intelligence information that would be endangered, the purpose for which it might be disclosed, the likelihood that it would be disclosed, and the potential consequences of such disclosure on the national security of the United States.

Sec. 13. Requires the Attorney General to report to Congress, on a semiannual basis, about all cases which were not prosecuted pursuant to the guidelines issued by the Attorney General under this act. The report shall be given to both the House and Senate Intelligence Committees and to the chair and ranking member of the respective Judiciary Committees. The Attorney General is also directed to report on the operation and effectiveness of the act and on any suggested amendments as necessary.

Sec. 14. Authorizes the Attorney General to delegate authority under this act to the Deputy Attorney General, the Associate Attorney General, or an Assistant Attorney General.

Sec. 15. Provides that this act became effective immediately upon enactment.

Sec. 16. Provides the short title for this act, the "Classified Information Procedures Act."

Appendix B. Section-by-Section Summary of H.R.984

Sec. 1. This act would be referred to as the State Secret Protection Act of 2009.

Sec. 2. The government would have a statutorily recognized privilege against providing information in civil litigation if public disclosure of that information would be reasonably likely to cause significant harm to the national defense or foreign relations of the United States.

Sec. 3. Courts would be directed to take steps to protect sensitive information. Courts would be authorized to use security mechanisms to protect against inadvertent disclosure, including those procedures developed under CIPA. All hearings and proceedings could be conducted in camera, as necessary, and participation of counsel would not be restricted unless the court determined it

was necessary. Such restrictions can not be more restrictive than necessary and the court would provide a written explanation of its decision to all parties. During the court's evaluation of the privilege, the court could order the government to provide a substitute of the underlying information, if feasible, in order to provide counsel with a substantially equivalent opportunity to challenge the claim.

Sec. 4. The head of the agency with control over the evidence would be required to formally assert the state secrets privilege. Additionally, the government would be required to provide classified and unclassified affidavits explaining the factual basis of the claim.

Sec. 5. Additional preliminary procedures could be used in cases involving the state secrets privilege. These procedures would permit the court to issue protective orders upon government request, to appoint a special master or expert witness, to order the government to provide a manageable index of the underlying information, to hold prehearing conferences to address administrative matters, and to order counsel to obtain security clearances.

Sec. 6. Courts would be required to actually examine the underlying information about which the privilege was asserted in addition to any other information necessary to evaluate whether the claim of privilege was valid. Where the amount of information is so great that it cannot be reviewed in a timely fashion, the court may base its determination on a sampling of the information. The court would be directed to weigh testimony from government experts in the same manner as it does other expert testimony.

Sec. 7. Where the information is found to be protected by the privilege, the court would be authorized to order the government to provide a non-privileged substitute, if feasible. Refusals to provide a substitute could result in sanctions against the government in civil actions brought against the government. A valid privilege would not result in dismissal or summary judgment until all parties have had an opportunity to complete non-privileged discovery. Where privileged information, that cannot be replaced with a non-privileged substitute, is central to a question of fact or law, the court would be authorized to take appropriate action including striking testimony, finding in favor of a party, or dismissing the claim.

Sec. 8. Interlocutory appeals could be taken by any party, and would be heard in an expedited fashion. Trials shall be adjourned during the pendency of an interlocutory appeal and the appellate court may dispense with written briefs or a written opinion.

Sec. 9. The Attorney General would be required to report, within 30 days, on any case in which the government invokes the state secrets privilege. This report would be given to the congressional Intelligence Committees and the chair and ranking member of the Judiciary Committees. The Attorney General would also be required to report on the operation and effectiveness of this act, and suggest

amendments. This report would be issued annually for three years, and then only as necessary.

Sec. 10. The privilege in this act would be identified as the only privilege that may be asserted in civil cases based on state secrets. The procedures of the act would apply to any invocation of the state secrets privilege.

Sec. 11. This act would apply to claims pending on or after the date of enactment. It would also purport to authorize courts to vacate final judgments that were based on the state secrets privilege, if a motion for relief from a final judgment is filed within one year of the date of enactment, the final judgment was entered after January 1, 2002, and the claim was made against the government or arose out of conduct by persons acting in the capacity of a government officer, employee, or agent.

Appendix C. Section-by-Section Summary of S. 417

Sec. 1. This act would be referred to as the State Secrets Protection Act of 2009.

Sec. 2. Title 28 of the U.S. Code would be amended to provide a new Chapter 181 with the following new sections:

- Sec. 4051. Evidence, as used in this chapter, would include anything admissible under the Federal Rules of Evidence or discoverable under the Federal Rules of Civil Procedure. A state secret would be defined as any information, the public disclosure of which, would be reasonably likely to cause significant harm to the national defense or foreign relations of the United States.
- Sec. 4052. Federal courts would be authorized to determine which documents should be submitted ex parte and whether substitutions or redactions should be provided, after weighing the interests of justice and national security. Hearings would be conducted in camera unless they relate solely to a question of law. Hearings could be held ex parte if protective orders and security clearances are insufficient to protect the interests of justice and national security. Courts could limit attendance in hearings to individuals with security clearances and could appropriate a guardian ad litum with a security clearance to represent any party. The court could stay proceedings while security clearances are being obtained. The court could review in camera and ex parte the government's reasons for denying or delaying the issuance of a security clearance. Orders and opinions could be issued under seal. The court could also appoint a special master with the necessary security clearance to assist the court.
- Sec. 4053. The government would be permitted to intervene in any civil action to protect against disclosure of information that may be subject to the state secrets privilege. A civil action could not be dismissed based solely upon a claim of state secrets until after all hearings required by this act have taken place. The government may assert the privilege in response to any allegation in a complaint or counterclaim, regardless of whether the

action is against the government or a private party. The government would be required to formally assert the privilege through the submission of an affidavit by the head of the agency with responsibility for, and control over, the information. The affidavit would explain the factual basis for the claim of privilege. This duty would not be delegable by the head of an agency

- Sec. 4054. The government could assert the privilege at any time during a civil action to prevent the disclosure of information contained in court filings or evidence. A formal assertion of the privilege would be required, made by an affidavit issued by the appropriate agency head. The government would be required to make an unclassified version of the affidavit public. A court would be required to conduct a hearing to examine the underlying information and any affidavits submitted in support of the privilege in order to determine the validity of the claim of privilege. The government would be required to provide the court with all information to which the privilege is claimed to apply before the hearing. The court could base its conclusion on a sampling of the information where the volume of information is too large to be reviewed in a timely fashion. The government would be required to provide the court with an index of all the information it claims is subject to the privilege. A piece of information would be privileged if it contains a state secret or cannot be effectively segregated from other evidence that contains a state secret. Privileged evidence would not be admitted or disclosed. Non-privileged evidence would be subject to the Federal Rules of Evidence and the Federal Rules of Civil Procedure. The court would be required to give substantial weight to assertions by the government as to why a public disclosure would be harmful to national security. Testimony by government experts would be treated the same as testimony by other experts. The court could order the government to provide a non-privileged substitute in lieu of evidence found to be privileged, if it would give a party a substantially equivalent opportunity to litigate the issue. In suits against the government or an officer or agent of the government, the court would be required to find against the government on any issue where the government was ordered, but refused, to provide a non-privileged substitute.
- Sec. 4055. A federal court could dismiss an action as a result of the state secrets privilege, only if a non-privileged substitute is not possible, dismissal of the claim or counterclaim would not harm national security, and continuing the litigation without the privileged information would substantially impair a valid defense to the action.
- Sec. 4056. Interlocutory appeals could be taken by any party, and would be heard in an expedited fashion. Trials shall be adjourned during the pendency of an interlocutory appeal and the appellate court may dispense with written briefs or a written opinion.
- Sec. 4057. The security procedures created under CIPA would be used to protect against unauthorized disclosure of evidence determined to be privileged. The Chief Justice of the United States, in consultation with the

Attorney General, the Director of National Intelligence, and the Secretary of Defense, may amend the rules to implement this chapter. Any amendments would be submitted to the Intelligence and Judiciary Committees of the House of Representatives and the Senate. Such amendments would become effective 90 days after submission to Congress, unless Congress provides otherwise.

- Sec. 4058. The Attorney General would be required to report, within 30 days, on any case in which the government invokes the state secrets privilege. This report would be given to the Intelligence and Judiciary Committees. The Attorney General would be required to produce evidence for which the privilege was asserted upon request by a member of the Intelligence or Judiciary Committees. The Attorney General would also be required to report on the operation and effectiveness of this act, and suggest amendments. These report would be issued annually for three years, and then only as necessary.
- Sec. 4059. No other limit on the state secrets privilege under any other provision of law would be superseded by this act. No court would be prohibited from dismissing a claim or counterclaim on grounds unrelated to the state secrets privilege.

Sec. 3. Any provision of this act that is found to be invalid would be severable from the other provisions of this act.

Sec. 4. This act would apply to cases pending on or after the date of enactment.

18 U.S.C. CHAPTER 113C: TORTURE (18 U.S.C. §§ 2340-2340B)

Extraordinary Rendition

Renditions: Constraints Imposed by Laws on Torture, RL32890 (September 8, 2009).

MICHAEL JOHN GARCIA, CONGRESSIONAL RESEARCH SERV., RENDITIONS: CONSTRAINTS IMPOSED BY LAWS ON TORTURE (2009), *available at* http://www.intelligencelaw.com/library/secondary/crs/pdf/RL32890_9-8-2009.pdf.

Michael John Garcia
Legislative Attorney
mgarcia@crs.loc.gov, 7-3873

September 8, 2009

Congressional Research Service

7-5700
www.crs.gov
RL32890

Summary

Persons suspected of criminal or terrorist activity may be transferred from one State (i.e., country) to another for arrest, detention, and/or interrogation. Commonly, this is done through extradition, by which one State surrenders a person within its jurisdiction to a requesting State via a formal legal process, typically established by treaty. Far less often, such transfers are effectuated through a process known as "extraordinary rendition" or "irregular rendition." These terms have often been used to refer to the extrajudicial transfer of a person from one State to another. In this report, "rendition" refers to extraordinary or irregular renditions unless otherwise specified.

Although the particularities regarding the usage of extraordinary renditions and the legal authority behind such renditions are not publicly available, various U.S.

officials have acknowledged the practice's existence. During the Bush Administration, there was controversy over the use of renditions by the United States, particularly with regard to the alleged transfer of suspected terrorists to countries known to employ harsh interrogation techniques that may rise to the level of torture, purportedly with the knowledge or acquiescence of the United States. In January 2009, President Obama issued an Executive Order creating a special task force to review U.S. transfer policies, including the practice of rendition, to ensure compliance with applicable legal requirements. In August, the task force issued recommendations to ensure that U.S. transfer practices comply with applicable standards and do not result in the transfer of persons to face torture. These recommendations include strengthening procedures used to obtain assurances from a country that a person will not face torture if transferred there, and the establishment of mechanisms to monitor the treatment of transferred persons.

This report discusses relevant international and domestic law restricting the transfer of persons to foreign states for the purpose of torture. The U.N. Convention against Torture and Other Cruel, Inhuman, or Degrading Treatment or Punishment (CAT), and its domestic implementing legislation (the Foreign Affairs Reform and Restructuring Act of 1998) impose the primary legal restrictions on the transfer of persons to countries where they would face torture. Both CAT and U.S. implementing legislation generally prohibit the rendition of persons to countries in most cases where they would more likely than not be tortured, though there are arguably limited exceptions to this prohibition. Historically, the State Department has taken the position that CAT's provisions concerning the transfer of persons do not apply extraterritorially, though as a matter of policy the United States does not transfer persons in its custody to countries where they would face torture (U.S. regulations and statutes implementing CAT, however, arguably limit the extraterritorial transfer of individuals nonetheless). Under U.S. regulations implementing CAT, a person may be transferred to a country that provides credible assurances that the rendered person will not be tortured. Neither CAT nor its implementing legislation prohibit the rendition of persons to countries where they would be subject to harsh treatment not rising to the level of torture. Besides CAT, additional obligations may be imposed upon U.S. rendition practice via the Geneva Conventions, the War Crimes Act (as amended by the Military Commissions Act (P.L. 109-366), the International Covenant on Civil and Political Rights (ICCPR), and the Universal Declaration on Human Rights.

Legislation was introduced in the 110th Congress to limit or bar U.S. participation in renditions. It is possible that similar legislation will be proposed in the 111th Congress.

Introduction

Persons suspected of terrorist or criminal activity may be transferred from one State (i.e., country) to another to answer charges against them.[2228] The surrender of a fugitive from one State to another is generally referred to as *rendition*.[2229] A distinct form of rendition is *extradition*, by which one State surrenders a person within its territorial jurisdiction to a requesting State via a formal legal process, typically established by treaty between the countries.[2230] However, renditions may be effectuated in the absence of extradition treaties, as well.[2231] The terms "irregular rendition" and "extraordinary rendition" have been used to refer to the *extrajudicial* transfer of a person from one State to another, generally for the purpose of arrest, detention, and/or interrogation by the receiving State (for purposes of this report, the term "rendition" will be used to describe irregular renditions, and not extraditions, unless otherwise specified). Unlike in extradition cases, persons subject to this type of rendition typically have no access to the judicial system of the sending State by which they may challenge their transfer.[2232] Sometimes persons are rendered from the territory of the

---

[2228] The surrender of persons to a requesting State to answer criminal charges was originally guided by principles of comity and reciprocity. Beginning in the late eighteenth century, the surrender of persons to a requesting State to answer charges increasingly became governed by formal extradition treaties between States (though the practice of extradition can be traced back to antiquity). For background, see CRS Report 98-958, Extradition To and From the United States: Overview of the Law and Recent Treaties, by Charles Doyle. In contrast to earlier practices, extradition treaties established formal procedures governing the surrender of persons from one treaty party to another, facilitating treaty parties' shared interest in punishing certain crimes while providing persons with a legal means to challenge their proposed transfer to a requesting State. By the 20th century, extradition treaties became the predominant means of permitting the transfer of persons from one State to another to answer charges against them. For background, see id. at 1-3; M. BASSIOUNI, INTERNATIONAL EXTRADITION: UNITED STATES LAW AND PRACTICE (4th ed. 2002).

[2229] BLACK'S LAW DICTIONARY 1298-99 (7th ed. 1999).

[2230] U.S. extradition procedures for transferring a person to another State are governed by the relevant treaty with that State, as supplemented by 18 U.S.C. §§ 3181-3196. U.S. law generally prohibits the extradition of individuals from the United States in the absence of a treaty. 18 U.S.C. § 3181.

[2231] For example, via statutory authorization, the U.S. may in the exercise of comity surrender a person to a foreign country to face criminal charges for committing a crime of violence against a U.S. national, if the offense is nonpolitical in nature and the person is not a U.S. citizen, national, or permanent resident. 18 U.S.C. § 3181(b). Courts have also recognized that an extradition may be effectuated pursuant to a statute rather than a treaty. See Ntakirutimana v. Reno, 184 F.3d 419 (5th Cir. 1999) (upholding surrender of Rwandan citizen to international tribunal, when surrender was authorized via executive agreement and implementing statute rather than treaty).

[2232] Before the United States may extradite a person to another State, an extradition hearing must be held before an authorized judge or magistrate, during which the judge or magistrate must determine whether the person's extradition would comply with the terms of the extradition treaty between the United States and the requesting State. Even if the magistrate or authorized judge

rendering State itself, while other times they are seized by the rendering State in another country and immediately rendered, without ever setting foot in the territory of the rendering State.[2233] Sometimes renditions occur with the consent of the State where the fugitive is located;[2234] other times, they do not.[2235]

---

finds extradition to be appropriate, a fugitive can still institute habeas corpus proceedings to obtain release from custody and thereby prevent his extradition, or the Secretary of State may decide not to authorize the extradition. See CRS Report 98-958, supra footnote 1. These protections do not apply in situations where an alien is being removed from the United States for immigration purposes. Nevertheless, separate procedural and humanitarian relief protections do pertain.

[2233] In 2005, Khaled El-Masri, a German citizen of Lebanese descent, filed suit against a former CIA director and other persons for their involvement in his alleged rendition from Macedonia to a detention center in Afghanistan, where he was subjected to harsh interrogation for several months on account of suspected terrorist activities. El-Masri claimed that after the CIA discovered that its suspicions of El-Masri were mistaken, it released him in Albania. Don Van Natta Jr.& Souad Mekhennet, "German's Claim of Kidnapping Brings Investigation of U.S. Link," New York Times, January 9, 2005, at 11. The federal district court dismissed El-Masri's claim without evaluating its merits, finding that the claim could not be fairly litigated without disclosure of sensitive information protected by the state secrets privilege. El-Masri v. Tenet, 437 F.Supp.2d 530 (E.D.Va. 2006). The district court's ruling was affirmed by the Fourth Circuit Court of Appeals in 2007, and the Supreme Court subsequently denied plaintiff's petition for writ of certiorari. El-Masri v. United States, 479 F.3d 296 (4th Cir. 2007), cert. denied, 128 S.Ct. 373 (2008). In 2007, German public prosecutors issued arrest warrants for 13 CIA agents who were allegedly involved in El-Masri's rendition, but the Justice Ministry declined to request the agents' extradition from the United States. "Renditions Victim to Sue German Government," Spiegel Online, June 9, 2008, at http://www.spiegel.de/international/germany/0,1518,558496,00.html.

[2234] In some instances, questions as to whether a State has consented to the rendition of a person located in its territory have been subject to controversy and investigation. In Italy, the trial of several Italian intelligence officers and 26 American intelligence operatives (being tried in absentia) for the rendition of an Islamic cleric from Italy to Egypt was suspended after the Italian government said testimony could reveal state secrets threatening Italy's national security. "CIA-Linked Kidnapping Trial on Hold," Chicago Tribune, December 4, 2008, at 22. The trial was subsequently permitted to proceed, but without reference to top secret information. In late 2006, a committee established by the European Parliament (the parliamentary body of the European Union) to investigate European governments' participation in renditions by the CIA found evidence indicating the involvement of European State agents or officials in a number of investigated renditions. Temporary Committee on the Alleged Use of European Countries by the CIA for the Transport and Illegal Detention of Prisoners, Eur. Parl., Working Doc. 7, November 16, 2006, available at http://www.europarl.europa.eu/comparl/tempcom/tdip/working_docs/pe380593_en.pdf at 2. The final report by the committee was issued in January 2007. Temporary Committee on the Alleged Use of European Countries by the CIA for the Transport and Illegal Detention of Prisoners, Eur. Parl., Final Report, January 30, 2007, available at http://www.europarl.europa.eu/comparl/tempcom/tdip/final_report_en.pdf. For additional background, see CRS Report RL33643, Undisclosed U.S. Detention Sites Overseas: Background and Legal Issues, by Jennifer K. Elsea and Julie Kim.

[2235] In 1980, the Department of Justice's Office of Legal Counsel issued an opinion that irregular renditions absent the consent of the State where the fugitives are seized would violate customary international law because they would be an invasion of sovereignty for one country to carry out law enforcement activities in another without that country's consent. Extraterritorial

Besides irregular rendition and extradition, aliens present or attempting to enter the United States may be removed to another State under U.S. immigration laws, if such aliens are either deportable or inadmissible and their removal complies with relevant statutory provisions.[2236] Unlike in the case of rendition and extradition, the legal justification for removing an alien from the United States via deportation or denial of entry is not so that he can answer charges against him in the receiving State; rather, it is because the United States possesses the sovereign authority to determine which non-nationals may enter or remain within its borders, and the alien fails to fulfill the legal criteria allowing non-citizens to enter, remain in, or pass in transit through the United States. Although the deportation or exclusion of an alien under immigration laws may have the same practical effect as an irregular rendition (especially if the alien is subject to "expedited removal" under § 235 of the Immigration and Nationality Act, in which case judicial review of a removal order may be very limited), this practice is arguably distinct from the historical understanding of what constitutes a rendition.[2237] Nonetheless, the term "extraordinary rendition" has occasionally been used by some commentators to describe the transfer of aliens suspected of terrorist activity to third countries for the purposes of detention and interrogation, even though the transfer was conducted pursuant to immigration procedures.[2238]

Apprehension by the Federal Bureau of Investigation, 4B. OP. OFF. LEGAL COUNSEL 543 (1980). Additionally, Article 2(4) of the U.N. Charter prohibits Member States from violating the sovereignty of another State. In 1989, the Office of Legal Counsel constrained the 1980 opinion, though not on the grounds that such renditions are consistent with customary international law. Authority of the Federal Bureau of Investigation to Override International Law in Extraterritorial Law Activities, 13 OP. OFF. LEGAL COUNSEL 163 (1989) (finding that extraterritorial law enforcement activities authorized by domestic law are not barred even if they contravene unexecuted treaties or treaty provisions, such as Article 2(4) of the United Nations Charter, as well as customary international law). Further, while upholding court jurisdiction over a Mexican national brought to the United States via rendition, despite opposition from the Mexican government, the Supreme Court nevertheless noted that such renditions were potentially "a violation of general international law principles." United States v. Alvarez-Machain, 505 U.S. 655, 669 (1992). In a related case twelve years later, however, the Court held that any such principle—at least as it related to the rights of the rendered individual—did not "rest on a norm of international character accepted by the civilized world and defined with a specificity comparable to the features of the 18th century paradigms." Sosa v. Alvarez-Machain, 124 S.Ct. 2739, 2761-62 (2004).

[2236] See, e.g., 8 U.S.C. §§ 1182 (providing grounds for alien inadmissibility into the United States), 1227 (describing classes of deportable aliens), 1251 (providing guidelines for removal of deportable and inadmissible aliens).

[2237] See BASSIOUNI, supra footnote 1, at 183-248 (discussing deportation and exclusion as an alternative to extradition).

[2238] Perhaps the most notable case of alleged rendition involved Maher Arar, a dual citizen of Canada and Syria. Mr. Arar filed suit in January 2004 against certain U.S. officials that he claims were responsible for rendering him to Syria, where he was allegedly tortured and interrogated for

Over the years, several persons have been rendered into the United States by U.S. authorities, often with the cooperation of the States where such persons were seized, to answer criminal charges, including charges related to terrorist activity.[2239] The Obama Administration has continued this practice.[2240] Besides receiving persons through rendition, the United States has also rendered persons to other countries over the years, via the Central Intelligence Agency (CIA) and various law enforcement agencies.[2241]

---

suspected terrorist activities with the acquiescence of the United States. Arar was allegedly first detained by U.S. officials while waiting in New York's John F. Kennedy International Airport for a connecting flight to Canada after previously flying from Tunisia. According to U.S. officials, Mr. Arar's removal to Syria was done pursuant to § 235(c) of the Immigration and Nationality Act, which authorizes the "expedited removal" of arriving aliens suspected of terrorist activity. U.S. Department of State, U.S. Views Concerning Syrian Release of Mr. Maher Arar, October 6, 2003, available at http://2001-2009.state.gov/r/pa/prs/ps/2003/24965.htm; see also 8 U.S.C. § 1225(c). On February 16, 2006, the U.S. District Court for the Eastern District of New York dismissed Arar's civil case on a number of grounds, including that certain claims raised against U.S. officials implicated national security and foreign policy considerations, and assessing the propriety of those considerations was most appropriately reserved to Congress and the executive branch. Arar v. Ashcroft, 414 F.Supp.2d 250 (E.D.N.Y. 2006). The district court's dismissal was upheld by a three-judge panel of the Court of Appeals for the Second Circuit on June 30, 2008. Arar v. Ashcroft, 532 F.3d 157 (2nd Cir. 2008). A rehearing en banc was granted on August 12, 2008, but a ruling has yet to be issued. The Canadian government established a commission to investigate Canada's involvement in Arar's arrest and transfer to Syria. The final report of the Arar Commission, released in September 2006, concluded that Arar had not been a security threat to Canada, but Canadian officials provided U.S. authorities with inaccurate information regarding Arar that may have led to his transfer to Syria. Arar Commission, Factual Inquiry, at http://www.ararcommission.ca/eng/26.htm. See also, Department of Homeland Security, OIG-0818, Office of Inspector General, The Removal of a Canadian Citizen to Syria (Unclassified Summary), March 2008.

[2239] See generally State Department, Office of the Coordinator of Counterterrorism, Patterns of Global Terrorism, Appendix D: Extraditions and Renditions of Terrorists to the United States, 1993-2001 (May 21, 2002), available at http://www.state.gov/documents/organization/10306.pdf. See also State Department, Bureau for International Narcotics and Law Enforcement Affairs International Narcotics Control Strategy Report, 2005: Southeast Asia (March 2005), available at http://www.state.gov/p/inl/rls/nrcrpt/2005/vol1/html/42367.htm (mentioning Vietnam and Cambodia as countries that have permitted the rendition of persons to the United States to answer drug charges).

[2240] In August 2009, a Lebanese citizen was seized by FBI agents in Afghanistan and rendered to the United States to face charges for bribery. The rendition was committed with the consent of the Afghan government. Bob Drogin, "Lebanese Man Is Target of First Rendition under Obama," L.A. Times, August 22, 2009.

[2241] For a historical discussion of U.S. policy and practice regarding rendition, see William G. Weaver & Robert M. Pallitto, "The Law: 'Extraordinary Rendition' and Presidential Fiat, 36 PRESIDENTIAL STUD. Q. 102 (2006).

There have been no widely-reported cases of persons being rendered from the interior of the United States, perhaps due to the constitutional and statutory limitations upon the summary transfer of persons from U.S. territory.[2242] There have been cases where non-U.S. citizens were allegedly "rendered" at U.S. ports of entry but had yet to legally enter/be admitted into the United States. However, these "renditions" appear to have been conducted pursuant to immigration removal procedures.[2243] Noncitizens arriving at ports of entry have no recognized constitutional rights with regard to their admission into the United States,[2244] and federal immigration law provides arriving aliens with fewer procedural protections against their removal than aliens residing in the United States.[2245]

Instead, it appears that renditions by the U.S. to third countries have involved non-citizens seized outside U.S. territory. The Supreme Court has found that the Constitution protects U.S. citizens abroad from actions taken against them by the federal government,[2246] and this would generally appear to limit the summary transfer of such persons to the custody of foreign governments.[2247] In contrast,

---

[2242] See,e.g., 18 U.S.C. § 3181 (generally prohibiting extradition of U.S. citizens and legal permanent residents in the absence of a treaty); Valentine v. United States ex rel. Neidecker, 299 U.S. 5 (1936) (holding that Executive may not extradite U.S. citizens unless granted legal authority to do so); Yamata v. Fischer, 189 U.S. 86, 100-101 (deportation proceedings must reflect procedural due process requirements).

[2243] See supra footnote 11.

[2244] See, e.g., United States ex rel. Knauff v. Shaughnessy, 338 U.S. 537, 542, (1950) ("At the outset we wish to point out that an alien who seeks admission to this country may not do so under any claim of right."); Nishimura Ekiu v. United States, 142 U.S. 651, 659-660 (1892) ("It is an accepted maxim of international law that every sovereign nation has the power, as inherent in sovereignty, and essential to self-preservation, to forbid the entrance of foreigners within its dominions, or to admit them only in such cases and upon such conditions as it may see fit to prescribe.").

[2245] Arriving aliens who are deemed inadmissible may be subject to "expedited removal," a more streamlined removal process than that applicable to aliens who have been admitted into the United States. 8 U.S.C. § 1225.

[2246] See, e.g., Reid v. Covert, 354 U.S. 1, 6 (1957) ("When the Government reaches out to punish a citizen who is abroad, the shield which the Bill of Rights and other parts of the Constitution provide to protect his life and liberty should not be stripped away just because he happens to be in another land.").

[2247] See Valentine, 299 U.S. at 9 (1936) (stating that there is "no executive prerogative to dispose of the liberty of the individual ... There is no executive discretion to surrender him to a foreign government, unless that discretion is granted by law."). In limited circumstances, the involuntary transfer of a U.S. citizen to a foreign government may occur in the absence of an authorizing statute or treaty, in cases "involving the transfer to a sovereign's authority of an individual captured and already detained [by the U.S.] in that sovereign's territory." Munaf v. Geren, 553 U.S. __, 128 S.Ct. 2207, 2227 (2008), In Munaf, the Supreme Court found that while the federal habeas corpus statute gives U.S. courts jurisdiction over petitions filed on behalf of U.S. citizens

noncitizens who have not entered the United States have historically been recognized as receiving few, if any, constitutional protections[2248] (though noncitizens in foreign territory under the de facto control of the United States, such as Guantanamo Bay, Cuba, may be owed greater protections than other noncitizens abroad).[2249]

Reportedly, the rendition of terrorist suspects to other countries was authorized by President Ronald Reagan in 1986 and has been part of U.S. counterterrorism efforts at least since the late 1990s.[2250] In testimony before the House Foreign Affairs Committee in April 2007, former CIA official Michael F. Scheuer claimed authorship of the CIA's rendition program and stated that it originally began in mid-1995. The initial goals of the rendition program, according to Scheuer, were to ensure the detention of Al Qaeda members posing a threat to U.S. security and to seize any documents in their possession.[2251] However,

> *[a]fter 9/11, and under President Bush, rendered al-Qaeda operatives have most often been kept in U.S. custody. The goals of the program remained the same, although … Mr. Bush's national*

---

held by U.S. authorities in foreign territory, courts may not exercise habeas jurisdiction to enjoin the surrender of such persons to the foreign territory's sovereign for criminal prosecution.

[2248] See, e.g., Verdugo-Urquidez v. United States, 494 U.S. 259, 270-71 (1990) ("aliens receive constitutional protections when they have come within the territory of the United States and developed substantial connections with the country").

[2249] In the 2008 case of Boumediene v. Bush, 553 U.S. ___, 128 S.Ct. 2229, the Supreme Court held that the constitutional writ of habeas corpus extended to non-citizen detainees held at Guantanamo, in significant part because Guantanamo, while not technically part of the United States, was nonetheless subject to its complete control. The Court's opinion did not address the extent to which other constitutional protections extended to Guantanamo detainees, and it suggested that noncitizens held by the United States in foreign territories where U.S. control was less absolute than Guantanamo would be afforded lesser protections. See id. at 2262 (noting that the Court had never before found that the noncitizens detained in another country's territory have any rights under the U.S. Constitution, but concluding that the case before it "lack[ed] any precise historical parallel"). Notably, the Court did not overrule its decision in Johnson v. Eisentrager, 339 U.S. 763 (1950), where it held that the constitutional writ of habeas did not extend to enemy aliens held in postwar Germany. Instead, the Court distinguished the two cases, and noted that unlike the petitioners in Eisentrager, the Guantanamo detainees denied they were enemy combatants and the government's control over post-WWII German territory was not nearly as complete as its control over Guantanamo. Boumediene, 128 S. Ct. at 2259-2260.

[2250] See Dana Priest, "CIA's Assurances On Transferred Suspects Doubted," Washington Post, March 17, 2005, p. A1.

[2251] Statement of Michael F. Scheuer, Former Chief, Bin Laden Unit, Central Intelligence Agency, House For. Affairs Comm. (April 17, 2007), Hearing, Extraordinary Rendition in U.S. Counterterrorism Policy: The Impact on Transatlantic Relations, available at http://foreignaffairs.house.gov/110/sch041707.htm.

security team wanted to use U.S. officers to interrogate captured al-Qaeda fighters.[2252]

In a 2002 written statement to the Joint Committee Inquiry into Terrorist Attacks Against the United States, then-CIA Director George Tenet reported that even prior to the 9/11 terrorist attacks, the "CIA (in many cases with the FBI) had rendered 70 terrorists to justice around the world."[2253] The *New York Times* has reported that following the 9/11 attacks, President Bush issued a still-classified directive that broadened the CIA's authority to render terrorist suspects to other States.[2254] Although there are some reported estimates that the United States has rendered more than 100 individuals following 9/11,[2255] the actual number is not a matter of the public record.

Controversy has arisen over the United States allegedly rendering suspected terrorists to States known to practice torture for the purpose of arrest, detention, and/or harsh interrogation.[2256] Critics charge that the United States has rendered persons to such States so that they will be subjected to harsh interrogation techniques prohibited in the United States, including torture. The Bush Administration did not dispute charges that U.S. authorities rendered persons to foreign States believed to practice torture, but denied rendering persons for the purpose of torture.[2257] Answering a question regarding renditions in a March 16, 2005 press conference, President Bush stated that prior to transferring persons to other States, the United States received "promise[s] that they won't be tortured ... This country does not believe in torture."[2258] In testimony before the Senate

---

[2252] Id.

[2253] Statement of Director of Central Intelligence George Tenet, Joint Committee Inquiry into Terrorist Attacks Against the United States (October 17, 2002), available online at. https://www.cia.gov/news-information/speeches-testimony/ 2002/dci_testimony_10172002.html.

[2254] Douglas Jehl and David Johnston, "Rule Change Lets CIA Freely Send Suspects Abroad to Jails," N.Y. Times, March 6, 2005.

[2255] See Priest, supra footnote 23.

[2256] See generally Jane Mayer, "Outsourcing Torture," New Yorker, February 14, 2005, p. 106.

[2257] See, e.g., R. Jeffrey Smith, "Gonzales Defends Transfer of Detainees," Washington Post, March 8, 2005, p. A3 (quoting Attorney General Gonzales as stating that it is not U.S. policy to send persons "to countries where we believe or we know that they're going to be tortured").

[2258] White House, Office of the Press Secretary, President's Press Conference, March 16, 2005, available at http://georgewbush-whitehouse.archives.gov/news/releases/2005/03/20050316-3.html. This position was reiterated by President Bush in another press conference the following month. White House, Office of the Press Secretary, President's Press Conference, April 28, 2005, available at http://georgewbush-whitehouse.archives.gov/news/releases/ 2005/04/20050428-

Armed Services Committee in 2005, acting CIA Director Porter Goss stated that in his belief, "we have more safeguards and more oversight in place [over renditions] than we did before" 9/11.[2259] Secretary of State Condoleezza Rice stated that "the United States has not transported anyone, and will not transport anyone, to a country when we believe he will be tortured. Where appropriate, the United States seeks assurances that transferred persons will not be tortured."[2260]

In January 2009, President Obama issued an Executive Order creating a special task force to review U.S. transfer policies, including the practice of rendition, to ensure compliance with applicable legal requirements. In August, the task force issued recommendations to ensure that

U.S. transfer practices comply with applicable standards and do not result in the transfer of persons to face torture. These recommendations include strengthening procedures used to obtain assurances from a country that a person will not face torture if transferred there, including through the establishment of mechanisms to monitor the treatment of transferred persons. Little publicly available information from government sources exists regarding the nature and frequency of U.S. renditions to countries believed to practice torture, or the nature of any assurances obtained from them before rendering persons to them. To what extent U.S. agencies have legal authority to engage in renditions remains unclear. The only provision within the United States Code appearing to expressly permit an agency's participation in a rendition is 10 U.S.C. § 374(b)(1)(D), as amended in 1998, which permits the Department of Defense (DOD), upon request from the head of a federal law enforcement agency, to make DOD personnel available to operate equipment with respect to "a rendition of a suspected terrorist from a foreign country to the United States to stand trial."[2261] On the other hand, given that the United States has participated in renditions, there would appear to be legal limits on the practice, especially with regard to torture. This report describes the most relevant legal guidelines limiting the

---

9.html (remarking that the United States "operate[s] within the law and we send people to countries where they say they're not going to torture the people").

[2259] "McCain, Dems Press Goss On Torture Allegations," Congressional Daily, March 18, 2005.

[2260] Remarks of Secretary of State Condoleezza Rice Upon Her Departure for Europe, December 5, 2005, online at http://2001-2009.state.gov/secretary/rm/2005/57602.htm [hereinafter "Rice Statement"].

[2261] 10 U.S.C. § 374(b)(1)(D), added by Omnibus Consolidated and Emergency Supplemental Appropriations Act, 1999, P.L. 105-277, Div. B, Title II, § 201(2) (1998). Though U.S. law expressly permits the surrender of certain fugitives to face criminal charges in the requesting State in the absence of an extradition treaty , such persons (at least if found in the United States) are provided with certain procedural protections under statute and the Constitution. See 18 U.S.C. §§ 3181-3196; In re Kaine, 55 U.S. 103, 113 (1852) ("an extradition without an unbiased hearing before an independent judiciary [is] highly dangerous to liberty, and ought never to be allowed in this country").

transfer of persons to foreign States where they may face torture, as well as recent legislation seeking to limit the rendition of persons to countries believed to practice torture.

Limitations Imposed on Renditions by the Convention Against Torture and Implementing Legislation

The U.N. Convention against Torture and Other Cruel, Inhuman, or Degrading Treatment or Punishment (CAT)[2262] and U.S. domestic implementing legislation impose the primary legal restrictions on the transfer of persons to countries where they would face torture. CAT requires signatory parties to take measures to end torture within territories under their jurisdiction, and it prohibits the transfer of persons to countries where there is a substantial likelihood that they will be tortured.[2263] Torture is a distinct form of persecution, and is defined for purposes of CAT as "severe pain or suffering ... intentionally inflicted on a person" under the color of law.[2264] Accordingly, many forms of persecution—including certain harsh interrogation techniques that would be considered cruel and unusual under the U.S. Constitution—do not necessarily constitute torture, which is an extreme and particular form of mistreatment.[2265]

CAT also obligates parties to take measures to prevent "other acts of cruel, inhuman or degrading treatment or punishment which do not amount to torture," but this obligation only extends to acts occurring in territory under a State Party's jurisdiction.[2266] CAT also established the Committee against Torture, a monitoring body which has declaratory but non-binding authority concerning interpretation of the Convention.[2267] State parties are required to submit periodic reports to the Committee concerning their compliance with CAT.[2268]

[2262] Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment (CAT), G.A. Res. 39/46, Annex, 39 U.N. GAOR Supp. No. 51, U.N. Doc. A/39/51 (1984).

[2263] Id., art. 2(1).

[2264] Id., art. 1 (emphasis added).

[2265] For further background on the applicability of CAT to interrogation techniques, see CRS Report RL32438, U.N. Convention Against Torture (CAT): Overview and Application to Interrogation Techniques, by Michael John Garcia.

[2266] CAT art. 16(1).

[2267] See id., arts. 17-24.

[2268] Id., art. 19(1).

The United States ratified CAT in 1994, subject to certain declarations, reservations, and understandings, including that the Convention was not self-executing and therefore required domestic implementing legislation to take effect.[2269]

The express language of CAT Article 2 allows for no circumstances or emergencies where torture could be permitted by Convention parties.[2270] On the other hand, a number of CAT provisions limiting the acts of Convention parties does not use language coextensive as that contained in CAT Article 2. The following paragraphs describe the relevant provisions of CAT and implementing statutes and regulations that restrict the rendition of persons to countries when there is a substantial likelihood that such persons will be tortured. As will be discussed below, while CAT imposes an absolute prohibition on the use of torture by Convention parties, the plain language of certain CAT provisions may nevertheless permit parties in limited circumstances to transfer persons to countries where they would likely face torture, though such an interpretation arguably conflicts with the intent of the treaty.

[2269] It could be argued that despite its declaration that CAT was not self-executing and required implementing legislation to take effect, such legislation was actually unnecessary in the case of certain CAT provisions, including those related to the removal of persons to countries where they would likely face torture. However, U.S. courts hearing cases concerning the removal of aliens have regularly interpreted CAT provisions prohibiting alien removal to countries where an alien would likely face torture to be non-self executing and judicially unenforceable, except to the extent permitted under domestic implementing legislation. See, e.g., Pierre v. Gonzales, 502 F.3d 109 (2nd Cir. 2007) (finding that alien had no directly enforceable right to relief from removal under CAT, and such a claim must instead arise under U.S. law implementing the treaty); Castellano-Chacon v. INS, 341 F.3d 533 (6th Cir. 2003) (applicant for withholding of removal could not invoke CAT directly, but could rely upon implementing regulations); Akhtar v. Reno, 123 F.Supp.2d 191 (S.D.N.Y. 2000) (rejecting challenge made by criminal alien to removal pursuant to CAT, and stating that "[g]iven the apparent intent of the United States that the Convention not be self-executing, this Court joins the numerous other courts that have concluded that the Convention is not self-executing").

[2270] CAT Article 2(2) declares that "[n]o exceptional circumstances whatsoever, whether a state of war or a threat of war, internal political instability or any other public emergency, may be invoked as a justification of torture." According to the State Department's analysis of CAT, which was included in President Reagan's transmittal of the Convention to the Senate for its advice and consent, this explicit prohibition of all torture, regardless of the circumstances, was viewed by the drafters of CAT as "necessary if the Convention is to have significant effect, as public emergencies are commonly invoked as a source of extraordinary powers or as a justification for limiting fundamental rights and freedoms." President's Message to Congress Transmitting the Convention Against Torture and Other Cruel, Inhuman, or Degrading Treatment or Punishment, Summary and Analysis of the Convention Against Torture and Other Cruel, Inhuman, or Degrading Treatment or Punishment, May 23, 1988, S. Treaty Doc. No. 100-20 at 5, reprinted in 13857 U.S. Cong. Serial Set. [hereinafter "State Dept. Summary"].

CAT Limitation on the Transfer of Persons to Foreign States for the Purpose of Torture[2271]

CAT Article 3 provides that no State Party "shall expel, return ('refouler') or extradite a person to another State where there are substantial grounds for believing that he would be in danger of being subjected to torture." The U.S. ratification of CAT was contingent on its understanding that this requirement refers to situations where it would be "more likely than not" that a person would be tortured if removed to a particular country, a standard commonly used by U.S. courts when determining whether to withhold an alien's removal for fear of persecution.[2272]

It is important to note that CAT does not prohibit a State from transferring a person to another State where he or she would likely be subjected to harsh treatment that, while it would be considered cruel and unusual under the standards of the U.S. Constitution, would nevertheless not be severe enough to constitute "torture."[2273]

Domestic Implementation of CAT Article 3

The Foreign Affairs Reform and Restructuring Act of 1998 (FARRA) implemented U.S. obligations under CAT Article 3.[2274] Section 2242 of the act

---

[2271] For additional information, see CRS Report RL32276, The U.N. Convention Against Torture: Overview of U.S. Implementation Policy Concerning the Removal of Aliens, by Michael John Garcia.

[2272] Sen. Exec. Rpt. 101-30, Resolution of Advice and Consent to Ratification, (1990) at II.(2). See generally INS v. Stevic, 467 U.S. 407, 429-30 (1984). This standard is in contrast to the lower standard for determining whether an alien is eligible for consideration for asylum based on a "well-founded fear of persecution" if transferred to a particular country. To demonstrate a "well-founded" fear, an alien only needs to prove that the fear is reasonable, not that it is based on a clear probability of persecution. See INS v. Cardoza-Fonseca, 480 U.S. 421 (1987).

[2273] According to the State Department's analysis of CAT, the Convention's definition of torture was intended to be interpreted in a "relatively limited fashion, corresponding to the common understanding of torture as an extreme practice which is universally condemned." State Dept. Summary, supra footnote 43, p. 3. For example, the State Department suggested that rough treatment falling into the category of police brutality, "while deplorable, does not amount to 'torture'" for purposes of the Convention, which is "usually reserved for extreme, deliberate, and unusually cruel practices ... [such as] sustained systematic beating, application of electric currents to sensitive parts of the body, and tying up or hanging in positions that cause extreme pain." Id., p. 4 (presumably, police brutality of extreme severity could rise to the level of "torture"). This understanding of torture as a particularly severe form of cruel treatment is made explicit by CAT Article 16, which obligates Convention parties to "prevent in any territory under [their] jurisdiction other acts of cruel, inhuman, or degrading treatment or punishment which do not amount to acts of torture," thereby indicating that not all forms of inhumane treatment constitute torture.

[2274] P.L. 105-277 at § 2242(a)-(b).

announced the U.S. policy "not to expel, extradite, or otherwise effect the involuntary return of any person to a country in which there are substantial grounds for believing the person would be in danger of being subjected to torture, regardless of whether the person is physically present in the United States."[2275] The act further required all relevant federal agencies to adopt appropriate regulations to implement this policy.[2276]

In doing so, however, Congress opened the door for administrative action limiting CAT protection by requiring that, "to the maximum extent consistent" with Convention obligations, regulations adopted to implement CAT Article 3 exclude from their protection those aliens described in § 241(b)(3)(B) of the Immigration and Nationality Act (INA).[2277] INA § 241(b)(3)(B) acts as an exception to the general U.S. prohibition on the removal of aliens to countries where they would face persecution (which may or may not include actions constituting torture). An alien may be removed despite the prospect of likely persecution if the alien:

- assisted in Nazi persecution or engaged in genocide;
- ordered, incited, assisted, or otherwise participated in the persecution of an individual because of the individual's race, religion, nationality, membership in a particular social group, or political opinion;
- having been convicted of a particularly serious crime, is a danger to the community of the United States;
- is strongly suspected to have committed a serious nonpolitical crime outside the United States prior to arrival;[2278] or
- is believed, on the basis of reasonable grounds, to be a danger to the security of the United States.

Thus far, however, U.S. regulations concerning the removal of aliens and extradition of fugitives have prohibited the removal of all persons to States where they would more likely than not be tortured,[2279] regardless of whether they are described in INA § 241(b)(3)(B). CIA regulations concerning renditions (i.e., renditions where a person is seized outside the United States and transferred to a

---

[2275] Id., at § 2242(a) (emphasis added).

[2276] Id., at § 2242(b).

[2277] P.L. 105-277 at § 2242(c).

[2278] The distinction between political and nonpolitical crimes is occasionally unclear. For more background, see CRS Report 98-958, Extradition To and From the United States: Overview of the Law and Recent Treaties, by Charles Doyle, supra footnote 1.

[2279] See 8 C.F.R. §§ 208.16-18, 1208.16-18 (relating to the removal of aliens); 22 C.F.R. §95.2 (relating to extradition of persons).

third country) are not publicly available. Nevertheless, such regulations would presumably need to comply with the requirements of FARRA.

The Role of Diplomatic Assurances in Transfer Decisions

U.S. regulations implementing CAT Article 3 permit the consideration of diplomatic assurances in removal/extradition decisions.[2280] Pursuant to removal and extradition regulations, a person subject to removal or extradition may be transferred to a specified country that provides diplomatic assurances to the Secretary of State that the person will not be tortured if removed there. Such assurances must be deemed "sufficiently reliable" before a person can be transferred to a country where he or she would otherwise more likely than not be tortured.[2281] Although the DoD has not promulgated regulations implementing CAT Article 3, diplomatic assurances are also used by military authorities when determining whether to transfer a person from U.S. military detention at Guantanamo Bay, Cuba.[2282]

Assurances have also reportedly been used in rendition decisions made by the CIA. The *Washington Post* reported in 2005 that the CIA Office of General Counsel required the CIA station chief in a given country to obtain verbal assurances from that country's security service that a person will not be tortured if rendered there.[2283] Such assurances would then reportedly be cabled to CIA headquarters before the rendition may occur.[2284] In August 2009, a special task force created by the Obama Administration to review U.S. interrogation and transfer policies recommended that the State Department be involved in the evaluation of assurances in all cases.

CAT Article 3 itself (as opposed to U.S. regulations implementing CAT) provides little guidance as to the application of diplomatic assurances to decisions to transfer a person to another country. Although CAT Article 3 obligates signatory parties to take into account the proposed receiving State's human rights record, it also provides that the proposed sending State should take into account "all relevant considerations" when assessing whether to remove an individual to a

---

[2280] 8 C.F.R. § 208.18; 22 C.F.R. § 95.3(b) (describing authority of Secretary of State to surrender fugitive "subject to conditions").

[2281] 8 C.F.R. § 208.18(c).

[2282] For additional discussion, see CRS Report R40139, Closing the Guantanamo Detention Center: Legal Issues, by Michael John Garcia et al.

[2283] Priest, supra footnote 23.

[2284] Id.

particular State.[2285] A State's assurances that it will not torture an individual would appear to be a "relevant consideration" in determining whether or not it would be appropriate to render him there, at least so long as the assurances are accompanied by a mechanism for enforcement.[2286] Article 3 does not provide guidelines for how these considerations should be weighed in determining whether substantial grounds exist to believe a person would be tortured in the proposed receiving State.[2287] In its second periodic report to the Committee against Torture, the United States claimed that it:

> *obtains assurances, as appropriate, from the foreign government to which a detainee is transferred that it will not torture the individual being transferred. If assurances [are] not considered sufficient when balanced against treatment concerns, the United States would not transfer the person to the control of that government unless the concerns are satisfactorily resolved.*[2288]

On the other hand, the Committee against Torture has expressed concern over the use of diplomatic assurances by the United States. In 2006, it made a non-binding recommendation that the United States:

> *should only rely on "diplomatic assurances" in regard to States which do not systematically violate the Convention's provisions, and after a thorough examination of the merits of each individual case. The State party should establish and implement clear procedures for obtaining such assurances, with adequate judicial*

[2285] CAT art. 3(2).

[2286] See Committee against Torture, Communication No 233/2003: Sweden. 24/05/2005 (Agiza v. Sweden), CAT/C/34/D/233/2003 (2005) at para. 13.4., reprinted in 44 ILM 1103 (2005)(finding that diplomatic assurances which provided no mechanism for their enforcement did not suffice to protect against the risk of torture and thus did not absolve sending State of its responsibility under CAT art. 3).

[2287] The U.N. Special Rapporteur, an expert assigned by the U.N. Commission on Human Rights to examine issues related to torture, has stated that while diplomatic assurances "should not be ruled out a priori," they should be coupled with a system to monitor the treatment of transferred persons to ensure that they are not inhumanely treated. Interim Report of the Special Rapporteur of the Commission on Human Rights on the Question of Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, U.N. General Assembly, 59th Sess., A/59/324. While the Rapporteur's opinion may provide persuasive guidance in the interpretation of CAT obligations, the Rapporteur is not part of the CAT Committee and his opinions are not legally binding under the terms of CAT.

[2288] Second Periodic Report of the United States of America to the Committee Against Torture, submitted May 6, 2005, available at http://www.state.gov/g/drl/rls/45738.htm.

mechanisms for review, and effective post-return monitoring arrangements.[2289]

In addition, the United States has an obligation under customary international law to execute its Convention obligations in good faith,[2290] and is therefore required under international law to exercise appropriate discretion in its use of diplomatic assurances. For instance, if a State consistently violated the terms of its diplomatic assurances, the United States would presumably need to look beyond the face of such promises before permitting the transfer of an individual to that country.[2291]

Criminal Penalties for Persons Involved in Torture

One of the central objectives of CAT is to criminalize all instances of torture, regardless of whether they occur inside or outside a State's territorial jurisdiction. CAT Article 4 requires signatory States to criminalize all instances of torture, as well as attempts to commit and complicity or participation in torture.[2292] While CAT does not necessarily obligate a State to prevent acts of torture beyond its territorial jurisdiction, State Parties are nevertheless required to criminalize such acts and impose appropriate penalties.

CAT Article 5 establishes minimum jurisdictional measures that each State Party must adopt with respect to offenses described in CAT Article 4. A State Party to CAT must establish jurisdiction over CAT Article 4 offenses when:

- the offenses are committed in any territory under its jurisdiction or on board a ship or aircraft registered in that State;
- the alleged offender is a national of that State;
- the victim was a national of that State if that State considers it appropriate; or

---

[2289] Conclusions and Recommendations of the Committee against Torture regarding the United States of America, July 25, 2006, available at http://www.unhchr.ch/tbs/doc.nsf/898586b1dc7b4043c1256a450044f331/e2d4f5b2dccc0a4cc12571ee00290ce0/$FILE/G0643225.pdf [hereinafter "Committee Recommendations"], at para. 21.

[2290] See RESTATEMENT (THIRD) OF FOREIGN RELATIONS § 321 (1987) (recognizing that "every international agreement in force is binding upon the parties to it and must be performed by them in good faith").

[2291] The CAT Committee has stated that unenforceable diplomatic assurances are insufficient to meet Article 3 obligations. See Agiza v. Sweden, supra footnote 59.

[2292] CAT art. 4(1).

- the alleged offender is present in any territory under its jurisdiction and the state does not extradite him in accordance with CAT Article 8, which makes torture an extraditable offense.[2293]

In order to fulfill its obligations under CAT Articles 4 and 5, the United States enacted §§ 23402340B of the United States Criminal Code, which criminalize torture occurring *outside* the United States.[2294] Jurisdiction occurs when the alleged offender is either a national of the United States or is present in the United States, irrespective of the nationality of the victim or alleged offender.[2295] Congress did not enact legislation expressly prohibiting torture occurring *within* the United States, as it was presumed that such acts would "be covered by existing applicable federal and [U.S.] state statutes,"[2296] such as those statutes criminalizing assault, manslaughter, and murder. The Federal Torture Statute criminalizes torture, as well as attempts and conspiracies to commit torture.[2297]

The Federal Torture Statute provides that the specific intent of the actor to commit torture is a requisite component of the criminal offense.[2298] Specific intent is "the intent to accomplish the precise criminal act that one is later charged with."[2299] This degree of intent differs from general intent, which usually "takes the form of recklessness (involving actual awareness of a risk and the culpable taking of that risk) or negligence (involving blameworthy inadvertence)."[2300]

[2293] Id., art. 5.

[2294] Pursuant to an amendment made by the Ronald W. Reagan National Defense Authorization Act for Fiscal Year 2005, "United States" is defined as "the several States of the United States, the District of Columbia, and the commonwealths, territories, and possessions of the United States." Previously, the statute had defined "United States" as including all areas under U.S. jurisdiction, including U.S. special maritime and territorial jurisdiction. 18 U.S.C. § 2340(3).

[2295] 18 U.S.C. § 2340A. The USA PATRIOT Act amended the Federal Torture Statute to criminalize conspiracies to commit torture outside the United States. P.L. 107-56, Title VIII, § 811(g) (2001).

[2296] S.Rept. 103-107, at 59 (1993) (discussing legislation implementing CAT arts. 4 and 5).

[2297] 18 U.S.C. § 2340A(a).

[2298] For purposes of the federal criminal statute, "torture" is defined as "an act committed by a person acting under the color of law specifically intended to inflict severe physical or mental pain or suffering (other than pain or suffering incidental to lawful sanctions) upon another person within his custody or physical control." 18 U.S.C. § 2340(1) (emphasis added).

[2299] BLACK'S LAW DICTIONARY 814 (7th ed. 1999).

[2300] Id., at 813.

Application of CAT and Implementing Legislation to the Practice of Extraordinary Renditions

Although the express intent of CAT was to help ensure that no one would be subjected to torture,[2301] it is arguably unclear as to whether CAT would in *all* circumstances bar renditions to countries that practice torture, including possibly in certain cases where the rendering State was aware that a rendered person would likely be tortured. Clearly, it would violate U.S. criminal law and CAT obligations for a U.S. official to conspire to commit torture via rendition, regardless of where such renditions would occur. However, it is not altogether clear that CAT prohibits the rendering of persons seized *outside* the United States, or whether criminal sanctions would apply to a U.S. official who authorized a rendition without intending to facilitate the torture of the rendered person (as opposed to, for instance, the harsh mistreatment of the rendered person to a degree not rising to the level of torture).

Renditions from the United States

CAT Article 3 clearly prohibits the rendition of persons from the territory of a signatory State to another State when there are substantial grounds for believing the person would be tortured. Even if it could be technically argued that renditions do not constitute "extraditions" within the meaning of CAT Article 3, and the rendition was to a country other than one where the person previously resided (meaning that the person was not being "returned" to a country where he would risk torture), such transfers would still violate the Convention's requirement that no State Party "expel" a person from its territory to another State where he is more likely than not to be tortured.

If the United States were to receive diplomatic assurances from a State that it would not torture a person rendered there, and such assurances were deemed sufficiently credible, the rendition would not facially appear to violate either CAT Article 3 or domestic implementing legislation.

U.S. regulations permit the use of assurances in removal and extradition decisions, and CAT does not discuss their usage. As mentioned previously, however, the United States is obligated to execute its CAT obligations in good faith,[2302] and therefore must exercise appropriate discretion in its use of diplomatic assurances. If a State consistently violated the terms of its diplomatic assurances, or the United States learned that a particular assurance would not be met, the United States would presumably need to look beyond the face of such

---

[2301] CAT at Preamble.

[2302] See RESTATEMENT (THIRD) OF FOREIGN RELATIONS § 321 (1987) (recognizing that "every international agreement in force is binding upon the parties to it and must be performed by them in good faith").

promises before permitting the transfer of an individual to that country. Again, neither CAT nor U.S. implementing regulations prohibit the United States from transferring persons to States where they would face harsh treatment—including treatment that would be prohibited if carried out by U.S. authorities—that does not rise to the level of torture. Indeed, the United States could conceivably render a person to a State after receiving sufficient diplomatic representations that the rendered person could be accorded cruel and inhumane treatment not rising to the level of torture without violating CAT or CAT-implementing regulations.

Renditions from Outside the United States

As mentioned earlier, while CAT Article 2(2) provides that there are "no … circumstances whatsoever" allowing torture, certain other CAT provisions do not use language coextensive in scope when discussing related obligations owed by Convention parties. While CAT Article 3 clearly limits renditions from the United States, it is not altogether certain as to what extent CAT applies to situations where a country seizes suspects outside of its territorial jurisdiction and directly renders them to another country.[2303]

Extraterritorial Application of CAT Article 3

The territorial scope of CAT Article 3 is a matter of debate. As a general matter, the United States has taken the position that human rights treaties "apply to persons living in the territory of the United States, and not to any person with whom agents of our government deal in the international community."[2304] In 2006, representatives of the U.S. State Department informed the CAT Committee Against Torture that the United States does not believe CAT Article 3 applies to persons outside U.S. territory.[2305] However, these representatives also claimed that as a matter of policy, the United States accords CAT Article 3 protections to all persons in U.S. custody, regardless of whether such persons were found in U.S. territory.[2306] In congressional testimony in June 2008, State Department

[2303] The Washington Post has alleged that U.S. intelligence and law-enforcement officials have, on occasion, seized a terrorist suspect abroad and rendered him to a foreign intelligence service known to employ torture with a list of questions that these U.S. officials want answered. Dana Priest & Barton Gellman, "U.S. Decries Abuse but Defends Interrogations," Washington Post, December 26, 2002, p. A1.

[2304] JAG's Legal Ctr. & Sch., Operational Law Handbook 50 (Maj. Derek I. Grimes ed., 2006), available at http://www.fas.org/irp/doddir/army/law2006.pdf.

[2305] United States Written Response to Questions Asked by the Committee Against Torture, April 28, 2006, available at http://www.state.gov/g/drl/rls/68554.htm [hereinafter "Written Responses"].

[2306] Id.; Second Periodic Report of the United States of America to the Committee Against Torture, May 6, 2005, available at http://www.state.gov/g/drl/rls/45738.htm[hereinafter "Report to CAT Committee"], para. 30 (describing U.S. compliance with CAT Article 3, and

Legal Advisor John Bellinger testified that the view that CAT Article 3 did not apply to extraterritorially has "been the long-standing legal position[] of the United States since the Convention against Torture was ratified in 1994."[2307]

Although the scope of human rights treaties may generally be limited to conduct occurring within the territorial jurisdiction of parties, it seems clear that at least some CAT provisions are extraterritorial in scope. Most notably, CAT Articles 4-5 require parties to criminalize all acts of torture, regardless of where they occur.[2308] Indeed, the Federal Torture Statute implementing this obligation expressly covers torture occurring "outside the United States."[2309] Although several CAT provisions limit their scope to acts occurring "in any territory under [the State Party's] jurisdiction,"[2310] CAT Article 3 does not contain a similar limiting provision. Accordingly it could be argued that, like CAT Articles 4-5, CAT Article 3 is intended to be extraterritorial in scope.

Nevertheless, it could still be argued that the express provisions of CAT Article 3 do not apply to extraordinary renditions occurring outside the United States, at least so long as the person is not rendered to a country where he has formerly resided. Article 3 states that no party shall "expel, return ('refouler') or extradite a person" to a country where there are substantial grounds to believe that he or she will be tortured. It could be argued, however, that certain extraterritorial renditions are not covered by this provision. Seizing a person in one country and transferring him to another would arguably not constitute "expelling" the person, if a State is understood only to be able to "expel" persons from territory over which it exercises sovereign authority. So long as these persons were rendered to countries where they had not previously resided, it also could not be said that the

---

broadly stating that "The United States does not transfer persons to countries where the United States believes it is 'more likely than not' that they will be tortured. This policy applies to all components of the United States government."). See also Rice Statement, supra footnote 33 (describing U.S. rendition policy as complying with U.S. laws and treaties, including CAT, and denying the transport of anyone to a country where he would face torture).

[2307] Subcommittee on International Organizations, Human Rights, and Oversight, Diplomatic Assurances and Rendition to Torture: The Perspective of the State Department's Legal Advisor, committee print, 110th Cong., 2nd sess., June 10, 2008, p. 11 (statement by John B. Bellinger, III, Legal Advisor, State Department).

[2308] CAT Article 5 requires each State to establish jurisdiction over some (but not all) extraterritorial torture offenses, including when the offender is either a national of the State or is found in the State's territory and the State does not extradite him.

[2309] 18 U.S.C. §2340A. See also Report to CAT Committee, supra footnote 79, at paras 44-46 (discussing U.S. implementation of obligations under CAT Articles 4-5, including through the Federal Torture Statute and the Military Extraterritorial Jurisdiction Act, 18 U.S.C. §§ 3261 et seq., which extends U.S. criminal jurisdiction over certain categories of individuals for conduct occurring outside the United States).

[2310] See CAT arts. 2, 6-7, 11-13, 16.

United States "returned" these persons to countries where they faced torture (though persons rendered to countries where they had previously resided would presumably be protected under CAT Article 3). In addition, if such renditions were not executed via a formal process, it could be argued they did not constitute extraditions for the purposes of Article 3.[2311] Accordingly, it could be argued that the United States would not violate the express language of Article 3 if it rendered persons to countries where they faced torture, so long as no part of these renditions occurred within the territorial jurisdiction of the United States.[2312]

Critics of this view might argue that such a narrow interpretation of CAT Article 3 would contradict the Convention's over-arching goal to prevent torture. The fact that CAT requires parties to take legal steps to eliminate torture within their respective territories and to impose criminal penalties on torture offenders, coupled with the Convention's statement that "no exceptional circumstances whatsoever" can be used to justify torture, arguably imply that a State Party may never exercise or be complicit in the use of torture, even when it occurs extraterritorially. It could be further argued that the drafters of CAT did not explicitly discuss extraterritorial renditions because they were either not contemplated or, in cases where such renditions might occur absent the consent of the hosting country, because these actions were arguably already understood to be impermissible under international law.[2313] Indeed, some of the drafters of

---

[2311] See BASSIOUNI, supra footnote 1, at 29 ("Extradition in contemporary practice means a formal process by which a person is surrendered by one state to another based on a treaty, reciprocity, or comity.").

[2312] In Sale v. Haitian Centers Council, Inc., 509 U.S. 155 (1993), the Supreme Court held that the interdiction of Haitian refugees by the United States did not violate U.S. obligations under the U.N. Convention Relating to the Status of Refugees. The Court concluded that the Convention's provisions providing that no Contracting Party "shall expel or return ('refouler') a refugee" facing persecution applies only to refugees within a Party's territory, and not to those interdicted on the high seas. Id. at 179-183. Some have suggested that CAT Article 3's limitation on the transfer of persons should also be interpreted in a non-extraterritorial fashion. John Yoo, Transferring Terrorists, 79 NOTRE DAME L. REV. 1183, 1229 (2004) ("Given the Supreme Court's interpretation [in Sale] of identical language in the Refugee Convention, it makes no sense to view the Torture Convention as affecting the transfer of prisoners held outside the United States to another country."). On the other hand, the Sale Court's interpretation of the Refugee Convention's prohibition on the expulsion or return of refugees was largely based on this prohibition's interplay with other Convention provisions. Reading this prohibition to apply extraterritorially would create "an absurd anomaly" with a related Convention provision that only applied to refugees within a Convention Party's territory. Sale, 509 U.S. at 179180. In contrast, reading CAT Article 3 as being extraterritorial in scope would not have an incongruous effect on the interpretation of other CAT provisions.

[2313] See supra footnote 8.

CAT have taken the position that Article 3 was "intended to cover all measures by which a person is physically transferred to another State."[2314]

Opponents of a narrow interpretation of CAT would likely argue that it is contrary to the purpose of CAT to interpret the Convention as prohibiting formal transfers of persons to States where they face torture while still allowing such transfers through irregular forms of transfer. In 1994, the CAT Committee against Torture declared in a non-binding opinion that Article 3 prevents not only the return of a person to a country where he or she is in danger of being tortured, but also prohibits the person's transfer to "any other country where he runs a real risk of being expelled or returned to [his or her country of origin] or of being subjected to torture."[2315] More recently in 2006, the Committee urged the United States to "apply the non-refoulement guarantee [of CAT Article 3] to all detainees in its custody, cease the rendition of suspects, in particular by its intelligence agencies, to States where they face a real risk of torture, in order to comply with its obligations under article 3 of the Convention."[2316]

Extraterritorial Application of Legislation Implementing CAT Article 3

Beyond CAT, it is important to note that, given the express language of CAT-implementing legislation, the United States cannot "expel, extradite, or otherwise effect the involuntary return of any person to a country in which there are substantial grounds for believing the person would be in danger of being subjected to torture, *regardless of whether the person is physically present in the United States*."[2317] It may be argued that this express statutory language prohibits renditions from outside the United States, even if such renditions would not otherwise be in violation of CAT obligations.[2318]

[2314] J. HERMAN BURGERS & HANS DANELIUS, THE UNITED NATIONS CONVENTION AGAINST TORTURE: A HANDBOOK ON THE CONVENTION AGAINST TORTURE AND OTHER CRUEL, INHUMAN, OR DEGRADING TREATMENT OR PUNISHMENT 126 (1988). On the other hand, the State Department has claimed that "Neither the text of the Convention, its negotiating history, nor the U.S. record of ratification supports a view that Article 3 of the CAT applies to persons outside the territory of [a Party]." Written Responses, supra footnote 78.

[2315] Committee against Torture, Communication No 13/1993: Switzerland. 27/04/94 (Mutombo v. Switzerland), CAT/C/12/D/13/1993 (1994) at para. 10.

[2316] Committee Recommendations, supra footnote 62, at para. 20.

[2317] P.L. 105-277 at § 2242(a) (emphasis added).

[2318] Though it generally could be argued that a State can only "expel" someone from a territory over which the State exercises sovereign authority, the language of the U.S. legislation implementing CAT may suggest an intent by Congress to broadly define the prohibition on "expel[ling]" persons to countries where they would likely face torture, so that this prohibition covers not only expulsions from areas over which the United States exercises sovereign authority,

Two possible counter-arguments could be made to this position, at least in certain circumstances. The first and perhaps most compelling counter-argument is that although FARRA generally prohibits persons from being expelled, extradited, or involuntarily returned regardless of whether the person is physically present in the United States, section 2243(c) of the act makes an exception requiring federal agencies to exclude from the protection of CAT-implementing regulations any aliens who, inter alia, are reasonably believed to pose a danger to the United States, "to the maximum extent [such exclusions are] consistent" with CAT obligations.[2319] Accordingly, presuming for the sake of argument that CAT does not protect persons believed to be security dangers from being rendered from outside the United States, FARRA would require such persons to be excluded from the protection of any CAT-implementing regulations as well.

A second counter-argument is that the clause "regardless of whether the person is physically present in the United States" should be read only in reference to the prohibition contained in the CAT-implementing legislation upon the "involuntary return" of persons to countries where they would more likely than not be tortured, and not be read in reference to the prohibition on the extradition or expulsion of persons. CAT Article 3 obligates States not to "expel, return ('refouler') or extradite a person" to a State where he would be at substantial risk of torture. The principle of *non-refoulement* is commonly understood to prohibit not simply the exclusion of persons from the territory of the receiving State, but also a State from "turning back" persons at its borders and compelling their involuntary return to their country of origin.[2320] Unlike CAT Article 3, CAT-implementing legislation enacted by the United States does not use the term "refouler." However, its use of the phrase "involuntary return ... regardless of whether the person is physically present in the United States" appears to reflect the principle of non-refoulement expressed in CAT. It could be argued that the use of the phrase "regardless of whether the person is physically present in the

---

but also "expulsions" from all other areas (e.g., rendering persons captured in non-U.S. territory to other States).

[2319] Id. at § 2242(c).

[2320] For additional background on the concept of non-refoulement and its development in international human rights law, see Elihu Lauterpacht & Daniel Bethlehem, The Scope and Content of the Principle of Non-refoulement, in REFUGEE PROTECTION IN INTERNATIONAL LAW:UNHCR'S GLOBAL CONSULTATIONS ON INTERNATIONAL PROTECTION 78-177 (Erika Feller, Volker Türk and Frances Nicholson eds., 2003). It should be noted that the CAT-implementing legislation prohibiting the return of any person to a country where he would face torture, regardless of whether he was physically present in the United States, was enacted five years after the Supreme Court's decision in Sale v. Haitian Centers Council, Inc., 509 U.S. 155 (1993). In Sale, the Court found that the Refugee Convention's prohibition on the refoulement of refugees was not intended to apply extraterritorially. Sale, 509 U.S. at 179-187. See also supra footnote 85.

United States" in CAT-implementing legislation was only intended to be read in reference to the "involuntary return" phrase that precedes it (a reading that reflects the non-refoulement obligation imposed by CAT), and not meant also to be read in reference to the prohibition imposed upon the expulsion and extradition of persons to countries where they would likely face torture, as this alternative reading would arguably go beyond the non-refoulement obligations imposed upon the United States by the express language of CAT.

Regardless of whether renditions that occur outside of the United States are covered under CAT Article 3 and CAT-implementing legislation and regulations, CAT Article 4 and corresponding domestic law criminalizing all acts of torture and complicity therein would be controlling. Accordingly, U.S. officials could not conspire with officials in other States to render a person so that he would be tortured. As discussed below, however, criminal penalties may not necessarily attach to a person who renders another with the knowledge that he will likely be tortured.

Criminal Sanctions for Participation in Torture

CAT Article 4 and the Federal Torture Statute do not expressly prohibit the transfer of a person to a State where he is more likely than not to face torture. Indeed, the Federal Torture Statute only imposes criminal penalties for acts or attempts to commit torture and, most relevantly to the subject of renditions, conspiracies to commit torture. Clearly, if a U.S. official rendered a person to another country with instructions for the country to torture the rendered individual, that official could be criminally liable under the Federal Torture Statute.[2321]

However, it appears unlikely that a U.S. official would be found criminally liable for conspiracy to commit torture if he authorized a rendition after receiving assurances that the rendered person would not be tortured. It is generally understood that a conspiracy to commit a crime requires an agreement between parties for a common purpose.[2322] Presuming that the United States received

[2321] Such an official might also be charged under the federal statute governing accomplice liability, which makes it a criminal offense to willfully cause an act to be done which, if directly performed by him or another, would be a criminal offense. 18 U.S.C. § 2.

[2322] See, e.g., Iannelli v. United States, 420 U.S. 770, 777 (1975) ("[c]onspiracy is an inchoate offense, the essence of which is an agreement to commit an unlawful act"); United States v. Evans, 970 F.2d 663, 668 (10th Cir. 1992) ("[to] prove conspiracy, the government must show '[1] that two or more persons agreed to violate the law, [2] that the defendant knew at least the essential objectives of the conspiracy, … [3] that the defendant knowingly and voluntarily became a part of it,' and [4] that the alleged coconspirators were interdependent") (quoting United States v. Fox, 902 F.2d 1508, 1514 (10th Cir. 1990)); United States v. Pearce, 912 F.2d 159, 161 (6th Cir. 1990) ("the essential element of conspiracy is that 'the members of the conspiracy in some way or

assurances before rendering a person to another country, it would be difficult to argue that the official "agreed" to facilitate the rendered person's subsequent torture.

Other Statutes and Treaties Relevant to the Issue of Renditions

Although CAT and its implementing legislation provide the primary legal constraints upon the rendition of persons to countries believed to engage in torture, other treaties and statutes are also potentially relevant. The following paragraphs briefly discuss a few of them.

1949 Geneva Conventions

In certain situations, the 1949 Geneva Conventions may impose limitations on the use of renditions separate from those imposed by CAT. Each of the four Conventions accords protections to specified categories of persons in armed conflict or in post-conflict, occupied territory.[2323] The torture, or inhumane or degrading treatment of persons belonging to specified categories—including civilians and protected prisoners of war (POWs)—is expressly prohibited by the Conventions.[2324] In addition, "[n]o physical or moral coercion shall be exercised against protected [civilians], in particular to obtain information from them or from third parties."[2325]

The Geneva Conventions impose limitations on the transfer of protected persons. Civilians may not be *forcibly* (as opposed to voluntarily) transferred to another State.[2326] A violation of this obligation represents a "grave breach" of the relevant Geneva Convention and therefore constitutes a war crime.[2327] However, it is not a violation of the Geneva Conventions to extradite such persons, in compliance

---

manner, or through some contrivance, came to a mutual understanding to try to accomplish a common and unlawful plan'") (internal citation omitted).

[2323] Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, 6 U.S.T. 3114; Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea, 6 U.S.T. 3217; Geneva Convention Relative to the Treatment of Prisoners of War, 6 U.S.T. 3316 [hereinafter "Third Geneva Convention"]; Geneva Convention Relative to the Protection of Civilian Persons in Time of War, 6 U.S.T. 3516 [hereinafter "Fourth Geneva Convention"] (entered into force October 21, 1950). The United States, Iraq, and Afghanistan are all parties to the Conventions.

[2324] See, e.g., Third Geneva Convention, arts. 3, 17, 87, 130; Fourth Geneva Convention, arts. 3, 32, 147.

[2325] Fourth Geneva Convention, art. 31.

[2326] Id., art. 49.

[2327] Id., art. 147.

with extradition treaties concluded before the outbreak of hostilities, who are charged with ordinary criminal law offenses.[2328]

Neither civilians nor protected POWs may be transferred to penitentiaries for disciplinary punishment.[2329] In addition, persons protected by the Conventions may only be transferred to other Convention parties, and then only after the transferring Power "has satisfied itself of the willingness and ability of such transferee Power to apply the Convention."[2330] If the transferee Power fails to abide by the Convention in any important respect (e.g., torturing a transferred person), upon notification the transferring Power is required to either request their return or "take effective measures to correct the situation."[2331] Accordingly, in order to comply with its Convention obligations, the United States may only render a protected person if (1) the State to which the person was being rendered was a member of the Convention; (2) the United States had received assurances that the person would not be tortured if rendered there; and (3) the United States requested the return of the rendered person or took other effective measures if the rendered individual was subsequently tortured.

In the case of armed conflicts that are not of an international character and occur in the territory of a High Contracting Party, each party is obligated under Article 3 of each of the 1949 Geneva Conventions (Common Article 3) to accord *de minimis* protections to "[p]ersons taking no active part in the hostilities, including members of armed forces who have laid down their arms and those placed hors de combat by sickness, wounds, detention, or any other cause." Parties are required to treat such persons "humanely," and are prohibited from subjecting such persons to "violence to life and person … mutilation, cruel treatment and torture … [and] [o]utrages upon personal dignity, in particular humiliating and degrading treatment."

As mentioned previously, the Geneva Conventions apply in limited circumstances. Besides only applying in armed conflict or in post-conflict occupied territory, the Conventions also only protect designated categories of persons (though other persons may nevertheless be owed certain protections under customary laws of war). At least since early 2002, the Bush Administration took the position that the Geneva Conventions did not apply to members of Al

---

[2328] Id., art. 45.

[2329] Third Geneva Convention, art. 97; Fourth Geneva Convention art. 124. The Conventions do not expressly prohibit the transfer of such persons for non-disciplinary reasons.

[2330] Third Geneva Convention, art. 12; Fourth Geneva Convention, art. 45.

[2331] Third Geneva Convention, art. 12; Fourth Geneva Convention, art. 45.

Qaeda.[2332] Reportedly, the Administration also concluded that the Geneva Convention prohibition on the "forcible transfer" of civilians did not apply to "illegal aliens" who entered Iraq following the U.S.-led invasion, or bar the temporary removal of persons from Iraq for the purposes of interrogation.[2333]

In the 2006 case of *Hamdan v. Rumsfeld*, the Supreme Court held that Common Article 3 of the Geneva Conventions applied to the armed conflict with Al Qaeda and accorded Al Qaeda members certain minimal protections, even if such persons were not otherwise covered by other Convention provisions (i.e., those covering "lawful combatants" and civilians in conflicts between States). Common Article 3 does not expressly prohibit the transfer of persons to other countries, even if such persons might face cruel treatment or torture there. Some have argued that Common Article 3 nevertheless prohibits renditions committed to facilitate the rendered person's torture or cruel treatment.[2334] However, it is unclear whether this interpretation is proper[2335] or that it would cover all renditions to countries where the detainee would face torture or cruel treatment (e.g., when the rendering country does not request the torture or cruel treatment of the detainee by the party to which he is rendered).

For purposes of U.S. law, however, it does not appear that Common Article 3 has been understood to cover renditions of persons to countries where they might face torture.[2336] The Military Commissions Act of 2006 (MCA, P.L. 109-366),

---

[2332] See White House Memorandum, Humane Treatment of Taliban and Al Qaeda Detainees (February 7, 2002), available at http://www.pegc.us/archive/White_House/bush_memo_20020207_ed.pdf.

[2333] See Dana Priest, "Memo Lets CIA Take Detainees Out of Iraq," Washington Post, October 24, 2004, p. A1 (discussing draft DOJ Office of Legal Counsel opinion dated March 19, 2004); Jack L. Goldsmith III, Asst. Attorney General, Permissibility of Relocating Certain "Protected Persons" from Occupied Iraq,. Dept. of Justice, Office of Legal Counsel, March 19, 2004 (draft), available at http://www.washingtonpost.com/wp-srv/nation/documents/ doj_memo031904.pdf. See also Jack L. Goldsmith III, Asst. Attorney General , "Protected Person" Status in Occupied Iraq under the Fourth Geneva Convention, Dept. of Justice, Office of Legal Counsel, March 18, 2004, http://www.usdoj.gov/olc/2004/gc4mar18.pdf.

[2334] See David Weissbrodt & Amy Bergquist, Extraordinary Rendition: a Human Rights Analysis, 19 HARV. HUM. RTS. J. 123, 151-153 (2006).

[2335] As discussed, several Convention provisions specifically discuss and limit the transfer of protected persons to third parties when such persons would face treatment prohibited by the Conventions. See infra at 19-20. It could be argued that these provisions would be made redundant if Convention provisions covering mistreatment were also read to cover the rendition of detainees to third-parties who might subject them to mistreatment.

[2336] U.S. authorities have apparently not considered Common Article 3 to be relevant in military transfer decisions, and have instead only considered whether the transfer would be consistent with CAT Article 3. Declaration of Joseph Benkert, Principal Deputy Assistant Secretary of

which was signed into law on October 17, 2006, provides that for purposes of U.S. law it is generally a violation of Common Article 3 to engage in conduct (1) inconsistent with the Detainee Treatment Act of 2005, which prohibits "cruel, inhuman, or degrading treatment" of persons in U.S. custody or control;[2337] or (2) subject to criminal penalty under provisions of the War Crimes Act, as amended, concerning "grave breaches" of Common Article 3.[2338] Under this standard, torture and cruel treatment would only be considered a violation of Common Article 3 in cases where the victim was in the custody or control of the United States, not in circumstances where the victim was transferred to the custody and control of a third-party and was subsequently treated harshly. As discussed in the following paragraph, however, this standard might still prohibit U.S. personnel from rendering a person covered by Common Article 3 if they have conspired with the receiving party to intentionally cause the transferee serious bodily injury.

War Crimes Act

The War Crimes Act imposes criminal penalties upon U.S. nationals or Armed Forces members who commit listed offenses of the laws of war.[2339] Persons who commit applicable war crimes are potentially subject to life imprisonment or, if death results from such acts, the death penalty. War crimes include "grave breaches" of the Geneva Conventions,[2340] such as torture of protected POWs or civilians and the "unlawful deportation or transfer or unlawful confinement" of protected civilians,[2341] as well as certain violations of Common Article 3.[2342]

As discussed previously, following the Supreme Court's ruling in Hamdan, it is understood as a matter of U.S. law that Common Article 3 covers the conflict with Al Qaeda and accords Al Qaeda members captured in that armed conflict with

---

Defense for Global Security Affairs, DoD, executed on June 8, 2007, at para. 3, In re Guantanamo Bay Detainee Litigation, Case No. 1:05-cv-01220 (D.D.C. 2007).

[2337] For background on the Detainee Treatment Act's prohibition on "cruel, inhuman, or degrading treatment," see CRS Report RL33655, Interrogation of Detainees: Requirements of the Detainee Treatment Act, by Michael John Garcia.

[2338] For background, see CRS Report RL33662, The War Crimes Act: Current Issues, by Michael John Garcia.

[2339] 18 U.S.C. § 2441.

[2340] 18 U.S.C. §§ 2441(c)(1).

[2341] E.g., Fourth Geneva Convention, art. 147.

[2342] 18 U.S.C. § 2441(c)(3). Until October 17, 2006, the War Crimes Act prohibited any violation of Common Article 3. The Military Commissions Act (P.L. 109-366) amended this provision so that only certain, "grave" violations of Common Article 3 are subject to criminal penalty. This amendment was retroactive in effect.

certain protections.[2343] Accordingly, certain forms of treatment with respect to Al Qaeda members is subject to criminal penalty, including torture, certain lesser forms of cruel treatment, and the intentional infliction of serious bodily injury.

Although the War Crimes Act imposes criminal penalties for conspiring to subject protected persons to torture or cruel treatment, such persons must be in the offender's custody or control. Accordingly, the provisions of the War Crimes Act covering torture and cruel treatment do not appear to cover the rendition of persons to countries for the purpose of cruel treatment or torture (though any U.S. personnel who conspired with officials in other States to render a person so that he would be tortured could still be prosecuted under the Federal Torture Statute).

However, the War Crimes Act may be interpreted as prohibiting some renditions. As amended by the MCA, the War Crimes Act expressly prohibits persons from conspiring to commit such acts as rape, mutilation or maiming, or causing "serious bodily injury" against persons protected by Common Article 3.[2344] A person may be subject to criminal penalty for these offenses regardless of whether the victim was in his custody or control. Accordingly, any U.S. personnel who conspire with officials in other States to render a person so that he would be subjected to serious bodily injury, rape, or sexual assault would appear to be subject to criminal liability under the War Crimes Act. As a practical matter, it is unclear whether the War Crimes Act would prohibit renditions in any circumstance not already prohibited under the Federal Torture Statute.[2345]

[2343] It is not clear that Common Article 3 is applicable to captured Al Qaeda agents in all circumstances. The Geneva Conventions concern treatment owed to protected persons in an armed conflict, and would arguably be inapplicable to law enforcement activities relating to Al Qaeda agents. International terrorism is recognized as a criminal offense under both domestic law and various international agreements. E.g., 18 U.S.C. § 2332b (concerning certain terrorist activities transcending international boundaries); International Convention for the Suppression of the Financing of Terrorism, S. Treaty Doc. No. 106.49, entered into force for the United States on July 26, 2002; International Convention for the Suppression of Terrorist Bombings, S. Treaty Doc. No. 106-6, entered into force for the United States on July 26, 2002. Whether the Geneva Conventions are applicable to the arrest and detention of Al Qaeda agents may depend upon whether such agents were (1) captured on or away from the battlefield; (2) captured by military or law enforcement agents; and (3) charged with a criminal offense, and if so, whether the offense relates to a violation of the laws of war or some other activity.

[2344] For an act of mutilation or maiming to be covered by the War Crimes Act, it must be committed in the course of committing another offense under the War Crimes Act that is listed as a "grave breach" of Common Article 3.

[2345] Mutilation and maiming, the intentional causing of serious bodily injury (defined by reference to 18 U.S.C. § 113b as bodily injury involving a substantial risk of death, extreme physical pain, disfigurement, or loss or impairment of the function of a bodily member, organ, or mental faculty), and rape have all been found by U.S. courts to constitute torture, at least in some circumstances. See Zubeda v. Ashcroft, 333 F.3d 463 (3rd Cir. 2003) ("[r]ape can constitute torture"); CRS Report RL33662, The War Crimes Act: Current Issues, by Michael John Garcia,

International Covenant on Civil and Political Rights

Article 7 of the International Covenant on Civil and Political Rights (ICCPR),[2346] ratified by the United States in 1992, prohibits the State Parties from subjecting persons "to torture or to cruel, inhuman, or degrading treatment or punishment."[2347] The Human Rights Committee, the monitoring body of the ICCPR, has interpreted this prohibition to prevent State Parties from exposing "individuals to the danger of torture or cruel, inhuman or degrading treatment or punishment upon return to another country by way of their extradition, expulsion or refoulement."[2348] Although the Committee is charged with monitoring the compliance of parties with the ICCPR and providing recommendations for improving treaty abidance, its opinions are not binding law.

U.S. ratification of the ICCPR was contingent upon the inclusion of a reservation that the treaty's substantive obligations were not self-executing (i.e., to take effect domestically, they require implementing legislation in order for courts to enforce them, though U.S. obligations under the treaty remain binding under international law).[2349] The United States also declared that it considered Article 7 binding "to the extent that 'cruel, inhuman or degrading treatment or punishment' [prohibited by ICCPR Article 7] means the cruel and unusual treatment or punishment prohibited by the Fifth, Eighth, and/or Fourteenth Amendments to the Constitution of the United States."[2350]

The United States has not enacted laws or regulations to comply with the Human Rights Committee's position that ICCPR Article 7 prohibits the transfer of persons to countries where they would likely face torture or cruel, inhuman, or degrading treatment. CAT-implementing regulations prohibit the transfer of

---

supra footnote 110, at 7-8. Whether sexual assault rises to the level of torture depends on the particular nature of the assault. Cf. Zubeda, 333 F.3d at 472-473 (discussing instances where courts have found rape or sexual abuse to constitute torture).

[2346] International Covenant on Civil and Political Rights, G.A. Res. 2200A, U.N. GAOR, 3rd Comm., 21st Sess., 1496th plen, mtg. at 49, U.N. Doc. A/RES/ 2200A (XXI) (1966).

[2347] Id., art. 7.

[2348] Human Rights Committee, General Comment 20, Article 7, UN Doc. A/47/40 (1992) reprinted in Compilation of General Comments and General Recommendations Adopted by Human Rights Treaty Bodies, U.N. Doc. HRI\GEN\1\Rev.1 at 30 (1994).

[2349] See United Nations Treaty Collection, Declarations and Reservations to the International Covenant on Civil and Political Rights, at http://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-4&chapter=4&lang= en.

[2350] Id.

persons to countries where they would more likely than not face torture, but not cruel, inhuman, or degrading treatment that does not rise to the level of torture.

Universal Declaration of Human Rights

The U.N. Charter provides that it is the duty of the United Nations to promote "universal respect for, and observance of, human rights and fundamental freedoms,"[2351] and Member States have an obligation to work jointly and separately to promote such rights and freedoms.[2352] In 1948, the

U.N. General Assembly adopted the Universal Declaration of Human Rights,[2353] to explicate the "human rights and fundamental freedoms" that Member States were obliged to protect. The Universal Declaration prohibits, inter alia, the arbitrary arrest, detention, or exile of persons,[2354] as well as torture and cruel, inhuman, or degrading treatment.[2355]

The Universal Declaration is not a treaty and accordingly is not technically binding on the United States,[2356] though a number of its provisions are understood to reflect customary international law.[2357] The Universal Declaration does not include an enforcement provision.

Recent Developments

On January 22, 2009, President Barack Obama issued a series of Executive Orders concerning the treatment of persons apprehended by the United States in connection with armed conflicts or counterterrorism operations. The Orders do not expressly modify U.S. rendition policy, though one Order does mandate the closure of all CIA detention facilities, some of which were used to hold persons

---

[2351] U.N. CHARTER art. 55.

[2352] Id., art. 56.

[2353] Universal Declaration of Human Rights, G.A. Res. 217A (III), U.N. Doc. A/810 (1948).

[2354] Id., art 9.

[2355] Id., art. 5.

[2356] See Sosa v. Alvarez-Machain, 542 U.S. 692, 734 (2004) (declining to apply protections espoused by the Universal Declaration of Human Rights because it "does not of its own force impose obligations as a matter of international law").

[2357] See Filartiga v. Pena-Irala, 630 F.2d 876, 882 (2d Cir. 1980). But see Sosa, 124 S.Ct. at 2761-62 (finding that certain provisions of the Universal Declaration did not in themselves constitute an international norm that would fulfill the criteria that existed in the 18th century for a norm to be customary international law).

seized by the United States in other locations.[2358] However, two of the Orders create separate task forces charged with reviewing aspects of U.S. detention policy, including the transfer of detainees to foreign States. The Executive Order entitled "Ensuring Lawful Interrogations" establishes a Special Interagency Task Force on Interrogation and Transfer Policies, which is charged with reviewing

> *the practices of transferring individuals to other nations in order to ensure that such practices comply with the domestic laws, international obligations, and policies of the United States and do not result in the transfer of individuals to other nations to face torture or otherwise for the purpose, or with the effect, of undermining or circumventing the commitments or obligations of the United States to ensure the humane treatment of individuals in its custody or control.[2359]*

Another Executive Order, entitled "Review of Detention Policy Options," creates a Special Task Force on Detainee Disposition, which is required

> *to conduct a comprehensive review of the lawful options available to the Federal Government with respect to the apprehension, detention, trial, transfer, release, or other disposition of individuals captured or apprehended in connection with armed conflicts and counterterrorism operations, and to identify such options as are consistent with the national security and foreign policy interests of the United States and the interests of justice.[2360]*

Each Task Force was required to issue a report to the President of its recommendations within 180 days, unless the Task Force chair determined that an extension was appropriate. In July, the Chairman of the Special Task Force on

---

[2358] Executive Order No. 13491, "Ensuring Lawful Interrogations," 74 FED. REG. 4893, January 22, 2009, at § 4. For additional background, see CRS Report RL33643, Undisclosed U.S. Detention Sites Overseas: Background and Legal Issues, by Jennifer K. Elsea and Julie Kim.

[2359] Id., § 5. The Task Force is chaired by the Attorney General, and includes the Director of National Intelligence and the Secretary of Defense (who serve as co-vice-chairs); the Secretary of State; the Secretary of Homeland Security; the Director of the CIA; the Chairman of the Joint Chiefs of Staff; and other officers or full-time or permanent part-time employees of the United States, as determined by the Attorney General, with the concurrence of the head of the department or agency concerned.

[2360] Executive Order 13493, "Review of Detention Policy Options," 74 FED. REG. 4901, January 22, 2009, at § 1. The Task Force includes the Attorney General and Secretary of Defense, who serve as co-chairs; the Secretary of State; the Secretary of Homeland Security; the Director of National Intelligence; the Director of the Central Intelligence Agency; the Chairman of the Joint Chiefs of Staff; and other officers or full-time or permanent part-time employees of the United States, as determined by either of the co-chairs, with the concurrence of the head of the department or agency concerned.

Interrogation and Transfer Polices extended the deadline for the Task Force's final report by two months, while the deadline for the Special Task Force on Detainee Disposition was extended by six months.[2361]

On August 24, 2009, the Special Task Force on Interrogation and Transfer Polices issued its recommendations to the President, including with respect to the practice of rendition.[2362] These included recommendations to ensure that U.S. transfer practices comply with applicable legal requirements and do not result in the transfer of persons to face torture. The Task Force supported the continued use of assurances from a receiving country that an individual would not face torture if transferred there. However, the Task Force made recommendations intended to strengthen the procedures used in obtaining and evaluating such assurances. These include involving the State Department in evaluating assurances in all cases. The Task Force advised that relevant agencies obtaining assurances should "insist on a monitoring mechanism, or otherwise establish a monitoring mechanism, to ensure consistent, private access to the individual who has been transferred, with minimal advance notice to the detaining government."[2363] The Task Force also recommended that the Inspectors General of the Departments of State, Defense, and Homeland Security prepare an annual, coordinated report on transfers which were effectuated in reliance on assurances and were conducted by each of their agencies.

The Task Force made specific recommendations with respect to immigration removal proceedings and military transfer decisions. Classified recommendations were also made to ensure that, in the event that the Intelligence Community participates in a transfer, any affected individual is subjected to lawful treatment.

In the 110th Congress, legislative proposals were introduced to limit the ability of U.S. agencies to render persons to foreign States, and it is possible that similar proposals will be introduced in the 111th Congress. S. 1876, the National Security with Justice Act of 2007, introduced by Senator Biden on July 25, 2007, would have barred the United States from rendering or participating in the rendition of any individual to a foreign State absent authorization from the Foreign Intelligence Surveillance Court, except under limited circumstances in the case of

---

[2361] See Department of Justice, "Detention Policy Task Force Issues Preliminary Report," press release, July 21, 2009, http://www.usdoj.gov/opa/pr/2009/July/09-ag-705.html.

[2362] Department of Justice, "Special Task Force on Interrogations and Transfer Policies Issues Its Recommendations to the President," press release, August 24, 2009, http://www.usdoj.gov/opa/pr/2009/August/09-ag-835.html. The Task Force considered seven types of transfers: extradition, immigration removal proceedings, transfers pursuant to the Geneva Conventions, transfers from Guantanamo Bay, military transfers within or from Afghanistan, military transfers within or from Iraq, and transfers pursuant to intelligence authorities.

[2363] Id.

enemy combatants held by the United States (though renditions in such circumstances would still have to comply with other legal requirements). For an order to be issued by the Foreign Intelligence Surveillance Court authorizing a rendition, the requesting U.S. official would have needed to provide evidence that the rendered person was (1) an international terrorist; and (2) would not be subjected to torture or lesser forms of cruel, inhuman, or degrading treatment—a more stringent limitation on the transfer of persons than that expressly imposed by CAT Article 3, which only bars the transfer of persons to countries where they would face torture.

H.R. 1352, the Torture Outsourcing Prevention Act, introduced by Representative Markey on March 6, 2007, would have required the State Department to provide annual reports to appropriate congressional committees regarding countries where there are substantial grounds for believing that torture or cruel, inhuman, or degrading treatment is commonly used in the detention or interrogation of individuals. Generally, persons could not be transferred to such countries, whether through rendition or some other process. This prohibition could be waived by the Secretary of State in limited circumstances, including, at a minimum, when continuing access to each such person was granted to an independent humanitarian organization. Written or oral assurances made to the U.S. government would have been deemed insufficient to demonstrate that a person would not face torture or cruel, inhuman, or degrading treatment if rendered to a particular State.

18 U.S.C. CHAPTER 119: WIRE AND ELECTRONIC COMMUNICATIONS INTERCEPTION AND INTERCEPTION OF ORAL COMMUNICATIONS (18 U.S.C. §§ 2510-2522)

Title III and the Electronic Communications Privacy Act

Privacy: An Abbreviated Outline of Federal Statutes Governing Wiretapping and Electronic Eavesdropping, 98-327 (September 2, 2008)

GINA MARIE STEVENS & CHARLES DOYLE, CONGRESSIONAL RESEARCH SERV., PRIVACY: AN ABBREVIATED OUTLINE OF FEDERAL STATUTES GOVERNING WIRETAPPING AND ELECTRONIC EAVESDROPPING (2008), *available at* http://www.intelligencelaw.com/library/secondary/crs/pdf/98-327_9-2-2008.pdf.

Order Code 98-327
Updated September 2, 2008

Gina Marie Stevens and Charles Doyle
American Law Division

Summary

It is a federal crime to intentionally wiretap or electronically eavesdrop on the conversation of another without a court order or the consent of one of the parties to the conversation. Moreover, in eleven states, it is a state crime for anyone other than the police to intentionally wiretap and/or electronically eavesdrop on the conversation of another without the consent of all of the parties to the conversation. The federal crimes are punishable by imprisonment for up to five years and expose offenders to civil liability for damages, attorneys' fees, and possibly punitive damages. State crimes carry similar consequences. Even in states where one party consent interceptions are legal, they may well be contrary

to the professional obligations of members of the bar. The proscriptions often include a ban on using or disclosing the fruits of an illegal interception.

Statutory exceptions to these general prohibitions permit judicially supervised wiretapping or electronic eavesdropping conducted for law enforcement or foreign intelligence gathering purposes. Similar regimes — proscriptions with exceptions for government access under limited circumstances — exist for telephone records, e-mail and other forms of electronic communications.

Introduction

The first federal wiretap statute was a World War I provision enacted for the duration of the conflict and designed to protect confidential government information (citation for the authority for this and other statements made throughout this report may be found in the long version of this report, CRS Report 98-326, *Privacy: An Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping*). The 1927 Radio Act outlawed intercepting and divulging private radio messages. The 1934 Communications Act extended the interception and divulgence ban to telephone and telegraph communications.

No federal law condemned secretly capturing face to face conversations by using hidden microphones or their ilk, and police and federal authorities employed them with increasing regularity. Then in the late 1960's, the Supreme Court held that the privacy protection afforded by the Fourth Amendment's warrant requirements enveloped all that over which an individual might have a "justifiable expectation of privacy" — including, under the appropriate circumstances, the individual's conversations.

In anticipation of the Court's announcement, several states had enlarged the powers of their courts to issue wiretapping and/or electronic eavesdropping warrants. The Court, however, found one of the more detailed of these constitutionally deficient. Congress responded with Title III of the Omnibus Crime Control and Safe Streets Act to provide a constitutionally viable procedure under which state and federal courts might approve wiretapping and electronic eavesdropping orders. Title III at the same time outlawed wiretapping and electronic eavesdropping except under court order or with the consent of one of the parties to the conversation.

Title III regulated capture of the spoken word, it did nothing to protect the more modern forms of communication — fax messages, e-mail, electronically transmitted data. Congress recast Title III in the Electronic Communications Privacy Act (ECPA) to correct this oversight. It responded to a Supreme Court opinion again — this one describing the President's inherent authority to approve warrantless wiretapping of purely domestic threats to national security — with the Foreign Intelligence Surveillance Act (FISA). FISA creates a judicial warrant procedure for foreign intelligence information gathering.

Crimes

Title III/ECPA bars the use of any mechanism (device), tape recorder included, to intentionally capture the spoken word or any communication being transmitted electronically (intercept wire, oral, or electronic communications) without the consent of one of the participants or a court order, 18 U.S.C. 2511(1)(a),(b). This applies to all telephone conversations whether a cell telephone is involved or not. It likewise applies to all face to face conversations unless they occur in a public place or under other circumstances where the speakers should reasonably have expected that their conversation would be overheard.

Most states have similar statutes, and even when it is not a federal crime, wiretapping and/or electronic eavesdropping by anyone other than the police is a state crime (under mens rea requirements that vary from state to state) when done without the consent of all parties to the conversation in California, Delaware, Florida, Illinois, Kansas, Maryland, Massachusetts, Montana, Oregon, Pennsylvania, and Washington.

Beyond interception (wiretapping or electronic eavesdropping), it is a federal crime:

- to endeavor to illegally intercept;
- to procure another to illegally intercept;
- to disclose information gained from an illegal interception, knowing or
- having reason to know that the information is the product of an illicit interception;
- to endeavor to knowingly disclose illegally intercepted information;
- to procure another to disclose illegally intercepted information;
- to endeavor to disclose or to disclose information:
    - knowing it was gained from a court ordered interception,
    - having acquired the information during a criminal investigation, and
    - intending to improperly obstruct a criminal investigation by the disclosure;
- to access stored e-mail communications or telephone records unlawfully;
- to use a trap and trace device or a pen register (machines that record the origin of income or the destination of outgoing calls respectively) without court approval or individual consent; or
- to abuse eavesdropping authority under the Foreign Intelligence Surveillance Act.

Violators face imprisonment for up to five years, fines of up to $250,000 ($500,000 for organizations); and civil liability to actual or liquidated damages, attorneys' fees, possibly punitive damages, and administrative or professional discipline. The products of illegal interceptions are inadmissible as evidence in either federal or state proceedings.

Procedure

Senior Justice Department officials or chief state or local prosecutors may authorize an application for court ordered wiretapping or electronic eavesdropping as part of the investigation of a list of predicate crimes. Applications and court orders authorizing interception include specifics as to the individuals and the details of the crime, the communication facilities or place where the interception is to occur, the communications to be intercepted, the identities (if known) of the person committing the offense and of the persons whose communications are to be intercepted, why alternative investigative methods would be futile or dangerous, the duration of the proposed interception, steps taken to avoid interception of innocent communications, the history of any prior interceptions, the nature of third party assistance required and the identity of those to provide it, and any additional information the judge may require.

A court may issue an order upon a finding of probable cause with respect to the offense, the suspect, the conversation, and futility or dangers associated with alternative methods. The orders are good for a maximum of 30 days, with the possibility of 30 day extensions. Intercepted communications are to be recorded and the evidence secured and placed under seal (with the possibility of copies for authorized law enforcement disclosure and use) along with the application and the court's order.

Within 90 days of the expiration of the termination of the order those whose communications have been intercepted are entitled to notice, and evidence secured through the intercept may be introduced into evidence with 10 days advance notice to the parties. Information secured through a court ordered interception may be disclosed to law enforcement or intelligence officers for the performance of their official duties and as evidence during legal proceedings.

In emergency cases involving organized crime, threats to national security, or immediate danger of death or serious injury, interceptions may be authorized by senior officials before the issuance of an order. In such cases, court approval must be sought within 48 hours and the interception abandoned and an inventory of the results turned over to the communicants, if approval is denied.

Any federal prosecutor may approve an application for a court order authorizing the interception of e-mail or other electronic communications upon probable cause of a felony and the other requirements for issuance and execution of a search warrant. With regard to stored e-mail or voice mail, communications in remote storage, and telephone and service provider records, government officials may gain access to electronic communications in electronic storage for less than six months under a search warrant issued upon probable cause to belief a crime has been committed and the search will produce evidence of the offense.

The government must use the same procedure to acquire older communications or those stored in remote computer storage if access is to be afforded without notice to the subscriber or customer. If the government officials are willing to afford the subscriber or customer prior notice, access may be granted under a court order showing that the information sought is relevant and material to a criminal investigation or under an administrative subpoena, a grand jury subpoena, a trial subpoena, or court order. General identifying and billing information is available to the government pursuant to an administrative subpoena, a grand jury or trial subpoena, a warrant, with the consent of the subscriber or customer, or under a court order issued with a showing that information is relevant and material to a criminal investigation.

Federal government attorneys and state and local police officers may apply for a court order authorizing the installation and use of a pen register and/or a trap and trace device upon certification that the information to be produced is relevant to a pending criminal investigation.

The approval procedure under the Foreign Intelligence Surveillance Act (FISA) is the most distinctive of the wiretap-related procedures. First, its focus is different. It is designed to secure foreign intelligence information not evidence of a crime (although the prospect of securing evidence is not disqualifying as long as there is a measurable foreign intelligence purpose); it operates in a highly secretive manner; and it is conducted entirely before the judges of an independent court convened for no other purpose.

The contents of FISA surveillance application and subsequent order include the identity of the applicant and an authorizing official; particularized information concerning the facilities or locations involved in the interception and of the foreign agent or power whose communications are the target of the interception; a detailed description of the communications to be intercepted and a summary of the minimization procedures to be followed; certification that the information cannot reasonable be obtained using alternative means; whether the information relates to a foreign attack, sabotage, terrorism or foreign clandestine intelligence activities; the means of accomplishing the interception; a history of past related applications; the term of the interception; any other information the judge requests.

FISA court judges issue orders approving electronic surveillance upon a finding that the application requirements have been met and that there is probable cause to believe that the target of the interceptions is a foreign power or the agent of a foreign power and the targeted places or facilities are used by foreign powers of their agents. As in the case of law enforcement wiretapping and electronic eavesdropping, there is authority to intercept prior to approval in emergency situations, but there is also statutory authority for a foreign intelligence surveillance interception without a court order when the communications sought are limited to those among or between foreign powers or involve nonverbal communications from places under the open and exclusive control of a foreign

power. The second of these is replete with reporting requirements to Congress and the FISA court.

In addition to surveillance provisions, FISA authorizes court orders in foreign intelligence cases for physical searches, the use of pen registers and trap and trace devices, and for the release of business records and other tangible items. The physical search sections mirror those governing electronic surveillance. FISA pen register and trap and trace procedures are similar to those of their law enforcement counterparts in ECPA, but with many of the attributes of other FISA provisions. The orders may be issued either by a member of the FISA court or by a FISA magistrate upon the certification of a federal officer that the information sought is likely to be relevant to an investigation of international terrorism or clandestine intelligence activities. They allow the Attorney General to authorize emergency installation and use as long as the application for an authorizing court order is filed within 48 hours and restrict the use of any resulting evidence if an order is not subsequently granted. The provisions for use of the information acquired run parallel to those that apply to FISA surveillance and physicalsearch orders.

The USA PATRIOT Act and later the USA PATRIOT Improvement and Reauthorization Act temporarily rewrote the FISA business records procedure that expires on December 31, 2009. In its temporary form FISA orders may apply to any tangible property relevant to foreign intelligence investigation. Recipients may challenge the legality of the order and ask that its secrecy requirements be lifted or modified. As additional safeguards, Congress insisted upon the promulgation of miminization standards; established use restrictions; required the approval of senior officials for orders covering library and certain other types of records; confirmed and reenforced reporting requirements; and directed the Justice Department's Inspector General to conduct an audit of the use of the FISA tangible item authority.

Protect America Act.

The Protect America Act (P.L. 110-55), which has since expired, granted the Attorney General and the Director of National Intelligence the power, under limited conditions, to authorize gathering foreign intelligence information, including by electronic surveillance, (for up to a year) relating to persons believed to be overseas. In order to exercise that power, the Attorney General and the Director of National Intelligence were required to certify under oath that the collection effort involved: (1) procedures reasonably calculated to assure that the information sought concerned a person outside the United States; (2) communications to which service providers or others had access; (3) a desire, at least in significant part, to gather foreign intelligence information; (4) accompanying minimization procedures; and (5) no electronic surveillance other than that directed at a person reasonably believed to be abroad, 50 U.S.C. 1805b(a)(expired).

That having been done or in emergency situations with their oral approval, the Attorney General and Director of National Intelligence might direct the communications providers, or others with access, to immediately assist in the gathering of the foreign intelligence information in a manner least disruptive of service to the target and under confidentiality restrictions imposed by the Attorney General and the Director of National Intelligence. The directive came with the promise of compensation at prevailing rates as well as immunity from civil liability and was enforceable through the contempt power of the FISA court. Recipients were entitled to seek judicial modification of a directive, issued contrary to the statute or otherwise unlawfully, in the FISA court under expedited procedures.

The FISA court was also tasked with the responsibility of reviewing the procedures crafted to ensure that the authority was only invoked with respect to persons reasonably believed to be found overseas. Should the court have determined that the procedures were clearly erroneous, the government was free to amend them or to appeal the determination initially to the Foreign Intelligence Surveillance Court of Review and then to the Supreme Court.

Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008 (P.L. 110-261).

P.L. 110-261 (H.R. 6304), signed July 10, 2008, addresses four FISA-related matters. First, in a manner reminiscent of the Protect America Act, it provides temporary authority to gather foreign intelligence information from or relating to overseastargets. Second, it reasserts the exclusivity of FISA and Title III/ECPA as a basis for governmental electronic surveillance. Third, it instructs the Inspectors General in various agencies to conduct a review and report to Congress on the Terrorist Surveillance Program. Fourth, it seeks to protect those who assist government surveillance activities from civil liability.

Federal Criminal Statutes Outlawing Wiretapping and Electronic Eavesdropping

Privacy: An Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping, 98-326 (December 3, 2009).

GINA MARIE STEVENS & CHARLES DOYLE, CONGRESSIONAL RESEARCH SERV., PRIVACY: AN OVERVIEW OF FEDERAL STATUTES GOVERNING WIRETAPPING AND ELECTRONIC EAVESDROPPING, 98-326 (2009), *available at* http://www.intelligencelaw.com/library/secondary/crs/pdf/98-326_12-3-2009.pdf.

Gina Marie Stevens
Legislative Attorney

Charles Doyle
Senior Specialist in American Public Law

December 3, 2009

Congressional Research Service

7-5700
www.crs.gov
98-326

Summary

This report provides an overview of federal law governing wiretapping and electronic eavesdropping. It also appends citations to state law in the area and contains a bibliography of legal commentary as well as the text of the Electronic Communications Privacy Act (ECPA) and the Foreign Intelligence Surveillance Act (FISA).

It is a federal crime to wiretap or to use a machine to capture the communications of others without court approval, unless one of the parties has given their prior consent. It is likewise a federal crime to use or disclose any information acquired by illegal wiretapping or electronic eavesdropping. Violations can result in imprisonment for not more than five years; fines up to $250,000 (up to $500,000 for organizations); in civil liability for damages, attorneys' fees and possibly punitive damages; in disciplinary action against any attorneys involved; and in suppression of any derivative evidence. Congress has created separate but comparable protective schemes for electronic communications (e.g., e-mail) and against the surreptitious use of telephone call monitoring practices such as pen registers and trap and trace devices.

Each of these protective schemes comes with a procedural mechanism to afford limited law enforcement access to private communications and communications records under conditions consistent with the dictates of the Fourth Amendment. The government has been given narrowly confined authority to engage in electronic surveillance, conduct physical searches, install and use pen registers and trap and trace devices for law enforcement purposes under the Electronic Communications Privacy Act and for purposes of foreign intelligence gathering under the Foreign Intelligence Surveillance Act. Two FISA provisions, born in the USA PATRIOT Act and dealing with roving wiretaps (section 206) and business records (section 215), are scheduled to expire on December 31, 2009.

This report includes a brief summary of the expired Protect America Act, P.L. 110-55 and of the Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, P.L. 110-261 (H.R. 6304). It is available in an abridged form without footnotes, quotations, or appendices as CRS Report 98-327, *Privacy: An Abbreviated Outline of Federal Statutes Governing Wiretapping and Electronic Eavesdropping*, by Gina Stevens and Charles Doyle.

Introduction

Depending on one's perspective, wiretapping and electronic eavesdropping are either "dirty business," essential law enforcement tools, or both. This is a very general overview of the federal statutes that proscribe wiretapping and electronic eavesdropping and of the procedures they establish for law enforcement and foreign intelligence gathering purposes. Although the specifics of state law are beyond the scope of this report, citations to related state statutory provisions have been appended. The text of pertinent federal statutes and a selected bibliography of legal materials appear as appendices as well.[2364]

[2364] Portions of this report draw upon a series of earlier reports, no longer available, entitled: Wiretapping and Electronic Surveillance: A Brief Discussion of Pertinent Supreme Court Cases, A Summary and Compilation of Federal State Statutes, and a Selected Legal Bibliography (1970); Wiretapping and Electronic Surveillance: A Brief Discussion of Pertinent Supreme Court Cases, A Summary and Compilation of Federal State Statutes, and a Selected Legal Bibliography (1971); Wiretapping and Electronic Surveillance: Federal and State Statutes (1974); Taps and Bugs: A Compilation of Federal and State Statutes Governing the Interception of Wire and Oral Communications (1981); The Interception of Communications: A Legal Overview of Bugs and Taps (1988); Wiretapping & Electronic Surveillance: The Electronic Communications Privacy Act and Related Matters (1992); Taps, Bugs & Telephony: An Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping (1998); Privacy: An Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping (2001); id. (2003); id. (2006).

As used in this report "electronic eavesdropping" refers to the use of hidden microphones, recorders and any other mechanical or electronic means of capturing ongoing communications, other than wiretapping (tapping into telephone conversations). In previous versions of this report and other earlier writings, it was common to use a more neutral, and consequently preferred, term – electronic surveillance – at least when referring to law enforcement use. Unfortunately, continued use of the term "electronic surveillance" rather than "electronic eavesdropping" risks

Background

At common law, "eavesdroppers, or such as listen under walls or windows, or the eaves of a house, to hearken after discourse, and thereupon to frame slanderous and mischievous tales, are a common nuisance and presentable at the court-leet; or are indictable at the sessions, and punishable by fine and finding of sureties for [their] good behavior."[2365] Although early American law proscribed common law eavesdropping, the crime was little prosecuted and by the late nineteenth century had "nearly faded from the legal horizon."[2366] With the invention of the telegraph and telephone, however, state laws outlawing wiretapping or indiscretion by telephone and telegraph operators preserved the spirit of the common law prohibition in this country.

Congress enacted the first federal wiretap statute as a temporary measure to prevent disclosure of government secrets during World War I.[2367] Later, it proscribed intercepting and divulging private radio messages in the Radio Act of

---

confusion with forms of surveillance that either have individualistic definitions (e.g., "electronic surveillance" under the Foreign Intelligence Surveillance Act, 50 U.S.C. 1801(f)), that involve surveillance that does not capture conversation (e.g., thermal imaging or electronic tracking devices), or that may or may not capture conversation (e.g., the coverage of video surveillance depends upon the circumstances and the statutory provision question).

Related developments are discussed in CRS Report RL30465, The Foreign Intelligence Surveillance Act: An Overview of the Statutory Framework and U.S. Foreign Intelligence Surveillance Court and U.S. Foreign Intelligence Surveillance Court of Review Decisions, by Elizabeth B. Bazan; CRS Report 97-1025, Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws, by Charles Doyle; CRS Report RL30677, Digital Surveillance: The Communications Assistance for Law Enforcement Act, by Patricia Moloney Figliola; and CRS Report RL34409, Selected Laws Governing the Disclosure of Customer Phone Records by Telecommunications Carriers, by Kathleen Ann Ruane.

[2365] 4 BLACKSTONE, COMMENTARIES ON THE LAWS OF ENGLAND, 169 (1769).

[2366] "Eavesdropping is indictable at the common law, not only in England but in our states. It is seldom brought to the attention of the courts, and our books contain too few decisions upon it to enable an author to define it with confidence. . . . It never occupied much space in the law, and it has nearly faded from the legal horizon." 1 BISHOP, COMMENTARIES ON THE CRIMINAL LAW, 670 (1882).

[2367] 40 Stat.1017-18 (1918)("whoever during the period of governmental operation of the telephone and telegraph systems of the United States . . . shall, without authority and without the knowledge and consent of the other users thereof, except as may be necessary for operation of the service, tap any telegraph or telephone line . . . or whoever being employed in any such telephone or telegraph service shall divulge the contents of any such telephone or telegraph message to any person not duly authorized or entitled the receive the same, shall be fined not exceeding $1,000 or imprisoned for not more than one year or both"); 56 Cong.Rec. 10761-765 (1918).

1927,[2368] but did not immediately reestablish a federal wiretap prohibition. By the time of the landmark Supreme Court decision in Olmstead, however, at least forty-one of the forty-eight states had banned wiretapping or forbidden telephone and telegraph employees and officers from disclosing the content of telephone or telegraph messages or both.[2369]

Olmstead was a Seattle bootlegger whose Prohibition Act conviction was the product of a federal wiretap. He challenged his conviction on three grounds, arguing unsuccessfully that the wiretap evidence should have been suppressed as a violation of either his Fourth Amendment rights, his Fifth Amendment privilege against self-incrimination, or the rights implicit in the Washington state statute that outlawed wiretapping.

For a majority of the Court, writing through Chief Justice Taft, Olmstead's Fourth Amendment challenge was doomed by the absence of "an official search and seizure of his person, or such a seizure of his papers or his tangible material effects, or an actual physical invasion of his house or curtilage[2370] for the purposes of making a seizure."[2371]

[2368] 44 Stat. 1172 (1927)(". . . no person not being authorized by the sender shall intercept any message and divulge or publish the contents, substance, purpose, effect, or meaning of such intercepted message to any person . . .").

[2369] Olmstead v. United States, 277 U.S. 438, 479-80 n.13 (1928)(Brandeis, J., dissenting). Olmstead is remembered most today for the dissents of Holmes and Brandeis, but for four decades it stood for the view that the Fourth Amendment's search and seizure commands did not apply to government wiretapping accomplished without a trespass onto private property.

[2370] Curtilage originally meant the land and buildings enclosed by the walls of a castle; in later usage it referred to the barns, stables, garden plots and the like immediately proximate to a dwelling; it is understood in Fourth Amendment parlance to describe that area which "harbors those intimate activities associated with domestic life and the privacies of the home," United States v. Dunn, 480 U.S. 294, 301 n.4 (1987).

[2371] 277 U.S. at 466. Olmstead had not been compelled to use his phone and so the Court rejected his Fifth Amendment challenge. 277 U.S.C. at 462. Any violation of the Washington state wiretap statute was thought insufficient to warrant the exclusion of evidence, 277 U.S. at 466-68. Justice Holmes in his dissent tersely characterized the conduct of federal wiretappers as "dirty business," 277 U.S. at 470. The dissent of Justice Brandeis observed that the drafters of the Constitution "conferred as against the Government, the right to be let alone – the most comprehensive of rights and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the Government against privacy of the individual whatever the means employed, must be deemed in violation of the Fourth Amendment," 277 U.S. at 478-79.

Chief Justice Taft pointed out that Congress was free to provide protection which the Constitution did not.[2372] Congress did so in the 1934 Communications Act by expanding the Radio Act's proscription against intercepting and divulging radio communications so as to include intercepting and divulging radio or wire communications.[2373]

The Federal Communications Act outlawed wiretapping, but it said nothing about the use of machines to surreptitiously record and transmit face to face conversations.[2374] In the absence of a statutory ban the number of surreptitious recording cases decided on Fourth Amendment grounds surged and the results began to erode Olmstead's underpinnings.[2375]

Erosion, however, came slowly. Initially the Court applied Olmstead's principles to the electronic eavesdropping cases. Thus, the use of a dictaphone to secretly overhear a private conversation in an adjacent office offended no Fourth Amendment precipes because no physical trespass into the office in which the conversation took place had occurred.[2376] Similarly, the absence of a physical trespass precluded Fourth Amendment coverage of the situation where a federal agent secretly recorded his conversation with a defendant held in a commercial laundry in an area open to the public.[2377] On the other hand, the Fourth Amendment did reach the government's physical intrusion upon private property during an investigation, as for example when they drove a "spike mike" into the

---

[2372] "Congress may of course protect the secrecy of telephone messages by making them, when intercepted inadmissible in evidence in federal criminal trials, by direct legislation," 277 U.S. at 465.

[2373] 48 Stat. 1103-104 (1934), 47 U.S.C. 605 (1940 ed.). The Act neither expressly condemned law enforcement interceptions nor called for the exclusion of wiretap evidence, but it was read to encompass both, Nardone v. United States, 302 U.S. 379 (1937); Nardone v. United States, 308 U.S. 321 (1939).

[2374] Section 605 did ban the interception and divulgence of radio broadcasts but it did not reach the radio transmission of conversations that were broadcast unbeknownst to all of the parties to the conversation. Late in the game, the FCC supplied a partial solution when it banned the use of licensed radio equipment to overhear or record private conversation without the consent of all the parties involved in the conversation, 31 Fed.Reg. 3400 (March 4, 1966), amending then 47 C.F.R. §§2.701, 15.11. The FCC excluded "operations of any law enforcement offices conducted under lawful authority," id.

[2375] The volume of all Fourth Amendment cases calling for Supreme Court review increased dramatically after Mapp v. Ohio, 367 U.S. 643 (1961), acknowledged the application of the Fourth Amendment exclusionary rule to the states.

[2376] Goldman v. United States, 316 U.S. 129 (1942).

[2377] On Lee v. United States, 343 U.S. 747 (1952).

common wall of a row house until it made contact with a heating duct for the home in which the conversation occurred.[2378]

The spike mike case presented something of a technical problem, because there was some question whether the spike mike had actually crossed the property line of the defendant's town house when it made contact with the heating duct. The Court declined to rest its decision on the technicalities of local property law, and instead found that the government's conduct had intruded upon privacy of home and hearth in a manner condemned by the Fourth Amendment.[2379]

Each of these cases focused upon whether a warrantless trespass onto private property had occurred, that is, whether the means of conducting a search and seizure had been so unreasonable as to offend the Fourth Amendment. Yet in each case, the object of the search and seizure had been not those tangible papers

---

[2378] Silverman v. United States, 365 U.S. 505 (1961).

[2379] "The absence of a physical invasion of the petitioner's premises was also a vital factor in the Court's decision in Olmstead v. United States . . . . In holding that the wiretapping there did not violate the Fourth Amendment, the Court noted that the insertions were made without trespass upon any property of the defendants. They were made in the basement of the large office building. The taps from house lines were made in the streets near the houses. 277 U.S. at 457. There was no entry of the houses or offices of the defendants. 277 U.S. at 464. Relying upon these circumstances, the Court reasoned that the intervening wires are not part of (the defendant's) house or office any more than are the highways along which they are stretched. 277 U.S. at 465. "Here, by contrast, the officers overheard the petitioners' conversations only by usurping part of the petitioners' house or office – a heating system which was an integral part of the premises occupied by the petitioners, a usurpation that was effected without their knowledge and without their consent. In these circumstances we need not pause to consider whether or not there was a technical trespass under the local property law relating to party walls. Inherent Fourth Amendment rights are not inevitably measurable in terms of ancient niceties of tort or real property law . . . .

"The Fourth Amendment, and the personal rights which it secures, have a long history. At the very core stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion . . . This Court has never held that a federal officer may without warrant and without consent physically entrench into a man's office or home, there secretly observe or listen, and relate at the man's subsequent criminal trial what was seen or heard.

"A distinction between the dictaphone employed in Goldman and the spike mike utilized here seemed to the Court of Appeals too fine a one to draw. The court was unwilling to believe that the respective rights are to be measured in fractions of inches. But decision here does not turn upon the technicality of a trespass upon a party wall as a matter of local law. It is based upon the reality of an actual intrusion into a constitutionally protected area. What the Court said long ago bears repeating now: It may be that it is the obnoxious thing in its mildest and least repulsive form; but illegitimate and unconstitutional practices get their first footing in that way, namely, by silent approaches and slight deviations from legal modes of procedure. Boyd v. United States, 116 U.S. 616, 635. We find no occasion to reexamine Goldman here, but we decline to go beyond it, by even a fraction of an inch," 365 U.S. at 510-12 (internal quotation marks omitted).

or effects for which the Fourth Amendment's protection had been traditionally claimed, but an intangible, a conversation. This enlarged view of the Fourth Amendment could hardly be ignored, for "[i]t follows from . . . Silverman . . . that the Fourth Amendment may protect against the overhearing of verbal statements as well as against the more traditional seizure of papers and effects."[2380]

Soon thereafter the Court repudiated the notion that the Fourth Amendment's protection was contingent upon some trespass to real property in Katz v. United States.[2381] Katz was a bookie convicted on the basis of evidence gathered by an electronic listening and recording device set up outside the public telephone booth that Katz used to take and place bets. The Court held that the gateway for Fourth Amendment purposes stood at that point where an individual should to able to expect that his or her privacy would not be subjected to unwarranted governmental intrusion.[2382]

One obvious consequence of Fourth Amendment coverage of wiretapping and other forms of electronic eavesdropping is the usual attachment of the Amendment's warrant requirement. To avoid constitutional problems and at the same time preserve wiretapping and other forms of electronic eavesdropping as a law enforcement tool, some of the states established a statutory system under which law enforcement officials could obtain a warrant, or equivalent court order, authorizing wiretapping or electronic eavesdropping.

The Court rejected the constitutional adequacy of one of the more detailed of these state statutory schemes in *Berger v. New York*.[2383] The statute was found deficient because of its failure to require:

- a particularized description of the place to be searched;

[2380] Wong Sun v. United States, 371 U.S. 471, 485 (1963).

[2381] 389 U.S. 347 (1967).

[2382] "We conclude that the underpinnings of Olmstead and Goldman have been so eroded by our subsequent decisions that the trespass doctrine there enunciated can no longer be regarded as controlling. The Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a search and seizure within the meaning of the Fourth Amendment. The fact that the electronic device employed to achieve that end did not happen to penetrate the wall of the booth can have no constitutional significance." Later courts seem to prefer the "expectation of privacy" language found in Justice Harlan's concurrence: "My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as reasonable," 389 U.S. at 361.

[2383] 388 U.S. 41 (1967).

- a particularized description of the crime to which the search and seizure related;
- a particularized description of the conversation to be seized;
- limitations to prevent general searches;
- termination of the interception when the conversation sought had been seized;
- prompt execution of the order;
- return to the issuing court detailing the items seized; and
- any showing of exigent circumstances to overcome the want of prior notice.[2384]

Berger helped persuade Congress to enact Title III of the Omnibus Crime Control and Safe Streets Act of 1968, a comprehensive wiretapping and electronic eavesdropping statute that not only outlawed both activities in general terms but that also permitted federal and state law enforcement officers to use them under strict limitations designed to meet the objections in *Berger*.[2385]

A decade later another Supreme Court case persuaded Congress to supplement Title III with a judicially supervised procedure for the use of wiretapping and electronic eavesdropping in foreign intelligence gathering situations. When Congress passed Title III there was some question over the extent of the President's inherent powers to authorize wiretaps – without judicial approval – in national security cases. As a consequence, the issue was simply removed from the Title III scheme.[2386] After the Court held that the President's inherent powers were insufficient to excuse warrantless electronic eavesdropping on purely domestic threats to national security,[2387] Congress considered it prudent to augment the foreign intelligence gathering authority of the United States with the Foreign Intelligence Security Act of 1978 (FISA).[2388] The FISA provides a procedure for judicial review and authorization or denial of wiretapping and other forms of electronic eavesdropping for purposes of foreign intelligence gathering.

[2384] 388 U.S. at 58-60.

[2385] 87 Stat. 197, 18 U.S.C. 2510 - 2520 (1970 ed.).

[2386] 18 U.S.C. 2511(3)(1970 ed.)("Nothing contained in this chapter or in section 605 of the Communications Act . . . shall limit the constitutional power of the President to take such measures as he deems necessary to protect the Nation against actual or potential attack or other hostile acts of a foreign power, to obtain foreign intelligence information deemed essential to the security of the United States, or to protect national security information against foreign intelligence activities. . .").

[2387] United States v. United States District Court, 407 U.S. 297 (1972).

[2388] 92 Stat. 1783, 50 U.S.C. 1801-1862.

In 1986, Congress recast Title III in the Electronic Communications Privacy Act (ECPA).[2389] The Act followed the general outline of Title III with adjustments and additions. Like Title III, it sought to strike a balance between the interests of privacy and law enforcement, but it also reflected a Congressional desire to avoid unnecessarily crippling infant industries in the fields of advanced communications technology.[2390] ECPA also included new protection and law enforcement access provisions for stored wire and electronic communications and transactional records access (e-mail and phone records),[2391] and for pen registers as well as trap and trace devices (devices for recording the calls placed to or from a particular telephone).[2392]

Over the years, Congress has adjusted the components of Title III/ECPA or FISA. Sometimes in the interests of greater privacy; sometimes in the interest of more effective law enforcement or foreign intelligence gathering. In the last decade, for instance, Congress amended the basic statutes in:

- the USA PATRIOT Act;[2393]
- the Intelligence Authorization Act for Fiscal Year 2002;[2394]
- the 21st Century Department of Justice Appropriations Authorization Act;[2395]
- the Department of Homeland Security Act;[2396]
- the USA PATRIOT Improvement and Reauthorization Act;[2397] and

---

[2389] 92 Stat. 1783, 50 U.S.C. 1801-1862.

[2390] H.Rept. 99-647, at 18-9 (1984); S.Rept. 99-541, at 5 (1986).

[2391] 18 U.S.C. 2701-2710.

[2392] 18 U.S.C. 3121-3126. These provisions were also grounded in Supreme Court jurisprudence. In United States v. Miller, 425 U.S. 435, 441-43 (1976), the Court held that a customer had no Fourth Amendment protected expectation of privacy in the records his bank maintained concerning his transactions with them. These third party records were therefore available to the government under a subpoena duces tecum rather than a more narrowly circumscribed warrant, 425 U.S. 44-45. In Smith v. Maryland, 442 U.S. 735, 741-46 (1979), it held that no warrant was required for the state's use of a pen register or trap and trace device which merely identified the telephone numbers for calls made and received from a particular telephone. No Fourth Amendment search or seizure occurred, the Court held, since the customer had no justifiable expectation of privacy in such information which he knew or should know that the telephone company might ordinarily capture for bill or service purposes, id.

[2393] P.L. 107-56, 115 Stat. 272 (2001).

[2394] P.L. 107-108, 115 Stat. 1394 (2001).

[2395] P.L. 107-273, 116 Stat. 1758 (2002).

[2396] P.L. 107-296, 116 Stat. 2135 (2002).

- the Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008 (P.L. 110-261).[2398]

Prohibitions

Unless otherwise provided, Title III/ECPA outlaws wiretapping and electronic eavesdropping; possession of wiretapping or electronic eavesdropping equipment; use or disclosure of information obtained through illegal wiretapping or electronic eavesdropping; and disclosure of information secured through court-ordered wiretapping or electronic eavesdropping, in order to obstruct justice, 18 U.S.C. 2511. Elsewhere, federal law proscribes:

- unlawful access to stored communications, 18 U.S.C. 2701;
- unlawful use of a pen register or a trap and trace device, 18 U.S.C. 3121; and
- abuse of eavesdropping and search authority or unlawful disclosures under the Foreign Intelligence Surveillance Act, 50 U.S.C. 1809, 1827.

Illegal Wiretapping and Electronic Eavesdropping

At the heart of Title III/ECPA lies the prohibition against illegal wiretapping and electronic eavesdropping, 18 U.S.C. 2511(1), that bans:

- any person from
- intentionally
- intercepting, or endeavoring to intercept,
- wire, oral or electronic communications
- by using an electronic, mechanical or other device
- unless the conduct is specifically authorized or expressly not covered, e.g.
    - one of the parties to the conversation has consent to the interception
    - the interception occurs in compliance with a statutorily authorized, (and ordinarily judicially supervised) law enforcement or foreign intelligence gathering interception,
    - the interception occurs as part of providing or regulating communication services,
    - certain radio broadcasts, and
    - in some places, spousal wiretappers.

Person

[2397] P.L. 109-177, 120 Stat. 192 (2006).

[2398] P.L. 110-261, 122 Stat. 2436 (2008).

The prohibition applies to "any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation."[2399]

Intentional

Conduct can only violate Title III/ECPA if it is done "intentionally," inadvertent conduct is no crime; the offender must have done on purpose those things which are outlawed.[2400] He need not be shown to have known, however, that his conduct was unlawful.[2401]

Jurisdiction

Section 2511(1) contains two interception bars – one, 2511(1)(a), simply outlaws intentional interception; the other, 2511(1)(b), outlaws intentional interception when committed under any of five jurisdictional circumstances with either an implicit or explicit nexus to interstate or foreign commerce.[2402] Congress adopted the approach because of concern that its constitutional authority might not be sufficient to ban instances of electronic surveillance that bore no discernable connection to interstate commerce or any other of the enumerated powers. So it

---

[2399] 18 U.S.C. 2510(6). Although the governmental entities are not subject to criminal liability, as noted infra, some courts believe them subject to civil liability under 18 U.S.C. 2520.

[2400] "In order to underscore that the inadvertent reception of a protected communication is not a crime, the subcommittee changed the state of mind requirement under Title III of the Omnibus Crime Control and Safe Streets Act of 1968 from 'willful' to 'intentional,'" S.Rept. 541, at. 23 (1986); "This provision makes clear that the inadvertent interception of a protected communication is not unlawful under this Act," H.Rept. 99-647, at 48-9 (1986). See, e.g., In re Pharmatrak, Inc., 329 F.3d 9, 23 (1st Cir. 2003); Sanders v. Robert Bosch Corp., 38 F.3d 736, 742-43 (4th Cir. 1994); Lonegan v. Hasty, 436 F.Supp.2d 419, 429 (E.D.N.Y. 2006).

[2401] Narducci v. Village of Bellwood, 444 F.Supp. 924, 835 (N.D. Ill. 2006).

[2402] "(1) Except as otherwise specifically provided in this chapter any person who – (a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;

"(b) intentionally uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when – (I) such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication; or (ii) such device transmits communications by radio, or interferes with the transmission of such communication; or (iii) such person knows, or has reason to know, that such device or any component thereof has been sent through the mail or transported in interstate or foreign commerce; or (iv) such use or endeavor to use (A) takes place on the premises of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or (B) obtains or is for the purpose of obtaining information relating to the operations of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or (v) such person acts in the District of Columbia, the Commonwealth of Puerto Rico, or any territory or possession of the United States," 18 U.S.C. 2511(1)(a),(b).

enacted a general prohibition, and as a safety precaution, a second provision more tightly tethered to specific jurisdictional factors.[2403] The Justice Department has honored that caution by employing subparagraph (b) to prosecute the interception of oral communications, while using subparagraph (a) to prosecute other forms of electronic eavesdropping.[2404]

Interception

Interception "means the aural or other acquisition of the contents" of various kinds of communications by means of "electronic, mechanical or other devices."[2405] The definition raises questions of where, when, what, and how. Although logic might suggest that interception occurs only in the place where the communication is captured, the cases indicate that interception occurs as well where the communication begins, is transmitted, or is received.[2406]

Once limited to aural acquisitions, ECPA enlarged the definition by adding the words "or other acquisition" so that it is no longer limited to interceptions of

---

[2403] "Subparagraph (a) establishes a blanket prohibition against the interception of wire communication. Since the facilities used to transmit wire communications form part of the interstate or foreign communications network, Congress has plenary power under the commerce clause to prohibit all interception of such communications whether by wiretapping or otherwise.

"The broad prohibition of subparagraph (a) is also applicable to the interception of oral communications. The interception of such communications, however, does not necessarily interfere with the interstate or foreign commerce network, and the extent of the constitutional power of Congress to prohibit such interception is less clear than in the case of interception of wire communications. . . .

"Therefore, in addition to the broad prohibitions of subparagraph (a), the committee has included subparagraph (b), which relies on accepted jurisdictional bases under the commerce clause, and other provisions of the Constitution to prohibit the interception of oral communications," S.Rept. 90-1097, at 91-2 (1968).

[2404] DEPARTMENT OF JUSTICE CRIMINAL RESOURCE MANUAL at 1050. As will be noted in moment, the statutory definitions of wire and electronic communications contain specific commerce clause elements, but the definition of oral communications does not. Subsequent Supreme Court jurisprudence relating to the breadth of Congress' commerce clause powers indicates that the precautions may have been well advised, United States v. Lopez, 514 U.S. 549 (1995) and United States v. Morrison, 529 U.S. 598 (2000).

[2405] 18 U.S.C. 2510(4). The dictionary definition of "aural" is "of or relating to the ear or to the sense of hearing," MERRIAM-WEBSTER'S COLLEGIATE DICTIONARY 76 (10th ed. 1996).

[2406] United States v. Luong, 471 F.3d 1107, 1109 (9th Cir. 2006)("an interception occurs where the tapped phone is located and where the law enforcement officers first overheard the call . . . United States v. Rodriguez, 968 F.2d 130, 136 (2d Cir. 1992); accord United States v. Ramirez, 112 F.3d 849, 852 (7the Cir. 1997)(concluding that an interception occurs in the jurisdiction where the tapped phone is located, where the second phone in the conversation is located, and where the scanner used to overhear the call is located); United States v. Denman, 100 F.3d 399, 403 (5th Cir. 1996)").

communications that can be heard.[2407] The change complicates the question of whether the wiretap, stored communications, or trap and trace portions of the ECPA govern the legality of various means of capturing information relating to a communication. The analysis might seem to favor wiretap coverage when it begins with an examination of whether an "interception" has occurred. Yet, there is little consensus over when an interception occurs; that is, whether "interception" as used in section 2511 contemplates only surreptitious acquisition, contemporaneous with transmission, or whether such acquisition may occur anytime before the initial cognitive receipt of the contents by the intended recipient.[2408]

The USA PATRIOT Act resolved some of the uncertainty when it removed voice mail from the wiretap coverage of Title III (striking the phrase "and such term includes any electronic storage of such communication" from the definition of "wire communications" in Title III (18 U.S.C. 2510(1)) and added stored wire communications to the stored communications coverage of 18 U.S.C. 2703.[2409]

As for the "what," the interceptions proscribed in Title III are confined to those that capture a communication's content. Trap and trace devices and pen registers once captured only information relating to the source and addressee of a

---

[2407] S.Rept. 99-541, at 13 (1986)(the "amendment clarifies that it is illegal to intercept the non-voice portion of a wire communication. For example, it is illegal to intercept the data or digitized portion of a voice communication"); see also H.Rept. 99-647, at 34 (1986).

[2408] United States v. Smith, 155 F.3d 1051, 1058 (9th Cir. 1998)(unauthorized retrieval and recording of another's voice mail messages constitutes an "interception"); Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 878 (9th Cir. 2002)(fraudulent access to stored communication does not constitute an "interception"; interception requires access contemporaneous with transmission); United States v. Councilman, 418 F.3d 67, 79-80(1st Cir. 2005)(en banc)(service provider's access to e-mail "during transient storage" constitutes "interception"; without deciding whether "interception is limited to acquisition contemporaneous with transmission"); United States v. Jones, 451 F.Supp.2d 71, 75 (D.D.C. 2006)(government's acquisition from the phone company of text messages was no interception because there was no contemporaneous access); Fraser v. National Mutual Insurance Co., 135 F.Supp.2d 623, 634-37 (E.D.Pa. 2001) ("interception" of e-mail occurs with its unauthorized acquisition prior to initial receipt by its addressee); Steve Jackson Games, Inc. v. United States Secret Service, 36 F.3d 457, 461-62n.7 (5th Cir. 1994) (Congress did not intend for "interception" to apply to e-mail stored on an electronic bulletin board; stored wire communications (voice mail), however, is protected from "interception"); United States v. Meriwether, 917 F.2d 955, 959-60 (6th Cir. 1990)(access to stored information through the use of another's pager does not constitute an "interception"); United States v. Reyes, 922 F.Supp. 818, 836-37 (S.D.N.Y. 1996)(same); Wesley College v. Pitts, 947 F.Supp. 375, 385 (D.Del. 1997)(no "interception" occurs when the contents of electronic communications are acquired unless contemporaneous with their transmission); Cardinal Health 414, Inc.v. Adams, 582 F.Supp.2d 967, 979-81 (M.D. Tenn. 2008)(same); see also, Adams v. Battle Creek, 250 F.3d 980, 982 (6th Cir. 2001)(use of a "clone" or duplicate pager to simultaneously receive the same message as a target pager is an "interception"); Brown v. Waddell, 50 F.3d 285, 294 (4th Cir. 1995)(same).

[2409] 115 Stat. 283 (2001).

communication, not its content. That is no longer the case. The "post-cut-through dialed digit features" of contemporary telephone communications now transmit communications in such a manner that the use of ordinary pen register or trap and trace devices will capture both non-content and content.[2410] As a consequence, a few courts have held, either as a matter of statutory construction or constitutional necessity, that the authorities must rely on a Title III wiretap order rather than a pen register/trap and trace order if such information will be captured.[2411]

By Electronic, Mechanical, or Other Device

The statute does not cover common law "eavesdropping," but only interceptions "by electronic, mechanical or other device."[2412] That phrase is in turn defined so as not to include hearing aids or extension telephones in normal use.[2413] Whether an extension phone has been installed and is being used in the ordinary course of business or in the ordinary course of law enforcement duties, so that it no longer constitutes an interception device for purposes of Title III/ECPA and comparable state laws has proven a somewhat vexing question.[2414]

[2410] "'Post-cut-through dialed digits' are any numbers dialed from a telephone after the call is initially setup or 'cutthrough.' Sometimes these digits are other telephone numbers, as when a party places a credit card call by first dialing the long distance carrier access number and then the phone number of the intended party. Sometimes these digits transmit real information, such as bank account numbers, Social Security numbers, prescription numbers, and the like. In the latter case, the digits represent communications content; in the former, they are non-content call processing numbers," In re United States, 441 F.Supp.2d 816, 818 (S.D. Tex. 2006).

[2411] In re United States for Orders (1) Authorizing Use of Pen Registers and Trap and Trace Devices, 515 F.Supp.2d 325, 328-38 (E.D.N.Y. 2007); In re United States, 441 F.Supp.2d 816, 818-27 (S.D. Tex. 2006).

[2412] 18 U.S.C. 2510(4). United States v. Jones, 451 F.Supp.2d 71, 75 (D.D.C. 2006)(government's acquisition from the phone company of text messages was not an interception because it did not involve contemporaneous access and because no electronic, mechanical, or other devices were used).

[2413] "'[E]lectronic, mechanical, or other device' means any device or apparatus which can be used to intercept a wire, oral, or electronic communication other than – (a) any telephone or telegraph instrument, equipment or facility, or any component thereof, (i) furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business; or (ii) being used by a provider of wire or electronic communication service in the ordinary course of its business, or by an investigative or law enforcement officer in the ordinary course of his duties; (b) a hearing aid or similar device being used to correct subnormal hearing to not better than normal," 18 U.S.C. 2510(5).

[2414] See the cases cited and commentary in Barnett & Makar, "In the Ordinary Course of Business": The Legal Limits of Workplace Wiretapping, 10 HASTINGS JOURNAL OF COMMUNICATIONS AND ENTERTAINMENT LAW 715 (1988); Application to Extension Telephones of Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (18 U.S.C.

Although often intertwined with the consent exception discussed below, the question generally turns on the facts in a given case.[2415] When the exemption is claimed as a practice in the ordinary course of business, the interception must be for a legitimate business reason, it must be routinely conducted, and at least in some Circuits employees must be notified that their conversations are being monitored.[2416] Similarly, "Congress most likely carved out an exception for law enforcement officials to make clear that the routine and almost universal recording of phone lines by police departments and prisons, as well as other law enforcement institutions, is exempt from the statute."[2417] The exception contemplates administrative rather than investigative monitoring,[2418] which must nevertheless be justified by a lawful, valid law enforcement concern.[2419]

---

§§2510 et seq.), Pertaining to Interceptions of Wire Communications, 58 ALR Fed. 594; Eavesdropping on Extension Telephone as Invasion of Privacy, 49 ALR 4th 430.

[2415] E.g., Deal v. Spears, 780 F.Supp. 618, 623 (W.D.Ark. 1991), aff'd, 980 F.2d 1153 (8th Cir. 1992)(employer regularly taped employee calls by means of a device attached to an extension phone; most of the calls were personal and recording and disclosing them served no business purpose).

[2416] Adams v. Battle Creek, 250 F.3d 980, 983 (6th Cir. 2001); Arias v. Mutual Central Alarm Service, 202 F.3d 553, 558 (2d Cir. 2000); Berry v. Funk, 146 F.3d 1003, 1008 (D.C.Cir. 1998); Sanders v. Robert Bosch Corp., 38 F.3d 736, 741 (4th Cir. 1994). See also, Hall v. Earthlink Network Inc., 396 F.3d 500, 503-04 (2d Cir. 2005) (Internet service provider's receipt and storage of former customer's e-mail after termination of the customer's account was done in ordinary course of business and consequently did not constitute an interception). Some courts include surreptitious, extension phone interceptions conducted within the family home as part of the "business extension" exception, Anonymous v. Anonymous, 558 F.2d 677, 678-79 (2d Cir. 1977); Scheib v. Grant, 22 F.3d 149, 154 (7th Cir. 1994); Newcomb v. Ingle, 944 F.2d 1534, 1536 (10th Cir. 1991); contra, United States v. Murdock, 63 F.3d 1391, 1400 (6th Cir. 1995).

[2417] Adams v. Battle Creek, 250 F.3d at 984; see also, United States v. Lewis, 406 F.3d 11, 18 (1st Cir. 2005); United States v. Hammond, 286 F.3d 189, 192 (4th Cir. 2002); Smith v. U.S.Dept. of Justice, 251 F.3d 1047, 1049-50 (D.C.Cir. 2001); United States v. Poyck, 77 F.3d 285, 292 (9th Cir. 1996); United States v. Daniels, 902 F.2d 1238, 1245 (7th Cir. 1990); United States v. Paul, 614 F.2d 115, 117 (6th Cir. 1980).

[2418] Amati v. Woodstock, 176 F.3d 952, 955 (7th Cir. 1999)("Investigation is within the ordinary course of law enforcement, so if 'ordinary' were read literally warrants would rarely if ever be required for electronic eavesdropping, which was surely not Congress's intent. Since the purpose of the statute was primarily to regulate the use of wiretapping and other electronic surveillance for investigatory purposes, .ordinary' should not be read so broadly; it is more reasonably interpreted to refer to routine noninvestigative recording of telephone conversations"); accord United States v. Lewis, 416 F.3d at 11 (1st Cir. 2005); Colandrea v. Orangetown, 411 F.Supp.2d 342, 347-48 (S.D.N.Y. 2007).

[2419] The exception, however, does not permit a county to record all calls in and out of the offices of county judges merely because a detention center and the judges share a common facility, Abraham v. Greenville, 237 F.3d 386, 390 (4th Cir. 2001), nor does it permit jailhouse telephone monitoring of an inmate's confession to a clergyman, Mockaitis v. Harcleroad, 104 F.3d 1522, 1530 (9th Cir. 1997). The courts are divided over whether private corrections officials are covered

Wire, Oral, or Electronic Communications

An interception can only be a violation of ECPA if the conversation or other form of communication intercepted is among those kinds which the statute protects, in oversimplified terms – telephone (wire), face to face (oral), and computer (electronic). Congress used the definitions of the three forms of communications to describe the communications beyond the Act's reach as well as those within its grasp. For example, "oral communication" by definition includes only those face to face conversations with respect to which the speakers have a justifiable expectation of privacy.[2420] Similarly, "wire communications" are limited to those that are at some point involve voice communications (i.e., only aural transfers).[2421] Radio and data transmissions are generally "electronic communications." The definition includes other forms of information transfer but excludes certain radio transmissions which can be innocently captured without great difficulty.[2422] Although it is not a federal crime to intercept radio communications under any number of conditions, the exclusion is not a matter of definition but of special general exemptions, 18 U.S.C. 2511(2)(g), discussed below.

Endeavoring to Intercept

---

by the law enforcement exception. Compare United States v. Faulkner, 323 F. Supp. 2d 1111, 1113-17 (D. Kan. 2004), aff'd on other grounds, 439 F.3d 1221 (10th Cir. 2006) (not covered) with United States v. Rivera, 292 F. Supp. 2d 838, 842-43 (E.D. Va. 2003) (covered).

[2420] "'[O]ral communication' means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication," 2510(2). Pattee v. Georgia Ports Authority, 512 F.Supp.2d 1372, 1376-377 (S.D.Ga. 2007)("the section contains two slightly different requirements: (1) that the circumstances justify an expectation that the communication is not being intercepted; and (2) that the speaker exhibits that expectation"). Note that unlike the definitions of wire and electronic communications, infra, there is no reference to interstate or foreign commerce here.

[2421] "'[W]ire communication' means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce," 18 U.S.C. 2510(1).

[2422] "'[E]lectronic communication' means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include – (A) the radio portion of a cordless telephone communication that is transmitted between the cordless handset and the base unit; (B) any wire or oral communication; (C) any communication made through a tone-only paging device; or (D) any communication from a tracking device (as defined in section 3117 of this title)," 18 U.S.C. 2510(12).

Although the statute condemns attempted wiretapping and electronic eavesdropping ("endeavoring to intercept"), 18 U.S.C. 2511(1), the provisions appear to have escaped use, interest, or comment heretofore, perhaps because the conduct most likely to constitute preparation for an interception – possession of wiretapping equipment – is already a separate crime, 18 U.S.C. 2512, discussed, infra.

Exemptions: Consent Interceptions

Consent interceptions are common, controversial and have a history all their own. The early bans on divulging telegraph or telephone messages had a consent exception.[2423] The Supreme Court upheld consent interceptions against Fourth Amendment challenge both before and after the enactment of Title III.[2424] The argument in favor of consent interceptions has always been essentially that a speaker risks the indiscretion of his listeners and holds no superior legal position simply because a listener elects to record or transmit his statements rather than subsequently memorializing or repeating them.[2425] Wiretapping or electronic eavesdropping by either the police or anyone else with the consent of at least one party to the conversation is not unlawful under the federal statute.[2426] These

---

[2423] E.g., 47 U.S.C. 605(1940 ed.).

[2424] On Lee v. United States, 343 U.S. 747 (1952); Lopez v. United States, 373 U.S. 427 (1963); United States v. White, 401 U.S. 745 (1971).

[2425] United States v. White, 401 U.S. at 751 (1971)("Concededly a police agent who conceals his police connections may write down for official use his conversations with a defendant and testify concerning them, without a warrant authorizing his encounters with the defendant and without otherwise violating the latter's Fourth Amendment rights . . . . For constitutional purposes, no different result is required if the agent instead of immediately reporting and transcribing his conversations with defendant, either (1) simultaneously records them with electronic equipment which he is carrying on his person, Lopez v. United States, supra; (2) or carries radio equipment which simultaneously transmits the conversations either to recording equipment located elsewhere or to other agents monitoring the transmitting frequency. On Lee v. United States, supra. If the conduct and revelations of an agent operating without electronic equipment do not invade the defendant's constitutionally justifiable expectations of privacy, neither does a simultaneous recording of the same conversations made by the agent or by others from transmissions received from the agent to whom the defendant is talking and whose trustworthiness the defendant necessarily risks"); Lopez v. United States 373 U.S. 427, 439 (1963)("Stripped to its essentials, petitioner's argument amounts to saying that he has a constitutional right to rely on possible flaws in the agent's memory, or to challenge the agent's credibility without being beset by corroborating evidence that is not susceptible of impeachment. For no other argument can justify excluding an accurate version of a conversation that the agent could testify to from memory. We think the risk that petitioner took in offering a bribe to Davis fairly included the risk that the offer would be accurately reproduced in court, whether by faultless memory or mechanical recording").

[2426] "(c) It shall not be unlawful under this chapter for a person acting under color of law to intercept a wire, oral, or electronic communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception.

provisions do no more than shield consent interceptions from the sanctions of federal law; they afford no protection from the sanctions of state law. Many of the states recognize comparable exceptions, but some only permit interception with the consent of all parties to a communication.[2427]

Under federal law, consent may be either explicitly or implicitly given. For instance, someone who uses a telephone other than his or her own and has been told by the subscriber that conversations over the instrument are recorded has been held to have implicitly consented to interception when using the instrument.[2428] This is not to say that subscriber consent alone is sufficient, for it is the parties to the conversation whose privacy is designed to be protected.[2429] Although consent may be given in the hopes of leniency from law enforcement officials or as an election between unpalatable alternatives, it must be freely given and not secured coercively.[2430]

Private consent interceptions may not be conducted for a criminal or tortious purpose.[2431] At one time, the limitation encompassed interceptions for criminal, tortious, or otherwise injurious purposes, but ECPA dropped the reference to injurious purposes for fear that First Amendment values might be threatened

---

"(d) It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State," 18 U.S.C. 2511(2)(c), (d).

[2427] For citations to state law, see Appendix B.

[2428] United States v. Friedman, 300 F.3d 111, 122-23 (2d Cir. 2002)(inmate use of prison phone);United States v. Faulkner, 439 F.3d 1221, 1224 (10th Cir. 2006)(same); United States v. Hammond, 286 F.3d 189, 192 (4th Cir. 2002) (same); United States v. Footman, 215 F.3d 145, 154-55 (1st Cir. 2000) (same); Griggs-Ryan v. Smith, 904 F.2d 112, 116-17 (1st Cir. 1990) (use of landlady's phone); United States v. Rivera, 292 F. Supp. 2d 838, 843-45 (E.D. Va. 2003)(inmate use of prison phone monitored by private contractors); see also, United States v. Conley, 531 F.3d 56, 589 (1st Cir. 2008)(explicit consent as a condition for phone privileges).

[2429] Anthony v. United States, 667 F.2d 870, 876 (10th Cir. 1981).

[2430] United States v. Antoon, 933 F.2d 200, 203-204 (3d Cir. 1991). But see O'Ferrell v. United States, 968 F.Supp. 1519, 1541 (M.D. Ala. 1997) (an individual who spoke to his wife on the telephone after being told by FBI agents who were then executing a search warrant at his place of business that he could only speak to her with the agents listening in consented to the interception, even if FBI's initial search was unconstitutional).

[2431] 18 U.S.C. 2511(2)(d); United States v. Lam, 271 F.Supp.2d 1182, 1183-184 (N.D.Cal. 2003).

should the clause be read to outlaw consent interceptions conducted to embarrass.[2432]

Exemptions: Publicly Accessible Radio Communications

Radio communications which can be inadvertently heard or are intended to be heard by the public are likewise exempt. These include not only commercial broadcasts, but ship and aircraft distress signals, tone-only pagers, marine radio and citizen band radio transmissions, and interceptions necessary to identify the source of any transmission, radio or otherwise, disrupting communications satellite broadcasts.[2433]

Exemptions: Government Officials

Government officials enjoy an exemption when acting under judicial authority, whether that authority is provided for in Title III/ECPA for federal and state law enforcement officers acting under a court order,[2434] acting in an emergency situation pending issuance of a court order,[2435] or in the case of communications

---

[2432] S.Rept. 99-541, at 17-8 (1986); H.Rept. 99-647, at 39-40 (1986).

[2433] "(g) It shall not be unlawful under this chapter or chapter 121 of this title for any person – (i) to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public;

"(ii) to intercept any radio communication which is transmitted – (I) by any station for the use of the general public, or that relates to ships, aircraft, vehicles, or persons in distress; (II) by any governmental, law enforcement, civil defense, private land mobile, or public safety communications system, including police and fire, readily accessible to the general public; (III) by a station operating on an authorized frequency within the bands allocated to the amateur, citizens band, or general mobile radio services; or (IV) by any marine or aeronautical communications system;

"(iii) to engage in any conduct which – (I) is prohibited by section 633 of the Communications Act of 1934; or (II) is excepted from the application of section 705(a) of the Communications Act of 1934 by section 705(b) of that Act;

"(iv) to intercept any wire or electronic communication the transmission of which is causing harmful interference to any lawfully operating station or consumer electronic equipment, to the extent necessary to identify the source of such interference; or

"(v) for other users of the same frequency to intercept any radio communication made through a system that utilizes frequencies monitored by individuals engaged in the provision or the use of such system, if such communication is not scrambled or encrypted," 18 U.S.C. 2511(2)(g).

[2434] "Except as otherwise specifically provided in this chapter any person who (a) intentionally intercepts . . . ." 18 U.S.C. 2511(1)(emphasis added).

[2435] "Notwithstanding any other provision of this chapter, any investigative or law enforcement officer, specially designated by the Attorney General, the Deputy Attorney General, the Associate

of an intruder in a communications system acting with the approval of the system provider;[2436] in the Foreign Intelligence Surveillance Act,[2437] or in the separate provisions according them the use of pen registers and trap and trace devices.[2438]

Exemptions: Communication Service Providers

There is a general exemption for those associated with supplying communications services, the telephone company, switchboard operators, and the like. The exemption not only permits improved service and lets the telephone

---

Attorney General, or by the principal prosecuting attorney of any State or subdivision thereof acting pursuant to a statute of that State, who reasonably determines that – (a) an emergency situation exists that involves – (i) immediate danger of death or serious physical injury to any person, (ii) conspiratorial activities threatening the national security interest, or (iii) conspiratorial activities characteristic of organized crime, [–] that requires a wire, oral, or electronic communication to be intercepted before an order authorizing such interception can, with due diligence, be obtained, and (b) there are grounds upon which an order could be entered under this chapter to authorize such interception, may intercept such wire, oral, or electronic communication if an application for an order approving the interception is made in accordance with this section within forty-eight hours after the interception has occurred, or begins to occur. In the absence of an order, such interception shall immediately terminate when the communication sought is obtained or when the application for the order is denied, whichever is earlier. In the event such application for approval is denied, or in any other case where the interception is terminated without an order having been issued, thecontents of any wire, oral, or electronic communication intercepted shall be treated as having been obtained in violation of this chapter, and an inventory shall be served as provided for in subsection (d) of this section on the person named in the application," 18 U.S.C. 2518(7).

[2436] "(i) It shall not be unlawful under this chapter for a person acting under color of law to intercept the wire or electronic communications of a computer trespasser transmitted to, through, or from the protected computer, if — (I) the owner or operator of the protected computer authorizes the interception of the computer trespasser's communications on the protected computer; (II) the person acting under color of law is lawfully engaged in an investigation; (III) the person acting under color of law has reasonable grounds to believe that the contents of the computer trespasser's communications will be relevant to the investigation; and (IV) such interception does not acquire communications other than those transmitted to or from the computer trespasser," 18 U.S.C. 2511(2)(i).

[2437] "(e) Notwithstanding any other provision of this title or section 705 or 706 of the Communications Act of 1934, it shall not be unlawful for an officer, employee, or agent of the United States in the normal course of his official duty to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, as authorized by that Act," 18 U.S.C. 2511(2)(e).

[2438] "(h) It shall not be unlawful under this chapter – (I) to use a pen register or a trap and trace device (as those terms are defined for the purpose of chapter 206). . . ." 18 U.S.C. 2511(2)(h). Neither the stored communications sections in chapter 121 nor the pen register and trap and trace device in chapter 206 authorize the contemporaneous interception of the contents of a communication. For the citations to state statutes permitting judicial authorization of law enforcement interception of wire, oral or electronic communications, for access to stored electronic communications, and for the use of pen registers and trap and trace devices, see Appendix D.

company protect itself against fraud,[2439] but it allows for assistance to federal and state officials operating under a judicially supervised interception order,[2440] and for the regulatory activities of the Federal Communications Commission.[2441]

[2439] "(a)(i) It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks . . .

* * *

"(h) It shall not be unlawful under this chapter . . .

"(ii) for a provider of electronic communication service to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire or electronic communication, or a user of that service, from fraudulent, unlawful or abusive use of such service," 18 U.S.C. 2511(2)(a)(I), (h).

[2440] "(ii) Notwithstanding any other law, providers of wire or electronic communication service, their officers, employees, and agents, landlords, custodians, or other persons, are authorized to provide information, facilities, or technical assistance to persons authorized by law to intercept wire, oral, or electronic communications or to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, if such provider, its officers, employees, or agents, landlord, custodian, or other specified person, has been provided with –

(A) a court order directing such assistance signed by the authorizing judge, or

(B) a certification in writing by a person specified in section 2518(7) of this title or the Attorney General of the United States that no warrant or court order is required by law, that all statutory requirements have been met, and that the specified assistance is required, setting forth the period of time during which the provision of the information, facilities, or technical assistance is authorized and specifying the information, facilities, or technical assistance required. No provider of wire or electronic communication service, officer, employee, or agent thereof, or landlord, custodian, or other specified person shall disclose the existence of any interception or surveillance or the device used to accomplish the interception or surveillance with respect to which the person has been furnished a court order or certification under this chapter, except as may otherwise be required by legal process and then only after prior notification to the Attorney General or to the principal prosecuting attorney of a State or any political subdivision of a State, as may be appropriate. Any such disclosure, shall render such person liable for the civil damages provided for in section 2520. No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, or agents, landlord, custodian, or other specified person for providing information, facilities, or assistance in accordance with the terms of a court order, statutory authorization, or certification under this chapter," 18 U.S.C. 2511(2)(a)(ii).

[2441] "(b) It shall not be unlawful under this chapter for an officer, employee, or agent of the Federal Communications Commission, in the normal course of his employment and in discharge of the monitoring responsibilities exercised by the Commission in the enforcement of chapter 5 of title 47 of the United States Code, to intercept a wire or electronic communication, or oral

Domestic Exemptions

A few courts recognize a "vicarious consent" exception under which a custodial parent may secretly record the conversations of his or her minor child in the interest of protecting the child.[2442] Although rejected by most,[2443] a handful of federal courts have held that Title III/ECPA does not preclude one spouse from wiretapping or electronically eavesdropping upon the other,[2444] a result other courts have sometimes reached through the telephone extension exception discussed above.[2445]

Consequences: Criminal Penalties

Interceptions in violation of Title III/ECPA are generally punishable by imprisonment for not more than five years and/or a fine of not more than $250,000 for individuals and not more than $500,000 for organizations.[2446] The

---

communication transmitted by radio, or to disclose or use the information thereby obtained," 18 U.S.C. 2511(2)(b).

[2442] Pollock v. Pollock, 154 F.3d 601, 611 (8th Cir. 1998); Wagner v. Wagner, 64 F.Supp. 2d 895, 889-901 (D.Minn. 1999); Campbell v. Price, 2 F.Supp. 2d 1186, 1191-192 (E.D.Ark. 1998); Thompson v. Dulaney, 838 F.Supp. 1535, 1544-45 (D.Utah 1993); cf., Babb v. Eagleton, 616 F.Supp.2d 1195, 1205-206 (N.D. Okla. 2007).

[2443] Glazner v. Glazner, 347 F.3d 1212, 1215-16 (11th Cir. 2003); Heggy v. Heggy, 944 F.2d 1537, 1539 (10th Cir. 1991); Kempf v. Kempf, 868 F.2d 970, 972 (8th Cir. 1989); Pritchard v. Pritchard, 732 F.2d 372, 374 (4th Cir. 1984); United States v. Jones, 542 F.2d 661, 667 (6th Cir. 1976); Kratz v. Kratz, 477 F.Supp. 463, 467-70 (E.D.Pa. 1979); Heyman v.Heyman, 548 F.Supp. 1041, 1045-47 (N.D.Ill.1982); Lombardo v. Lombardo, 192 F.Supp. 2d 885, 809 (N.D.Ill. 2002).

[2444] Simpson v. Simpson, 490 F.2d 803, 809 (5th Cir. 1974); Perfit v. Perfit, 693 F.Supp. 851, 854-56 (C.D.Cal. 1988); see generally, Applicability, in Civil Action, of Provisions of Omnibus Crime Control and Safe Streets Act of 1968 Prohibiting Interception of Communications (18 USCS §2511(1)), to Interception by Spouse, or Spouse's Agent, of Conversations of Other Spouse, 139 ALR Fed. 517, and the cases discussed therein.

[2445] Anonymous v. Anonymous, 558 F.2d 677, 678-79 (2d Cir. 1977); Scheib v. Grant, 22 F.3d 149, 154 (7th Cir. 1994); Newcomb v. Ingle, 944 F.2d 1534, 1536 (10th Cir. 1991); cf., Babb v. Eagleton, 616 F.Supp.2d 1195, 1203-205 (N.D. Okla. 2007); contra, United States v. Murdock, 63 F.3d 1391, 1400 (6th Cir. 1995).

[2446] "Except as provided in (b) of this subsection or in subsection (5), whoever violates subsection (1) of this section shall be fined under this title* or imprisoned not more than five years, or both." 18 U.S.C. 2511(4)(a).

* Section 3559 of title 18 classifies as a felony any offense with a maximum penalty of imprisonment of more than one year; and as a Class A misdemeanor any offense with a maximum penalty of imprisonment set at between six months and one year. Unless Congress clearly rejects the general fine ceilings it provides, section 3571 of title 18 sets the fines for felonies at not more than $250,000 for individuals and not more than $500,000 for organizations, and for class A misdemeanors at not more than $100,000 for individuals and not more than $200,000 for

same penalties apply to the unlawful capture of cell phone and cordless phone conversations, since the Homeland Security Act[2447] repealed the reduced penalty provisions that at one time applied to the unlawful interceptions using radio scanners and the like.[2448] There is a reduced penalty, however, for filching satellite communications as long as the interception is not conducted for criminal, tortious, nor mercenary purposes: unauthorized interceptions are broadly proscribed subject to an exception for unscrambled transmissions[2449] and are subject to the general five-year penalty, but interceptions for neither criminal, tortious, nor mercenary purposes subject offenders to only civil punishment.[2450] Equipment used to wiretap or eavesdrop in violation of Title III is subject to confiscation by the United States, either in a separate civil proceeding or a part of the prosecution of the offender.[2451]

---

organizations. If there is monetary loss or gain associated with the offense, the offender may alternatively be fined not more than twice the amount of the loss or gain, 18 U.S.C. 3571.

[2447] 116 Stat. 2158 (2002).

[2448] 18 U.S.C. 2511(4)(b)(2000 ed.).

[2449] "(b) Conduct otherwise an offense under this subsection that consists of or relates to the interception of a satellite transmission that is not encrypted or scrambled and that is transmitted – (i) to a broadcasting station for purposes of retransmission to the general public; or (ii) as an audio subcarrier intended for redistribution to facilities open to the public, but not including data transmissions or telephone calls, is not an offense under this subsection unless the conduct is for the purpose of direct or indirect commercial advantage or private financial gain," 18 U.S.C. 2511(4)(b).

[2450] "(5)(a)(I) If the communication is – (A) a private satellite video communication that is not scrambled or encrypted and the conduct in violation of this chapter is the private viewing of that communication and is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain; or (B) a radio communication that is transmitted on frequencies allocated under subpart D of part 74 of the rules of the Federal Communications Commission that is not scrambled or encrypted and the conduct in violation of this chapter is not for tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain, then the person who engages in such conduct shall be subject to suit by the Federal Government in a court of competent jurisdiction. (ii) In an action under this subsection – (A) if the violation of this chapter is a first offense for the person under paragraph (a) of subsection (4) and such person has not been found liable in a civil action under section 2520 of this title, the Federal Government shall be entitled to appropriate injunctive relief; and (B) if the violation of this chapter is a second or subsequent offense under paragraph (a) of subsection (4) or such person has been found liable in any prior civil action under section 2520, the person shall be subject to a mandatory $500 civil fine. "(b) The court may use any means within its authority to enforce an injunction issued under paragraph (ii)(A), and shall impose a civil fine of not less than $500 for each violation of such an injunction." 18 U.S.C. 2511(5). Under 18 U.S.C. 2520, victims may recover the greater of actual damages or statutory damages of not less than $50 and not more than $500 for the first offense; those amounts are increased to $100 and $1000 for subsequent offenses.

[2451] 18 U.S.C. 2513 ("Any electronic, mechanical, or other device used, sent, carried, manufactured, assembled, possessed, sold, or advertised in violation of section 2511 or section 2512 of this chapter may be seized and forfeited to the United States. . ."); 18 U.S.C.

In addition to exemptions previously mentioned, Title III provides a defense to criminal liability based on good faith.[2452] As noted below, the defense seems to lack sufficient breadth to shelter any offender other than a government official or someone working at their direction.

Consequences: Civil Liability

Victims of illegal wiretapping or electronic eavesdropping may be entitled to equitable relief, damages (equal to the greater of actual damages, $100 per day of violation, or $10,000),[2453] punitive damages, reasonable attorney's fees and reasonable litigation costs.[2454] A majority of federal courts hold that a court may decline to award damages, attorneys' fees and costs once a violation has been shown, but a few still consider such awards mandatory.[2455] In addition, a majority holds that governmental entities other than the United States may be liable for

---

983(a)(3)(C)("In lieu of, or in addition to, filing a civil forfeiture complaint, the Government may include a forfeiture allegation in a criminal indictment. . .").

[2452] "A good faith reliance on – (1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization; (2) a request of an investigative or law enforcement officer under section 2518(7) of this title; or (3) a good faith determination that section 2511(3) [electronic communications provider authority to disclose content of an electronic communication "(i) as otherwise authorized in section 2511(2)(a) or 2517 of this title; (ii) with the lawful consent of the originator or any addressee or intended recipient of such communication; (iii) to a person employed or authorized, or whose facilities are used, to forward such communication to its destination; or (iv) which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency] or 2511(2)(I) [interception of communications of a trespasser in a computer system] of this title permitted the conduct complained of; is a complete defense against any civil or criminal action brought under this chapter or any other law," 18 U.S.C. 2520(d).

[2453] The $10,000 lump sum for liquidated damages is limited to a single award per victim rather than permitting $10,000 multiples based on the number of violations or the number of types of violations, as long as the violations are "interrelated and time compacted," Smoot v. United Transportation Union, 246 F.3d 633, 642-645 (6th Cir. 2001); Desilets v. Wal-Mart Stores, Inc., 171 F.3d 711, 713 (1st Cir. 1999).

[2454] 18 U.S.C. 2520. The text of 18 U.S.C. 2520 is appended.

[2455] Compare, e.g., DIRECTV, Inc. v. Brown, 371 F.3d 814, 818 (11th Cir. 2004); Dorris v. Absher, 179 F.3d, 420, 42930 (6th Cir. 1999); Nalley v. Nalley, 53 F.3d 649, 651-53 (4th Cir. 1995), Reynolds v. Spears, 93 F.3d 428, 433 (8th Cir. 1996); DIRECTV, Inc. v. Neznak, 371 F.Supp.2d 130, 133-34 (D.Conn. 2005) (each concluding that courts have discretion), with, Rodgers v. Wood, 910 F.2d 444, 447-49 (7th Cir. 1990) and Menda Biton v. Menda, 812 F.Supp. 283, 284 (D. Puerto Rico 1993) (courts have no such discretion) (note that after Menda, the First Circuit in Desilets v. Wal-Mart Stores, Inc., 171 F.3d at 716-17 treated as a matter for the trial court's discretion the question of whether the award of plaintiff's attorneys' fees should be reduced when punitive damages have been denied).

violations of section 2520[2456] and that law enforcement officers enjoy a qualified immunity from suit under section 2520.[2457]

The cause of action created in section 2520 is subject to a good faith defense.[2458] The only apparent efforts to claim the defense by anyone other than a government official or someone working at their direction have been unsuccessful.[2459]

Consequences: Civil Liability of the United States

The USA PATRIOT Act authorizes a cause of action against the United States for willful violations of Title III, the Foreign Intelligence Surveillance Act or the provisions governing stored communications in 18 U.S.C. 2701-2712.[2460] Successful plaintiffs are entitled to the greater of $10,000 or actual damages, and reasonable litigation costs.[2461]

Consequences: Administrative Action

Upon a judicial or administrative finding of a Title III violation suggesting possible intentional or willful misconduct on the part of a federal officer or employee, the federal agency or department involved may institute disciplinary action. It is required to explain to its Inspector General's office if it declines to do so.[2462]

[2456] Adams v. Battle Creek, 250 F.3d 980, 984 (6th Cir. 2001); Organizacion JD Ltda. v. United States Department of Justice, 18 F.3d 91, 94-5 (2d Cir. 1994); Connor v. Tate, 130 F.Supp. 2d 1370, 1374 (N.D.Ga. 2001); Dorris v. Absher, 959 F.Supp. 813, 820 (M.D.Tenn. 1997), aff'd/rev'd in part on other grounds, 179 F.3d 420 (6th Cir. 1999); PBA Local No. 38 v. Woodbridge Police Department, 832 F.Supp. 808, 822-23 (D.N.J. 1993) (each concluding that governmental entities may be held liable); contra, Abbott v. Winthrop Harbor, 205 F.3d 976, 980 (7th Cir. 2000); Amati v. Woodstock, 176 F.3d 952, 956 (7th Cir. 1999).

[2457] Compare, Berry v. Funk, 146 F.3d 1003, 1013 (D.C.Cir. 1998)(no immunity), with, Tapley v. Collins, 211 F.3d 1210, 1216 (11th Cir. 2000)(immunity); Blake v. Wright, 179 F.3d 1003, 1011-13(6th Cir. 1999)(same); see generally, Qualified Immunity as Defense in Suit Under Federal Wiretap Act (18 U.S.C.A. §§2510 et seq.), 178 ALR FED. 1.

[2458] 18 U.S.C. 2520(d).

[2459] Williams v. Poulos, 11 F.3d 271, 285 (1st Cir. 1993); United States v. Wuliger, 981 F.2d 1497, 1507 (6th Cir. 1992).

[2460] 18 U.S.C. 2712. The text of 18 U.S.C. 2712 is appended.

[2461] 18 U.S.C. 2712(a).

[2462] "If a court or appropriate department or agency determines that the United States or any of its departments or agencies has violated any provision of this chapter, and the court or appropriate department or agency finds that the circumstances surrounding the violation raise serious questions about whether or not an officer or employee of the United States acted willfully or

Consequences: Attorney Discipline

At one time, the American Bar Association (ABA) considered it ethical misconduct for an attorney to intercept or record a conversation without the consent of all of the parties to the conversation, ABA Formal Op. 337 (1974). The reaction of state regulatory authorities with the power to discipline professional misconduct was mixed. Some agreed with the ABA.[2463] Some agreed with the ABA, but expanded the circumstances under which recording could be conducted within ethical bounds.[2464] Some disagreed with the ABA view.[2465] The ABA has

---

intentionally with respect to the violation, the department or agency shall, upon receipt of a true and correct copy of the decision and findings of the court or appropriate department or agency promptly initiate a proceeding to determine whether disciplinary action against the officer or employee is warranted. If the head of the department or agency involved determines that disciplinary action is not warranted, he or she shall notify the Inspector General with jurisdiction over the department or agency concerned and shall provide the Inspector General with the reasons for such determination," 18 U.S.C. 2520(f).

[2463] Ala. Opinion 84-22 (1984); People v. Smith, 778 P.2d 685, 686, 687 (Colo. 1989); Haw. Formal Opinion No. 30 (1988); Ind.State Bar Ass'n Op.No.1 (2000); Iowa State Bar Ass'n v. Mollman, 488 N.W.2d 168, 169-70, 171-72 (Iowa 1992); Mo.Advisory Comm. Op. Misc. 30 (1978); Tex.Stat.Bar Op. 514 (1996); Va. LEO #1635 (1995), Va. LEO #1324; Gunter v. Virginia State Bar, 238 Va. 617, 621-22, 385 S.E.2d 597, 600 (1989). The federal courts seem to have been in accord, Parrott v. Wilson, 707 F.2d 1262 (11th Cir. 1983); Moody v. IRS, 654 F.2d 795 (D.C. Cir. 1981); Ward v. Maritz, Inc., 156 F.R.D. 592 (D.N.J. 1994); Wilson v. Lamb, 125 F.R.D. 142 (E.D.Ky. 1989); Haigh V. Matsushita Electric Corp., 676 F.Supp. 1332 (E.D.Va. 1987).

[2464] Ariz. Opinion No. 95-03 (1995); Alaska Bar Ass'n Eth.Comm. Ethics Opinions No. 95-5 (1995) and No. 91-4 (1991); Idaho Formal Opinion 130 (1989); Kan.Bar.Ass'n Opinion 96-9 (1997); Ky.Opinion E-279 (1984); Minn.Law.Prof. Resp.Bd. Opinion No. 18 (1996); Ohio Bd.Com.Griev.Disp. Opinion No. 97-3 (1997); S.C. Ethics Advisory Opinion 92-17 (1992); Tenn.Bd.Prof.Resp. Formal Ethics Opinion No. 86-F-14(a) (1986).

[2465] D.C. Opinion No. 229 (1992) (recording was not unethical because it occurred under circumstances in which the uninformed party should have anticipated that the conversation would be recorded or otherwise memorialized); Mississippi Bar v. Attorney ST., 621 So.2d 229 (Miss. 1993)(context of the circumstances test); Conn.Bar Ass"n Op. 98-9 (1998)(same); Mich.State Bar Op. RI-309 (1998)(same); Me.State Bar Op.No. 168 (1999)(same); N.M.Opinion 1996-2 (1996)(members of the bar are advised that there are no clear guidelines and that the prudent attorney avoids surreptitious recording); N.C. RPC 171 (1994)(lawyers are encouraged to disclose to the other lawyer that a conversation is being tape recorded); Okla.Bar Ass'n Opinion 307 (1994)(a lawyer may secretly recording his or her conversations without the knowledge or consent of other parties to the conversation unless the recording is unlawful or in violation of some ethical standard involving more than simply recording); Ore.State Bar Ass'n Formal Opinion No. 1991-74 (1991) (an attorney with one party consent he or she may record a telephone conversation "in absence of conduct which would reasonably lead an individual to believe that no recording would be made"); Utah State Bar Ethics Advisory Opinion No. 96-04 (1996) ("recording conversations to which an attorney is a party without prior disclosure to the other parties is not unethical when the act, considered within the context of the circumstances, does not involve dishonesty, fraud, deceit or misrepresentation"); Wis.Opinion E-94-5 ("whether the secret recording of a telephone conversation by a lawyer involves .dishonesty, fraud, deceit or misrepresentation' under SCR 20:8.4(c) depends upon all the circumstances operating at the

now repudiated its earlier position, ABA Formal Op. 01-422 (2001). Attorneys who engage in unlawful wiretapping or electronic eavesdropping will remain subject to professional discipline in every jurisdiction;[2466] in light of the ABA's change of position, courts and bar associations have had varied reactions to lawful wiretapping or electronic eavesdropping by members of the bar.[2467]

Consequences: Exclusion of Evidence

When the federal wiretap statute prohibits disclosure, the information is inadmissible as evidence before any federal, state, or local tribunal or authority, 18 U.S.C. 2515.[2468] Individuals whose conversations have been intercepted or

---

time"). In New York, the question of whether an attorney's surreptitiously recording conversations is ethically suspect is determined by locality, compare, Ass'n of the Bar of City of N.Y. Formal Opinion No. 1995-10 (1995)(secret recording is per se unethical), with, N.Y.County Lawyer's Ass'n Opinion No. 696 (1993)(secret recording is not per se unethical).

[2466] Cf., Nissan Motor Co., Ltd. v. Nissan Computer Corp., 180 F.Supp.2d 1089, 1095-97 (C.D.Cal. 2002).

[2467] E.g., State v. Murtagh, 169 P.3d 602, 617-18 (Alaska 2007)("undisclosed recording is not unethical"); In re Crossen, 450 Mass. 533, 558, 880 N.E.2d 352, 372 (2008) (undisclosed recording was unethical where it was part of scheme to coerce or manufacture testimony against the judge presiding over pending litigation); Midwest Motor Sports v. Arctic Cat Sales, Inc., 347 F.3d 693, 699 (8th Cir. 2003) (citing ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 01-422, which states that recording without consent should be prohibited when circumstances make it unethical); United States v. Smallwood, 365 F. Supp. 2d 689, 697-98 (E.D. Va. 2005) (holding that a lawyer cannot ethically record a conversation without the consent of all parties, even though doing so is not illegal under Virginia law). Declaring the new ABA opinion to be an "overcorrection," one bar association explained that secret taping should not be routine practice, but that it should be permitted if it advances a "societal good." Ass'n of the Bar of the City of New York Formal Opinion No. 2003-02 (2003). For a New York state bar opinion employing a similar line of reasoning, see Mena v. Key Food Stores Co-operative, Inc., 758 N.Y.S.2d 246, 247-50 (N.Y. Sup. Ct. 2003) (conduct of attorney who obtained a private investigator's services for a client and instructed the client on the use of recording equipment held not to warrant severe sanctions, because there was a compelling public interest in exposing the racial discrimination that was the subject of the secret recordings).

[2468] "Whenever any wire or oral communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof if the disclosure of that information would be in violation of this chapter," 18 U.S.C. 2515 (emphasis added); United States v. Chavez, 416 U.S. 562, 570 (1974); United States v. Lnu, 575 F.3d 298, 301 (3d Cir. 2009); United States v. Lam, 271 F.Supp.2d 1182, 1183-184 (N.D.Cal. 2003). Note that suppression does not extend to unlawfully intercepted electronic communications, United States v. Steiger, 318 F.3d 1039, 1050-52 (11th Cir. 2003); United States v. Jones, 364 F. Supp. 2d 1303, 1308-09 (D. Utah 2005); nor does it extend to evidence secured in violation the pen register/trap and trace provisions, United States v. German, 486 F.3d 849, 852-53 (5th Cir. 2007).

against whom the interception was directed[2469] have standing to claim the benefits of the section 2515 exclusionary rule through a motion to suppress under 18 U.S.C. 2518(10)(a).[2470] Paragraph 2518(10)(a) bars admission as long as the evidence is the product of (1) an unlawful interception, (2) an interception authorized by a facially insufficient court order, or (3) an interception executed in manner substantially contrary to the order authorizing the interception. Mere technical noncompliance is not enough; the defect must be of a nature that substantially undermines the regime of court-supervised interception for law enforcement purposes.[2471]

Although the Supreme Court has held that section 2515 may require suppression in instances where the Fourth Amendment exclusionary rule would not,[2472] some of the lower courts have recognized the applicability of the good faith exception to the Fourth Amendment exclusionary rule in section 2515 cases.[2473] Other courts

---

[2469] 18 U.S.C. 2510(11)("'aggrieved person' means a person who was a party to any an intercepted wire, oral, or electronic communication or a person against whom the interception was directed"); United States v. Gonzales, 412 F.3d 1102, 1115-117 (9th Cir. 2005).

[2470] The text of 18 U.S.C. 2518(10)(a) is appended.

[2471] United States v. Williams, 124 F.3d 411, 426 (3d Cir. 1997)("The Supreme Court has explained the relationship between these two provisions. In United States v. Giordano, 416 U.S. 505 (1974), the Court wrote that 'what disclosures are forbidden under 2515 and we subject to motions to suppress is . . . governed by 2518(10)(a).' Thus, evidence may be suppressed only if one of the grounds set out in 2518(10)(a) is met. Moreover not every failure to comply fully with any requirement provided in Title III would render the interception of wire or oral communications unlawful under 2518(10)(a)(I). United States v. Donovan, 429 U.S. 413, 433 (1977), quoting United States v. Chavez, 416 U.S. 562 (1974). Rather suppression is mandated only for a failure to satisfy any of those statutory requirements that directly and substantially implement the congressional intention to limit the use of intercept procedures to those situations clearly calling for the employment of this extraordinary investigative device, Donovan, 429 U.S. at 433-34, quoting Girodano, 416 U.S. at 527"); United States v. Lopez, 300 F.3d 46, 55-6 (1st Cir. 2002); United States v. Staffeldt, 451 F.3d 578, 582-85 (9th Cir. 2006); United States v. Gray, 521 F.3d 514, 522 (6th Cir. 2008). This is the case even where the court is clearly troubled by the government's failure to comply with the requirements of Title III, United States v. Callum, 410 F.3d 571, 579 (9th Cir. 2005)("Under the force of precedent, we uphold the challenged wiretap applications and orders. Still, we note that the Department of Justice and its officers did not cover themselves with glory in obtaining the wiretap orders at issue in this case. Title III is an exacting statute obviously meant to be followed punctiliously, yet the officers repeatedly ignored its clear requirements").

[2472] Gelbard v. United States, 408 U.S. 41, 52 (1972).

[2473] United States v. Moore, 41 F.3d 370, 376 (8th Cir. 1994); United States v. Ambrosio, 898 F.Supp. 177, 187 (S.D.N.Y. 1995); United States v. Malelzadeh, 855 F.2d 1492, 1497 (11th Cir. 1988); United States v. Mullen, 451 F.Supp.2d 509, 530-31 (W.D.N.Y. 2006); contra, United States v. Rice, 478 F.3d 704, 711-14 (6th Cir. 2007). Gelbard held that a grand jury witness might claim the protection of section 2515 through a refusal to answer questions based upon an unlawful wiretap notwithstanding the fact that the Fourth Amendment exclusionary rule does not apply in grand jury proceedings. Gelbard, 408 U.S. at 51-52. The good faith exception to the

have held, moreover, that the fruits of an unlawful wiretapping or electronic eavesdropping may be used for impeachment purposes.[2474]

The admissibility of tapes or transcripts of tapes of intercepted conversations raise a number of questions quite apart from the legality of the interception. As a consequence of the prerequisites required for admission, privately recorded conversations are more likely to be found inadmissible than those recorded by government officials. Admissibility will require the party moving for admission to show that the tapes or transcripts are accurate, authentic and trustworthy.[2475] For some courts this demands a showing that, "(1) the recording device was capable of recording the events offered in evidence; (2) the operator was competent to operate the device; (3) the recording is authentic and correct; (4) changes, additions, or deletions have not been made in the recording; (5) the recording has been preserved in a manner that is shown to the court; (6) the speakers on the tape are identified; and (7) the conversation elicited was made voluntarily and in good faith, without any kind of inducement."[2476]

Fourth Amendment exclusionary rule permits the admission of evidence secured in violation of the Fourth Amendment, if the officers responsible for the breach were acting in good faith reliance upon the apparent authority of a search warrant or some like condition negating the remedial force of the rule, United States v. Leon, 468 U.S. 897, 909 (1984).

[2474] Culbertson v. Culbertson, 143 F.3d 825, 827-28 (4th Cir. 1998); United States v. Echavarria-Olarte, 904 F.2d 1391 (9th Cir. 1990); United States v. Vest, 813 F.2d 477, 484 (1st Cir. 1987); cf., United States v. Crabtree, 565 F.3d 887, 891-92 (4th Cir. 2009)(noting that the Circuit's recognition of admissibility for impeachment purposes does not require recognition of a clean hands exception under which the government may admit introduce illegal wiretap evidence as long as it was not involved in the illegal interception).

[2475] United States v. Thompson, 130 F.3d 676, 683 (5th Cir. 1997); United States v. Panaro, 241 F.3d 1104, 1111 (9th Cir. 2001); United States v. Smith, 242 F.3d 737, 741 (7th Cir. 2001).

[2476] United States v. Webster, 84 F.3d 1056, 1064 (8th Cir. 1996); United States v. Green, 175 F.3d 822, 830 n.3 (10th Cir. 1999); United States v. Green, 324 F.3d 375, 379 (5th Cir. 2003)(citing 4 of the 7 factors); cf., United States v. Calderin-Rodriguez, 244 F.3d 977, 986-87 (8th Cir. 2001). These seven factors have been fairly widely cited since they were first announced in United States v. McKeever, 169 F.Supp. 426, 430 (S.D.N.Y. 1958), rev'd on other grounds, 271 F.2d 669 (2d Cir. 1959). They are a bit formalistic for some courts who endorse a more ad hoc approach to the assessment of whether the admission of what purports to be a taped conversation will introduce fraud or confusion into the court, e.g., Stringel v. Methodist Hosp. of Indiana, Inc., 89 F.3d 415, 420 (7th Cir. 1996)(McKeever "sets out a rather formal, seven step checklist for the authentication of tape recordings, and we have looked to some of the features [in the past]"); United States v. White, 116 F.3d 903, 921 (D.C.Cir. 1997)("tapes may be authenticated by testimony describing the process or system that created the tape or by testimony from parties to the conversation affirming that the tapes contained an accurate record of what was said"); United States v. Tropeano, 252 F.3d 653, 661 (2d Cir. 2001)("[T]his Circuit has never expressly adopted a rigid standard for determining the admissibility of tape recordings"); United States v. Westmoreland, 312 F.3d 302, 310-11 (7th Cir. 2002); United States v. Dawson, 425 F.3d 389, 393 (7th Cir. 2005)("But there are no rigid rules, such as chain of custody, for authentication; all that is required is adequate evidence of genuineness. (There are such rules for electronic surveillance governed by Title III,

Illegal Disclosure of Information Obtained by Wiretapping or Electronic Eavesdropping

Although often overlooked, it also a federal crime to disclose information obtained from illicit wiretapping or electronic eavesdropping, 18 U.S.C. 2511(1)(c):

- any person [who]
- intentionally
- discloses or endeavors to disclose to another person
- the contents of any wire, oral, or electronic communication
- having reason to know
- that the information was obtained through the interception of a wire, oral, or electronic communication
- in violation of 18 U.S.C. 2511(1)
- is subject to the same sanctions and remedies as the wiretapper or electronic eavesdropper.

This is true of the wiretapper or electronic eavesdropper and of all those who disclose information, that in fact can be traced to a disclosure by the original wiretapper or eavesdropper, with reason to know of the information's illicit origins, except to the extent the First Amendment bans application.[2477] The legislative history speaks of a common knowledge limitation on the statute's coverage, but it is not clear whether it refers to common knowledge at the time of

---

but Title III is inapplicable to conversations that, as here, are recorded with the consent of one of the participants)").

[2477] Bartnicki v. Vopper, 532 U.S. 514, 533-34 (2001), pointed out that the First Amendment right to free speech bars the application of section 2511(1)(c) to the disclosure of illegally intercepted, but lawfully acquired, communications dealing with a matter of unusual public concern. Bartnicki was a union negotiator whose telephone conversations with the union's president were surreptitiously intercepted and recorded a discussion negotiation of a teachers' contract. During the conversation, the possibility of using violence against school board members was mentioned. After the teachers' contract was signed, the unknown wiretapper secretly supplied Yocum, a critic of the union's position, with a copy of the tape. Yocum in turn played it for members of the school board and turned it over to Vopper, a radio talk show host, who played it on his show. Other stations and media outlets published the contents as well. Bartnicki sued Vopper and Yocum for use and disclosure in violation of sections 2511(1)(c) and 2511(1)(d). Vopper and Yocum offered a free speech defense, which the Supreme Court accepted. But see, Quigley v. Rosenthal, 327 F.3d 1044, 106768 (10th Cir. 2003) (denying First Amendment protection for those knowingly involved with interceptors of private matters (not public concerns)); Boehner v. McDermott, 484 F.3d 573, 577-81 (D.C. Cir. 2007)(Members of Congress do not have a First Amendment right to disclose unlawful wiretap information in violation of House rules). For a more extensive examination of Bartnicki, see, CRS Report RS20974, The Right to Publish Lawfully Obtained But Illegally Intercepted Material of Public Concern: Bartnicki v. Vopper.

interception or at the time disclosure.[2478] By definition, a violation of paragraph 2511(1)(c) requires an earlier unlawful interception under subsection 2511(1). If there is no predicate unlawful interception there can be no violation of paragraph 2511(1)(c).

The results of electronic eavesdropping authorized under Title III/ECPA may be disclosed and used for law enforcement purposes[2479] and for testimonial purposes.[2480]

It is also a federal crime to disclose, with an intent to obstruct criminal justice, any information derived from lawful police wiretapping or electronic eavesdropping, i.e.:

- any person [who]
- intentionally discloses, or endeavors to disclose, to any other person
- the contents of any wire, oral, or electronic communication
- intercepted by means authorized by sections:
    - 2511(2)(a)(ii) (communication service providers, landlords, etc. who assist police setting up wiretaps or electronic eavesdropping devices)
    - 2511(2)(b) (FCC regulatory activity)
    - 2511(2)(c) (police one party consent)

[2478] "Subparagraphs (c) and (d) prohibit, in turn, the disclosure or use of the contents of any intercepted communication by any person knowing or having reason to know the information was obtained through an interception in violation of this subsection. The disclosure of the contents of an intercepted communication that had already become 'public information' or 'common knowledge' would not be prohibited. The scope of this knowledge required to violate either subparagraph reflects existing law (Pereira v. United States, 347 U.S. 1 (1954))," S.Rept. 90=-1097, at 93 (1967). The remark may also have been influenced by the high level of intent (willfully rather than intentionally) included in the disclosure provision as reported out.

[2479] "Any investigative or law enforcement officer who, by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents to another investigative or law enforcement officer to the extent that such disclosure is appropriate to the proper performance of the official duties of the officer making or receiving the disclosure," 18 U.S.C. 2517(1).

[2480] "Any person who has received, by any means authorized by this chapter, any information concerning a wire, oral, or electronic communication, or evidence derived therefrom intercepted in accordance with the provisions of this chapter may disclose the contents of that communication or such derivative evidence while giving testimony under oath or affirmation in any proceeding held under the authority of the United States or of any State or political subdivision thereof," 18 U.S.C. 2517(3). This does not entitle private litigants to disclosure in the view of at least one court, In re Motion to Unseal Electronic Surveillance Evidence, 990 F.2d 1015 (8th Cir. 1993). When court-ordered interception results in evidence of a crime other than the crime with respect to which the order was issued, the evidence is admissible only upon a judicial finding that it was otherwise secured in compliance with Title III/ECPA requirements, 18 U.S.C. 2517(5).

    - 2511(2)(e) (Foreign Intelligence Surveillance Act)
    - 2516 (court-ordered, police wiretapping or electronic surveillance)
    - 2518 (emergency wiretaps or electronic surveillance)
- knowing or having reason to know that
- the information was obtained through the interception of such a communication
- in connection with a criminal investigation
- having obtained or received the information in connection with a criminal investigation
- with intent to improperly obstruct, impede, or interfere with a duly authorized criminal investigation,
- is subject to the same sanctions and remedies as one who illegally wiretaps, 18 U.S.C. 2511(1)(e).[2481]

The proscriptions in 2511(1)(e) would appear to apply to efforts to obstruct justice by information gleaned from either federal or state police wiretaps. Use of the word "authorized" in conjunction with a list of federal statutes might suggest that the paragraph was only intended to protect wiretap information gathered by federal rather than by federal or state authorities. But most of the cited sections do not "authorize" anything; they simply confine the reach of the statutory prohibitions. And several are as likely to involve state interceptions as federal, e.g., the one-partyconsent-under-color-of-law interceptions.

Essentially, the same consequences flow from an unlawful disclosure under paragraphs 2511(1)(c) or 2511(1)(e) as follow unlawful interception under paragraphs 2511(1)(a) or 2511(1)(b):

- maximum five year prison terms and fines of not more than $250,000 or $500,000, depending upon whether the offender is an individual or organization;[2482]

[2481] When acting with a similar intent, disclosure of the fact of authorized federal wiretap or foreign intelligence gathering is proscribed elsewhere in title 18. "Whoever, having knowledge that a Federal investigative or law enforcement officer has been authorized or has applied for authorization under chapter 119 to intercept a wire, oral, or electronic communication, in order to obstruct, impede, or prevent such interception, gives notice or attempts to give notice of the possible interception to any person shall be fined under this title or imprisoned not more than five years, or both."

"Whoever, having knowledge that a Federal officer has been authorized or has applied for authorization to conduct electronic surveillance under the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801, et seq.), in order to obstruct, impede, or prevent such activity, gives notice or attempts to give notice of the possible activity to any person shall be fined under this title or imprisoned not more than five years, or both," 18 U.S.C. 2232(d),(e).

[2482] "[W]hoever violates subsection (1) of this section shall be fined under this title or imprisoned not more than five years, or both," 18 U.S.C. 2511(4)(a).

- exposure to civil liability including equitable relief and actual or statutory damages.[2483]

Illegal Use of Information Obtained by Unlawful Wiretapping or Electronic Eavesdropping

The prohibition on the use of information secured from illegal wiretapping or electronic eavesdropping mirrors the disclosure provision, 18 U.S.C. 2511(1)(d):

- any person [who]
- intentionally
- uses or endeavors to use to another person
- the contents of any wire, oral, or electronic communication
- having reason to know
- that the information was obtained through the interception of a wire, oral, or electronic communication
- in violation of 18 U.S.C. 2511(1)
- is subject to the same sanctions and remedies as the wiretapper or electronic eavesdropper.

The available case law under the use prohibition of section 2511(1)(d) is scant, and the section has rarely been invoked except in conjunction with the disclosure prohibition of section 2511(1)(c). The wording of the two is clearly parallel, the legislative history describes them in the same breath,[2484] and they are treated alike for law enforcement purposes.[2485] *Bartnicki* seems destined to change all of that, because it appears to parse the constitutionally suspect ban on disclosure

---

[2483] "(a) . . . any person whose wire, oral, or electronic communication is . . . disclosed . . . used in violation of this chapter may in a civil action recover from the person or entity, other than the United States, which engaged in that violation such relief as may be appropriate. . . .(g) Any willful disclosure . . . by an investigative or law enforcement officer or governmental entity of information beyond the extent permitted by section 2517 is a violation of this chapter for purposes of section 2520(a)," 18 U.S.C. 2520(a),(g).

[2484] "Subparagraphs (c) and (d) prohibit, in turn, the disclosure or use of the contents of any intercepted communication by any person knowing or having reason to know the information was obtained through an interception in violation of this subsection," S.Rept. 90-1097, at 93 (1967).

[2485] Compare, 18 U.S.C. 2517(1)("Any investigative or law enforcement officer who, by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents to another investigative or law enforcement officer to the extent that such disclosure is appropriate to the proper performance of the official duties of the officer making or receiving the disclosure"), with 18 U.S.C. 2517(2)("Any investigative or law enforcement officer who, by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication or evidence derived therefrom may use such contents to the extent such use is appropriate to the proper performance of his official duties").

from the constitutionally permissible ban on use.[2486] In doing so, it may also resolve a conflict among the lower federal appellate courts over the so-called "clean hands" exception. A few courts had recognized an exception to the disclosure-use bans of section 2511(1) where law enforcement officials might disclose or use the results of an illegal interception in which they had played no role.[2487] *Bartnicki* appears to dim the prospects of a clean hands exception because, to illustrate situations to which the section 2511(1)(d) use might be constitutionally outlawed, it points to one of the cases which rejected the exception.[2488]

The consequences of unlawful use of intercepted communications in violation of paragraph 2511(d) are similar to those for unlawful disclosure in violation of paragraphs 2511(1)(c) or 2511(1)(e), or for unlawful interception under paragraphs 2511(1)(a) or 2511(1)(b):

- maximum five year prison terms and fines of not more than $250,000 or $500,000, depending upon whether the offender is an individual or organization, 18 U.S.C. 2511(4)(a);
- exposure to civil liability including equitable relief and actual or statutory damages, 18 U.S.C. 2520(a), (g).

Shipping, Manufacturing, Distributing, Possessing or Advertising Wire, Oral, or Electronic Communication Interception Devices

The proscriptions for possession and trafficking in wiretapping and eavesdropping devices are even more demanding than those that apply to the

---

[2486] "[T]he naked prohibition against disclosures is fairly characterized as a regulation of pure speech. Unlike the prohibition against the .use' of the contents of an illegal interception in §2511(1)(d), subsection (c) is not a regulation of conduct," 532 U.S. at 526-27.

[2487] Forsyth v. Barr, 19 F.3d 1527, 1541-545 (5th Cir. 1994); United States v. Murdock, 63 F.3d 1391, 1400-403 (6th Cir. 1995); contra,United States v. Crabtree, 565 F.3d 887, 889 (4th Cir. 2009); Berry v. Funk, 146 F.3d 1003, 1011-13 (D.C.Cir. 1998); Chandler v. United States Army, 125 F.3d 1296, 1300-302 (9th Cir. 1997); In re Grand Jury, 111 F.3d 1066, 1077 (3d Cir. 1997); United States v. Vest, 813 F.2d 477, 481 (1st Cir. 1987); United States v. Lam, 271 F.Supp.2d 1182, 1184-187 (N.D.Cal. 2003); see also, United States v. Gray, 521 F.3d 514, 530 (6th Cir. 2008)(noting that doctrine is only available in cases of government use).

[2488] "Unlike the prohibition against the .use' of the contents of an illegal interception in §2511(1)(d),* subsection (c) is not a regulation of conduct.

*"The Solicitor General has catalogued some of the cases that fall under subsection (d): . . . . The statute has also been held to bar the use of illegally intercepted communications for important and socially valuable purposes, see, In re Grand Jury, 111 F.3d 1066, 1077-79 (3d Cir. 1997)," 532 U.S. at 527 (footnote 10 of the Court's opinion quoted after the *).

predicate offense itself. There are exemptions for service providers,[2489] government officials and those under contract with the government,[2490] but there is no exemption for equipment designed to be used by private individuals, lawfully but surreptitiously.[2491]

The three prohibitions in section 2512 present generally common features, declaring that:

- any person who
- intentionally
- either
  - (a)
    - sends through the mail or sends or carries in interstate or foreign commerce
    - any electronic, mechanical, or other device
    - knowing or having reason to know
    - that the design of such device renders it primarily useful
    - for the purpose of the surreptitious interception of wire, oral, or electronic communications; or
  - (b)
    - manufactures, assembles, possesses, or sells
    - any electronic, mechanical, or other device
    - knowing or having reason to know
    - that the design of such device renders it primarily useful

---

[2489] "It shall not be unlawful under this section for – (a) a provider of wire or electronic communication service or an officer, agent, or employee of, or a person under contract with, such a provider, in the normal course of the business of providing that wire or electronic communication service . . . to send through the mail, send or carry in interstate or foreign commerce, or manufacture, assemble, possess, or sell any electronic, mechanical, or other device knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications," 18 U.S.C. 2512(2)(a).

[2490] "(2) It shall not be unlawful under this section for . . . (b) an officer, agent, or employee of, or a person under contract with, the United States, a State, or a political subdivision thereof, in the normal course of the activities of the United States, a State, or a political subdivision thereof, to send through the mail, send or carry in interstate or foreign commerce, or manufacture, assemble, possess, or sell any electronic, mechanical, or other device knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications. "(3) It shall not be unlawful under this section to advertise for sale a device described in subsection (1) of this section if the advertisement is mailed, sent, or carried in interstate or foreign commerce solely to a domestic provider of wire or electronic communication service or to an agency of the United States, a State, or a political subdivision thereof which is duly authorized to use such device," 18 U.S.C. 2512(2)(b),(3).

[2491] United States v. Spy Factory, Inc., 951 F.Supp. 450, 473-75 (S.D.N.Y. 1997); United States v. Bast, 495 F.2d 138, 141 (D.C.Cir. 1974).

    - for the purpose of the surreptitious interception of wire, oral, or electronic communications, and
    - that such device or any component thereof has been or will be sent through the mail or transported in interstate or foreign commerce; or
- (c)
    - places in any newspaper, magazine, handbill, or other publication or disseminates electronically
    - any advertisement of —
        - any electronic, mechanical, or other device
        - knowing or having reason to know
        - that the design of such device renders it primarily useful
        - for the purpose of the surreptitious interception of wire, oral, or electronic communications; or
        - any other electronic, mechanical, or other device
        - where such advertisement promotes the use of such device
        - for the purpose of the surreptitious interception of wire, oral, or electronic communications
    - knowing the content of the advertisement and knowing or having reason to know
    - that such advertisement will be sent through the mail or transported in interstate or foreign commerce
- shall be imprisoned for not more than five years and/or fined not more than $250,000 (not more than $500,000 for organizations), 18 U.S.C. 2512.

The legislative history lists among the items Congress considered "primarily useful for the purpose of the surreptitious interception of communications: the martini olive transmitter, the spike mike, the infinity transmitter, and the microphone disguised as a wristwatch, picture frame, cuff link, tie clip, fountain pen, stapler, or cigarette pack."[2492]

Questions once raised over whether section 2512 covers equipment designed to permit unauthorized reception of scrambled satellite television signals have been resolved.[2493] Each of the circuits to consider the question has now concluded that

---

[2492] S.Rept. 90-1097, at 95 (1968).

[2493] The two appellate panel decisions that found the devices beyond the bounds of section 2512, United States v. Herring, 933 F.2d 932 (11th Cir. 1991) and United States v. Hux, 940 F.2d 314 (8th Cir. 1991) were overturned en banc, United States v. Herring, 993 F.2d 784, 786 (11th Cir. 1993); United States v. Davis, 978 F.2d 415, 416 (8th Cir. 1992).

2512 outlaws such devices,[2494] but simple possession does not give rise to a private cause of action.[2495]

Stored Electronic Communications

In its original form Title III was ill-suited to ensure the privacy of those varieties of modern communications which are equally vulnerable to intrusion when they are at rest as when they are in transmission. Surreptitious "access" is as least as great a threat as surreptitious "interception" to the patrons of electronic mail (e-mail), electronic bulletin boards, voice mail, pagers, and remote computer storage.

Accordingly, Title III/ECPA also bans surreptitious access to communications at rest, although it does so beyond the confines of that apply to interception, 18 U.S.C. 2701 - 2711. These separate provisions afford protection for e-mail, voice mail, and other electronic communications somewhat akin to that available for telephone and face to face conversations under 18 U.S.C. 2510-2522. Thus, subject to certain exceptions, it is a federal crime to:

- intentionally
- either
    - access without authorization or
    - exceed an authorization to access
- a facility through which an electronic communication service is provided
- and thereby obtain, alter, or prevent authorized access to a wire or electronic communication while it is in electronic storage in such system, 18 U.S.C. 2701(a).[2496]

[2494] United States v. Harrell, 983 F.2d 36, 37-39 (5th Cir. 1993); United States v. One Macom Video Cipher II, 985 F.2d 258, 259-61 (6th Cir. 1993); United States v. Shriver, 989 F.2d. 898, 901-06 (7th Cir. 1992); United States v. Davis, 978 F.2d 415, 417-20 (8th Cir. 1992); United States v. Lande, 968 F.2d 907, 910-11 (9th Cir. 1992); United States v. McNutt, 908 F.2d 561, 564-65 (10th Cir. 1990); United States v. Herring, 993 F.2d 784, 786-89 (11th Cir. 1991).

[2495] DIRECTV, Inc. v. Treworgy, 373 F.3d 1124, 1129 (11th Cir. 2004); DIRECTV, Inc. v. Robson, 420 F.3d 532, 538-39 (5th Cir. 2005)(citing several district court cases that have reached the same conclusion). Proof that the possessor used the device to intercept satellite transmission evidences a violation of section 2511 and exposure to civil liability under section 2520, DIRECTV, Inc. v. Nicholas, 403 F.3d 223, 227-28 (4th Cir. 2005); DIRECTV, Inc. v. Pepe, 431 F.3d 162, 169 (3d Cir. 2005).

[2496] E.g., State Analysis, Inc. v. American Finacial Services Ass'n, 621 F.Supp.2d 309, 317-18 (E.D. Va. 2009); Pure Power Boot Camp v. Warrior Fitness Boot Camp, 587 F.Supp.2d 548, 555 (S.D.N.Y. 2008).

The exceptions cover electronic storage facility operators, their customers, and – under procedural counterparts to court ordered wiretapping – governmental entities.[2497]

Violations committed for malicious, mercenary, tortious or criminal purposes are punishable by imprisonment for not more than five years and/or a fine of not more than $250,000 (not more than 10 years for a subsequent conviction); lesser transgressions, by imprisonment for not more than one year (not more than five years for a subsequent conviction) and/or a fine of not more than $100,000.[2498] Those who provide the storage service and other victims of unlawful access have a cause of action for equitable relief, reasonable attorneys' fees and costs, damages equal the loss and gain associated with the offense but not less than $1000.[2499] Both criminal and civil liability are subject to good faith defenses.[2500]

[2497] "Subsection (a) of this section does not apply with respect to conduct authorized – (1) by the person or entity providing a wire or electronic communications service; (2) by a user of that service with respect to a communication of or intended for that user; or (3) in section 2703 [requirements for government access], 2704 [backup preservation] or 2518 [court ordered wiretapping or electronic eavesdropping] of this title," 18 U.S.C. 2701(c). Section 2709 creates an exception for counterintelligence access to telephone records.

[2498] "The punishment for an offense under subsection (a) of this section is – (1) if the offense is committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain, or in furtherance of any criminal or tortious act in violation of the constitution and laws of the United States or any state – (A) a fine under this title or imprisonment for not more than 5 years, or both, in the case of a first offense under this subparagraph; and (B) a fine under this title or imprisonment for not more than 10 years, or both, for any subsequent offense under this subparagraph; and (2)(A) a fine under this title or imprisonment for not more than 1 year or both, in the case of a first offense under this paragraph; and (B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under this subparagraph that occurs after a conviction of another offense under this section,"18 U.S.C. 2701(b).

[2499] "(a) Cause of action – Except as provided in section 2703(e)[relating to immunity for compliance with judicial process], any provider of electronic communication service, subscriber, or customer aggrieved by any violation of this chapter in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind may, in a civil action, recover from the person or entity other than the United States which engaged in that violation such relief as may be appropriate.

"(b) Relief – In a civil action under this section, appropriate relief includes – (1) such preliminary and other equitable or declaratory relief as may be appropriate; (2) damages under subsection(c); and (3) a reasonable attorney's fee and other litigation costs reasonably incurred;

"(c) Damages – The court may assess as damages in a civil action under this section the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation, but in no case shall a person entitled to recover receive less than the sum of $1,000. . . ." 18 U.S.C. 2707.

Service providers, nevertheless, may incur civil liability for unlawful disclosures,[2501] unless they can take advantage of one of a fairly extensive list of exceptions and defenses.[2502]

To be eligible for statutory damages, a plaintiff must show actual damage, but attorneys' fees and punitive damages may be award without proof of actual damages, VanAlystyne v. Electronic Scriptorium, Ltd., 560 F.3d 199, 202 (4th Cir. 2009).

[2500] "A good faith reliance on – (1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization (including a request of a governmental entity under section 2703(f) of this title) [relating to an official request to for a service provider preserve evidence]; (2) a request of an investigative or law enforcement officer under section 2518(7) of this title [relating to emergency wiretapping and electronic eavesdropping]; or (3) a good faith determination that section 2511(3) of this title [relating to the circumstances under which an electronic communications provider may divulge the contents of communication] permitted the conduct complained of – is a complete defense to any civil or criminal action brought under this chapter or any other law," 18 U.S.C. 2707(e).

[2501] "Except as in subsection (b) or (c) – (1) a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; (2) a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service – (A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service; and (B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing; and (3) a provider of remote computing service or electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by paragraph (1) or (2)) to any government entity," 18 U.S.C. 2702(a). Section 2702 makes no mention of any consequences that follow a breach of its commands, but 2707 establishes a civil cause of action for the victims of any violation of chapter 121 (18 U.S.C. 2701 -2711).

[2502] "A provider described in subsection (a) may divulge the contents of a communication – (1) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient; (2) as otherwise authorized in section 2517, 2511(2)(a), or 2703 of this title; (3) with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service; (4) to a person employed or authorized or whose facilities are used to forward such communication to its destination; (5) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service; (6) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 227 of the Victims of Child Abuse Act of 1990; (7) to a law enforcement agency – (A) if the contents – (I) were inadvertently obtained by the service provider; and (ii) appear to pertain to the commission of a crime; (8) to a Federal, State, or local government entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency," 18 U.S.C. 2702(b). The Ninth Circuit recently explained that while a remote computer service provider may disclose to a subscriber (as noted in italics above), an electronic service provider, such as one who

Violations by the United States may give rise to a cause of action and may result in disciplinary action against offending officials or employees under the same provisions that apply to U.S. violations of Title III,[2503] but unlike Title III there is no statutory prohibition on disclosure or use of the information through a violation of section 2701[2504] nor is there a statutory rule for the exclusion of evidence as a consequence of a violation.[2505] A Sixth Circuit panel has held, in a decision since vacated en banc, that the Fourth Amendment precludes government access to the content of stored communications (e-mail) held by service providers in the absence of a warrant, subscriber consent, or other indication that the subscriber has waived his or her expectation of privacy.[2506] Where the government instead secures access through a subpoena or court order as section 2703 permits, the evidence may be subject to both the Fourth Amendment exclusionary rule and the exceptions to the rule.[2507]

Unlawful access to electronic communications may involve violations of several other federal and state laws, including for instance the federal computer fraud and abuse statute, 18 U.S.C. 1030, and state computer abuse statutes.[2508]

Pen Registers and Trap and Trace Devices

A trap and trace device identifies the source of incoming calls, and a pen register indicates the numbers called from a particular phone.[2509] Since neither allows the

---

provides text messaging services, may not, even when the material disclosed resides in storage, Quon v. Arch Wireless Operating Co., Inc., 529 F.3d 892, 900-901 (9th Cir. 2008).

[2503] "Any person who is aggrieved by any willful violation this chapter or of chapter 119 of this title [18 U.S.C. 25102520] . . . may commence an action in United States District Court . . . .If . . . any of the departments or agencies has violated any provision of this chapter . . . the department or agency shall . . . promptly initiate a proceeding to determine whether disciplinary action . . . is warranted. . . ."18 U.S.C. 2712(a),(c).

[2504] Cardinal Health 414, Inc. v. Adams, 582 F.Supp.2d 967, 976 (M.D.Tenn. 2008).

[2505] United States v. Steiger, 318 F.3d 1039, 1049 (11th Cir. 2003); United States v. Perrine, 518 F.3d 1196, 1202 (10th Cir. 2008); United States v. Navas, 640 F.Supp.2d 256, 262 (S.D.N.Y. 2009).

[2506] Warshak v. United States, 490 F.3d 455, 468-82 (6th Cir. 2007), vac'd en banc, 532 F.3d 521 (6th Cir. 2008) (vacated on grounds that the issue was not ripe for decision).

[2507] United States v. Ferguson, 508 F.Supp.2d 7, 8-10 (D.D.C. 2007)(even if a Fourth Amendment violation occurred, officers could rely in good faith on the magistrate's order issued before any court had raised the specter of constitutional suspicion which surfaced later in Warshak).

[2508] See generally, CRS Report 97-1025, Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws, by Charles Doyle. Citations to the various state computer abuse statutes appear in Appendix F.

eavesdropper to overhear the "contents" of the phone conversation, they were not considered interceptions within the reach of Title III prior to the enactment of ECPA.[2510] Although Congress elected to expand the definition of interception, it chose to continue to regulate these devices beyond the boundaries of Title III for most purposes, 18 U.S.C. 3121 - 3127.

As noted earlier, however, the Title III wiretap provisions apply when due to the nature of advances in telecommunications technology pen registers and trap and trace devices are able to capture wire communication "content."[2511]

The USA PATRIOT Act enlarged the coverage of sections 3121-3127 to include sender/addressee information relating to e-mail and other forms of electronic communications.[2512]

The use or installation of pen registers or trap and trace devices by anyone other than the telephone company, service provider, or those acting under judicial authority is a federal crime, punishable by imprisonment for not more than a year and/or a fine of not more than $100,000 ($200,000 for an organization).[2513]

[2509] "(3) the term 'pen register' means a device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached, but such term does not include any device used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business; (4) the term 'trap and trace device' means a device which captures the incoming electronic or other impulses which identify the originating number of an instrument or device from which a wire or electronic communication was transmitted," 18 U.S.C. 3127(3),(4). Although clone pagers are not considered pen registers, Brown v. Waddell, 50 F.3d 285, 290-91 (4th Cir. 1995), "caller id" services have been found to constitute trap and trace devices, United States v. Fregoso, 60 F.3d 1314, 1320 (8th Cir. 1995).

[2510] United States v. New York Telephone Co., 434 U.S. 159 (1977).

[2511] "'Post-cut-through dialed digits' are any numbers dialed from a telephone after the call is initially setup or 'cutthrough.' Sometimes these digits are other telephone numbers, as when a party places a credit card call by first dialing the long distance carrier access number and then the phone number of the intended party. Sometimes these digits transmit real information, such as bank account numbers, Social Security numbers, prescription numbers, and the like. In the latter case, the digits represent communications content; in the former, they are non-content call processing numbers," In re United States, 441 F.Supp.2d 816, 818 (S.D. Tex. 2006); see also, In re United States for Orders (1) Authorizing Use of Pen Registers and Trap and Trace Devices, 515 F.Supp.2d 325, 328-38 (E.D.N.Y. 2007); In re United States, 622 F.Supp.2d 411, 419-22 (S.D. Tex. 2007).

[2512] 115 Stat. 288-91 (2001).

[2513] "(a) In general – Except as provided in this section, no person may install or use a pen register or a trap and trace device without first obtaining a court order under section 3123 of this title or under the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.). (b) Exception –

There is no accompanying exclusionary rule, however, and consequently a violation of section 3121 will not serve as a basis to suppress any resulting evidence.[2514]

Unlike other violations of Title III/ECPA, there is no separate federal private cause of action for victims of a pen register or trap and trace device violation. Some of the states have established a separate criminal offense for unlawful use of a pen register or trap and trace device,[2515] yet most of these seem to follow the federal lead and decline to establish a separate private cause of action for unlawful installation or use of the devices.[2516]

Foreign Intelligence Surveillance Act

The Foreign Intelligence Surveillance Act (FISA) authorizes special court orders for four purposes: electronic surveillance, physical searches, installation and use pen registers/trap and trace devices, and orders to disclose tangible items, 50 U.S.C. 1801-1861. The electronic surveillance portion of FISA, 50 U.S.C. 1801-1811, creates a procedure for judicially supervised "electronic surveillance" (wiretapping) conducted for foreign intelligence gathering purposes. The Act classifies four kinds of wiretapping as "electronic surveillance." The four classes

---

The prohibition of subsection (a) does not apply with respect to the use of a pen register or a trap and trace device by a provider of electronic or wire communication service – (1) relating to the operation, maintenance, and testing of a wire or electronic communication service or to the protection of the rights or property of such provider, or to the protection of users of that service from abuse of service or unlawful use of service; or (2) to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire communication, or a user of that service, from fraudulent, unlawful or abusive use of service; or (3) where the consent of the user of that service has been obtained. (c) Limitation – A government agency authorized to install and use a pen register or trap and trace device under this chapter or under State law shall use technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to the dialing, routing, addressing, and signaling information utilized in identifying the origination or destination of wire or electronic communications. (d) Penalty. – Whoever knowingly violates subsection (a) shall be fined under this title or imprisoned not more than one year, or both," 18 U.S.C. 3121.

[2514] United States v. German, 486 F.3d 849, 852-53 (5th Cir. 2007); United States v. Fregoso, 60 F.3d 1314, 1320 (8th Cir. 1995); United States v. Thompson, 936 F.2d 1249, 1249-250 (11th Cir. 1991). To the extent that the unlawful use captures content, the Fourth Amendment exclusionary rule may apply, cf., In re United States for Orders (1) Authorizing Use of Pen Registers and Trap and Trace Devices, 515 F.Supp.2d 325, 328-38 (E.D.N.Y. 2007).

[2515] E.g., ARIZ. REV. STAT. ANN. §13-3005; FLA. STAT. ANN. §934.31; IOWA CODE ANN. §808B.10; N.H. RV. STAT. ANN. §570-B:2; UTAH CODE ANN. §77-23-13.

[2516] But see, MINN. STAT. ANN. §626A.391. Appendix E contains the citations of state statutes that authorized court ordered installation and use of pen registers and trap & trace devices. Appendix C lists the citations of state statutes that create a separate cause of action for unlawful interception.

of electronic surveillance involve wiretapping that could otherwise only be conducted under court order:

- "(1) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes;
- "(2) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States, does not include the acquisition of those communications of computer trespassers that would be permissible under section 2511(2)(I) of title 18, United States Code;
- "(3) the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States; or
- "(4) the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes," 50 U.S.C. 1801(f).

Section 1809 proscribes:

- intentionally, either
    - engaging in *electronic surveillance*
    - under color of law
    - except as authorized by statute, or
    - disclosing or using
    - information obtained under color of law
    - by electronic surveillance,
    - knowing or having reason to know
    - that the information was obtained by electronic surveillance not authorized by statute, 50 U.S.C. 1809.

The prohibitions of section 1809 apply only to federal officers and employees,[2517] but do not apply to a law enforcement officer operating under a warrant or court order.[2518] Violations are punishable by imprisonment for not more than five years and/or a fine of not more than $250,000, id. and expose the offender to civil liability.[2519] By virtue of USA PATRIOT Act amendments, victims of any improper use of information secured under a FISA surveillance order may also be entitled to actual or statutory damages.[2520]

FISA also has its own exclusionary rule for electronic surveillance, physical searches, and the installation and use of pen registers and trap & trace devices.[2521] However, Congress anticipated,[2522] and the courts have

---

[2517] "There is Federal jurisdiction over an offense under this section if the person committing the offense was an officer or employee of the United States at the time the offense was committed," 50 U.S.C. 1809(d). The criminal proscriptions and exemptions of Title III/ECPA (18 U.S.C. 2510-2518) may apply as well.

[2518] "It is a defense to a prosecution under subsection (a) of this section that the defendant was a law enforcement or investigative officer engaged in the course of his official duties and the electronic surveillance was authorized by and conducted pursuant to a search warrant or court order of a court of competent jurisdiction," 50 U.S.C. 1809(b).

[2519] "An aggrieved person, other than a foreign power or an agent of a foreign power, as defined in section 1801(a) or (b)(1)(A) of this title, respectively, who has been subjected to an electronic surveillance or about whom information obtained by electronic surveillance of such person has been disclosed or used in violation of section 1809 of this title shall have a cause of action against any person who committed such violation and shall be entitled to recover – (a) actual damages, but not less than liquidated damages of $1,000 or $100 per day for each day of violation, whichever is greater; (b) punitive damages; and (c) reasonable attorney's fees and other investigation and litigation costs reasonably incurred," 50 U.S.C. 1810. Victims are not entitled to injunctive relief, ACLU Foundation of Southern California v. Barr, 952 F.2d 457, 469-70 (D.C.Cir. 1992). The court did not address the question of whether conduct in violation of both FISA and Title III/EPCA might be enjoined under 18 U.S.C. 2520(b)(1). The Sixth Circuit, however, has held that the proscriptions of Title III/ECPA do not apply to interception in this country for foreign intelligence gathering purposes of communications between parties in the United States and those in other nations, ACLU v. National Security Agency, 493 F.3d 644, 680 (6th Cir. 2007), citing, 18 U.S.C. 2511(2)(f).

[2520] "Any person who is aggrieved by any willful violation of . . . section[] 106(a) . . . of the Foreign Intelligence Surveillance Act [relating to the use of information acquired from electronic surveillance under the Act] may commence an action in United States District Court against the United States to recover money damages. In any such action, if a person who is aggrieved successfully establishes a violation of . . . the above special provisions of title 50, the Court may assess as damages – (1) actual damages, but not less than $10,000, whichever amount is greater; and (2) litigation costs, reasonably incurred," 18 U.S.C. 2712(a).

[2521] "If the United States district court pursuant to subsection (f) of this section determines that the surveillance was not lawfully authorized or conducted, it shall, in accordance with the requirements of law, suppress the evidence which was unlawfully obtained or derived from electronic surveillance of the aggrieved person or otherwise grant the motion of the aggrieved person. If the court determines that the surveillance was lawfully authorized and conducted, it

acknowledged, that surveillance conducted under FISA for foreign intelligence purposes may result in admissible evidence of a crime.[2523]

The physical search portion of FISA authorizes the issuance of physical search orders for foreign intelligence gathering purposes, 50 U.S.C. 1821-1829. Its accompanying criminal proscriptions and civil liability provisions, and are identical to those used in the electronic surveillance portion of FISA.[2524]

The pen register/trap & trace portion of FISA declares that information acquired by virtue of a FISA pen register or trap & trade order may only be used and disclosed for lawful purposes and only consistent with use restrictions of 50 U.S.C.1845, 50 U.S.C. 1845(a). There are no criminal penalties for violations of section 1845, but the provisions of 18 U.S.C. 2712, which grant victims a cause of

---

shall deny the motion of the aggrieved person except to the extent that due process requires discovery or disclosure," 50 U.S.C. 1806(g); the language for FISA physical search and pen registers/trap & trace orders is similar, 1825(f), 1845(g); United States v. Campa, 529 F.3d 980, 993 (11th Cir. 2008). The text of 50 U.S.C. 1825(f) and 1845(g) is appended.

[2522] S.Rept. 95-701, at 61 (1978); 50 U.S.C. 1806(b)(". . . such information . . . may only be used in a criminal proceeding with the advance authorization of the Attorney General").

[2523] When FISA required certification that the acquisition of foreign intelligence was "the" purpose for seeking a FISA surveillance order, there was some debate among the courts over how prominent the foreign intelligence purpose had to be in order to permit the evidence it unearthed under a FISA order to be used in a criminal prosecution, United States v. Johnson, 952 F.2d 565, 572 (1st Cir. 1992); United States v. Duggan, 743 F.2d 59, 77 (2d Cir. 1984); United States v. Sarkissian, 841 F.2d 959, 964 (9th Cir. 1988); United States v. Badia, 827 F.2d 1458, 1463 (11th Cir. 1987). The USA PATRIOT Act changed "the purpose" to "a significant purpose," a change which the FISA review court concluded demands only that the government have a "measurable" foreign intelligence purpose when it seeks a FISA surveillance order, In re Sealed Case, 310 F.3d 717, 734-35 (F.I.S.Ct.Rev. 2002); see also, Seamon & Gardner, The Patriot Act and the Wall Between Foreign Intelligence and Law Enforcement, 28 HARVARD JOURNAL OF LAW AND PUBLIC POLICY 319 (2005).

[2524] 50 U.S.C. 1827 ("A person is guilty of an offense if he intentionally – (1) under color of law for the purpose of obtaining foreign intelligence information, executes a physical search within the United States except as authorized by statute . . . ."); 50 U.S.C. 1828 ("An aggrieved person, other than a foreign power or an agent of a foreign power, as defined in section 1801(a) or (b)(1)(A), respectively, of this title, whose premises, property, information, or material has been subjected to a physical search within the United States or about whom information obtained by such a physical search has been disclosed or used in violation of section 1827 of this title shall have a cause of action against any person who committed such violation . . . ."); 18 U.S.C. 2712(a)("Any person who is aggrieved by any willful violation of . . . section[] 305(a) . . . of the Foreign Intelligence Surveillance Act [relating to the use of information acquired from a physical search under the Act] may commence an action in United States District Court against the United States to recover money damages. . . . ").

action against the United States for FISA surveillance and search violations, are equally available to the victims of FISA pen register/trap & trace violations.[2525]

Procedure

Each of the prohibitions mentioned above recognizes a procedure for government use notwithstanding the general ban, usually under judicial supervision. Although Fourth Amendment concerns supply a common theme, the procedures are individually distinctive.

Law Enforcement Wiretapping and Electronic Eavesdropping

Title III/ECPA authorizes both federal and state law enforcement wiretapping and electronic eavesdropping, under court order, without the prior consent or knowledge of any of the participants, 18 U.S.C. 2516 - 2518. At the federal level, a senior Justice Department official must approve the application for the court order.[2526] The procedure is only available where there is probable cause to believe that the wiretap or electronic eavesdropping will produce evidence of one of a long, but not exhaustive, list of federal crimes,[2527] or of the whereabouts of a "fugitive from justice" fleeing from prosecution of one of the offenses on the predicate offense list, 18 U.S.C. 2516(1)(l). Any federal prosecutor may approve an application for a court order under section 2518 authorizing the interception of e-mail or other electronic communications during transmission.[2528]

[2525] "Any person who is aggrieved by any willful violation of . . . section[] 405(a) . . . of the Foreign Intelligence Surveillance Act [relating to the use of information acquired from electronic surveillance under the Act] may commence an action in United States District Court against the United States to recover money damages. In any such action, if a person who is aggrieved successfully establishes a violation of . . . the above special provisions of title 50, the Court may assess as damages – (1) actual damages, but not less than $10,000, whichever amount is greater; and (2) litigation costs, reasonably incurred," 18 U.S.C. 2712(a).

[2526] "The Attorney General, Deputy Attorney General, Associate Attorney General, or any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General or acting Deputy Assistant Attorney General in the Criminal Division specially designated by the Attorney General, may authorize an application to a Federal judge of competent jurisdiction for, and such judge may grant in conformity with section 2518 of this chapter an order authorizing or approving the interception of wire or oral communications by the Federal Bureau of Investigation, or a Federal agency having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of [the predicate offenses]. . ." 18 U.S.C. 2516(1).

[2527] The list appears in 18 U.S.C. 2516(1) the text of which is appended.

[2528] "Any attorney for the Government (as such term is defined for the purposes of the Federal Rules of Criminal Procedure) may authorize an application to a Federal judge of competent jurisdiction for, and such judge may grant, in conformity with section 2518 of this title, an order authorizing or approving the interception of electronic communications by an investigative or law enforcement officer having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of any Federal

At the state level, the principal prosecuting attorney of a state or any of its political subdivisions may approve an application for an order authorizing wiretapping or electronic eavesdropping based upon probable cause to believe that it will produce evidence of a felony under the state laws covering murder, kidnaping, gambling, robbery, bribery, extortion, drug trafficking, or any other crime dangerous to life, limb or property. State applications, court orders and other procedures must at a minimum be as demanding as federal requirements.[2529]

Applications for a court order authorizing wiretapping and electronic surveillance include:

- the identity of the applicant and the official who authorized the application;
- a full and complete statement of the facts including
    - details of the crime,
    - a particular description of nature, location and place where the interception is to occur,[2530]
    - a particular description of the communications to be intercepted, and
    - the identities (if known) of the person committing the offense and of the persons whose communications are to be intercepted;
- a full and complete statement of the alternative investigative techniques used or an explanation of why they would be futile or dangerous;
- a statement of the period of time for which the interception is to be maintained and if it will not terminate upon seizure of the communications sought, a probable cause demonstration that further similar communications are likely to occur;
- a full and complete history of previous interception applications or efforts involving the same parties or places;
- in the case of an extension, the results to date or explanation for the want of results; and
- any additional information the judge may require.[2531]

---

felony," 18 U.S.C. 2516(3). The less demanding procedures of 18 U.S.C. 2701-2711 may be used with respect to e-mail or other electronic communications that are in storage; recourse to subsection 2516(3) is only necessary when wire, oral or electronic communications are to be "intercepted."

[2529] 18 U.S.C. 2516(2). The text of subsection 2516(2) is appended.

[2530] Identification of the place where, or facilities over, which the targeted communications are to occur may be excused where the court finds that the suspect has or will take steps to thwart interception, 18 U.S.C. 2518(11), (12). The text of 18 U.S.C. 2518 is appended.

[2531] 18 U.S.C. 2518(1), (2).

Before issuing an order authorizing interception, the court must find:

- probable cause to believe that an individual is, has or is about to commit one or more of the predicate offenses;
- probable cause to believe that the particular communications concerning the crime will be seized as a result of the interception requested;
- that normal investigative procedures have been or are likely to be futile or too dangerous; and
- probable cause to believe that "the facilities from which, or the place where, the wire, oral, or electronic communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such person."[2532]

Subsections 2518(4) and (5) demand that any interception order include:

- the identity (if known) of the persons whose conversations are to be intercepted;
- the nature and location of facilities and place covered by the order;
- a particular description of the type of communication to be intercepted and an indication of the crime to which it relates;
- the individual approving the application and the agency executing the order;
- the period of time during which the interception may be conducted and an indication of whether it may continue after the communication sought has been seized;
- an instruction that the order shall be executed
    - as soon as practicable, and
    - so as to minimize the extent of innocent communication seized; and
- upon request, a direction for the cooperation of communications providers and others necessary or useful for the execution of the order.[2533]

Compliance with these procedures may be postponed briefly until after the interception effort has begun, upon the approval of senior Justice Department officials in emergency cases involving organized crime or national security threatening conspiracies or involving the risk of death or serious injury (7).[2534]

The court orders remain in effect only as long as required but not more than 30 days. After 30 days, the court may grant 30 day extensions subject to the

---

[2532] 18 U.S.C. 2518(3).

[2533] 18 U.S.C. 2518(4).

[2534] 18 U.S.C. 2518(7).

procedures required for issuance of the original order.[2535] During that time the court may require progress reports at such intervals as it considers appropriate.[2536] Intercepted communications are to be recorded and the evidence secured and placed under seal (with the possibility of copies for authorized law enforcement disclosure and use) along with the application and the court's order.[2537]

Within 90 days of the expiration of the order those whose communications have been intercepted are entitled to notice, and evidence secured through the intercept may be introduced into evidence with 10 days' advance notice to the parties.[2538]

Title III also circumscribes the conditions under which information derived from a court ordered interception may be disclosed or otherwise used. Nevertheless, it may be disclosed to and used for official purposes by:

- other law enforcement officials including foreign officials;[2539]
- federal intelligence officers to the extent that it involves foreign intelligence information;[2540]
- other American or foreign government officials to the extent that it involves the threat of hostile acts by foreign powers, their agents, or international terrorists.[2541]

It may also be disclosed by witnesses testifying in federal or state proceedings,[2542] provided the intercepted conversation or other communication is not privileged.[2543]

[2535] 18 U.S.C. 2518(5).

[2536] 18 U.S.C. 2518(6).

[2537] 18 U.S.C. 2518(8)(a),(b).

[2538] 18 U.S.C. 2518(8)(d), (9).

[2539] 18 U.S.C. 2517(1), (2), (5), (7).

[2540] 18 U.S.C. 2517(6). "'[F]oreign intelligence information', for purposes of section 2517(6) of this title, means – (A) information, whether or not concerning a United States person, that relates to the ability of the United States to protect against – (i) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power; (ii) sabotage or intentional terrorism by a foreign power or an agent of a foreign power; or (iii) clandestine intelligence activities by and intelligence service or network of a foreign power or by an agent of a foreign power; or (B) information, whether or not concerning a United States person, with respect to a foreign power or foreign territory that relates to – (i) the national defense or the security of the United States; or (ii) the conduct of the foreign affairs of the United States," 18 U.S.C. 2510(19).

[2541] 18 U.S.C. 2578(8).

Stored Electronic or Wire Communications

The procedural requirements for law enforcement access to stored wire or electronic communications and transactional records are less demanding but equally complicated, 18 U.S.C. 2701-2712. They deal with two kinds of information – often in the custody of the telephone company or some other service provider rather than of any of the parties to the communication – communications records and the content of electronic or wire communications. Law enforcement officials are entitled to access:

- with the consent of the one of the parties;[2544]
- on the basis of a court order or similar process under the procedures established in Title III/ECPA;[2545]
- in certain emergency situations;[2546] or
- under one of the other statutory exceptions to the ban on service provider disclosure.[2547]

[2542] 18 U.S.C. 2517(3), (5).

[2543] 18 U.S.C. 2517(4).

[2544] "(b) A provider described in subsection (a) may divulge the contents of a communication . . . (3) with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service. . . . (c) . . . A provider described in subsection (a) may divulge a record or other information pertaining to a subscriber to or customer of such service, (not including the contents of communications covered by subsection (a)(1) or (a)(2)) . . . (2) with the lawful consent of the customer or subscriber. " 18 U.S.C. 2702(b)(3),(c)(2).

[2545] "A provider described in subsection (a) may divulge the contents of a communication . . . (2) as otherwise authorized in section 2517, 2511(2)(a), or 2703 . . . .(c) . . . A provider described in subsection (a) may divulge a record or other information pertaining to a subscriber to or customer of such service, (not including the contents of communications covered by subsection (a)(1) or (a)(2)) (1) as otherwise authorized in section 2703," 18 U.S.C. 2702(b)(2), (c)(1).

[2546] "(b) A provider described in subsection (a) may divulge the contents of a communication . . . (8) to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency. (c) . . . A provider described in subsection (a) may divulge a record or other information pertaining to a subscriber to or customer of such service, (not including the contents of communications covered by subsection (a)(1) or (a)(2)) . . .(4) to a government entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of the information relating to the emergency," 18 U.S.C. 2702(b)(8),(c)(4).

[2547] "(b) A provider described in subsection (a) may divulge the contents of a communication — (1) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient; . . . (4) to a person employed or authorized or whose facilities are used to forward such communication to its destination; (5) as may be necessarily incident to the rendition

Section 2703, which affords law enforcement access to the content of stored wire and electronic communications, distinguishes between recent communications and those that have been in electronic storage for more than six months. Government officials may gain access to wire or electronic communications in electronic storage for less than six months under a search warrant issued upon probable cause to believe a crime has been committed and the search will produce evidence of the offense.[2548]

The government must use the same warrant procedure to acquire older communications or those stored in remote computer storage if access is to be afforded without notice to the subscriber or customer.[2549] If government officials are willing to afford the subscriber or customer notice or at least delayed notice, access may be granted under a court order showing that the information sought is relevant and material to a criminal investigation or under an administrative subpoena, a grand jury subpoena, a trial subpoena, or court order.[2550]

Under the court order procedure, the court may authorize delayed notification in 90 day increments when contemporaneous notice might have an adverse impact.[2551] Government supervisor officials may certify the need for delayed

---

of the service or to the protection of the rights or property of the provider of that service; (6) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 227 of the Victims of Child Abuse Act of 1990; (7) to a law enforcement agency – (A) if the contents – (I) were inadvertently obtained by the service provider; and (ii) appear to pertain to the commission of a crime . . . (c) . . . A provider described in subsection (a) may divulge a record or other information pertaining to a subscriber to or customer of such service, (not including the contents of communications covered by subsection (a)(1) or (a)(2)) . . . (3) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service," 18 U.S.C. 2702(b)(1),(4),(5),(6),(7); (c)(3).

[2548] 18 U.S.C. 2703(a)(text is appended). The 21st Century Department of Justice Appropriations Authorization Act, 116 Stat. 1822 (2002), amended section 2703 to permit execution of the warrant by service providers and others without requiring the presence of a federal officer, 18 U.S.C. 2703(g)("Notwithstanding section 3105 of this title, the presence of an officer shall not be required for service or execution of a search warrant issued in accordance with this chapter requiring disclosure by a provider of electronic communications service or remote computing service of the contents of communications or records or other information pertaining to a subscriber to or customer of such service"), see United States v. Bach, 310 F.3d 1063 (8th Cir. 2002)(the Fourth Amendment does not require the presence of a federal officer when technicians execute a search warrant on a service provider's server).

[2549] 18 U.S.C. 2703(a), (b)(1)(A), (b)(2) (text is appended).

[2550] 18 U.S.C. 2703(b)(1)(B), (d) (text is appended); United States v. Weaver, 636 F.supp.2d 769, 773 (C.D. Ill. 2009).

[2551] 18 U.S.C. 2705(a)(1)(A), (4) (text is appended).

notification in the case of a subpoena.[2552] Traditional exigent circumstances and a final general inconvenience justification form the grounds for delayed notification in either case:

- endangering the life or physical safety of an individual;
- flight from prosecution;
- destruction of or tampering with evidence;
- intimidation of potential witnesses; or
- otherwise seriously jeopardizing an investigation or unduly delaying a trial.[2553]

Comparable, if less demanding, procedures apply when the government seeks other customer information from a service provider (other than the content of a customer's communications). The information can be secured:

- with a warrant;
- with a court order;
- with customer consent;
- with a written request in telemarketing fraud cases; or
- with a subpoena in some instances.[2554]

Most customer identification, use, and billing information can be secured simply with a subpoena and without customer notification.[2555]

[2552] 18 U.S.C. 2705(a)(1)(B), (4) (text is appended).

[2553] 18 U.S.C. 2705(a)(2), (b). A Sixth Circuit panel, in a decision later vacated en banc on grounds of ripeness, held that the Fourth Amendment precluded the seizure of stored e-mail from a service provider under a section 2703 court order which featured a delayed notice authorization under section 2705, Warshak v. United States, 490 F.3d 455, 468-82 (6th Cir. 2007), vac'd en banc, 532 F.3d 521 (6th Cir. 2008). The panel did not address whether exigent circumstances would permit seizure with delayed notice, perhaps because the government apparently did not raise the question, 490 F.3d at 464-65.

[2554] "(1) A government entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) – (A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant; (B) obtains a court order for such disclosure under subsection (d) of this section; (C) has the consent of the subscriber or customer to such disclosure; or (D) submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud for the name, address, and place of business of a subscriber or customer of such provider, which subscriber or customer is engaged in telemarketing (as such term is defined in section 2325 of this title); or (E) seeks information under paragraph (2) . . . (3) A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer," 18 U.S.C. 2703(c)(1),(3).

Pen Registers and Trap and Trace Devices

Pen registers and trap and trace devices identify the source of calls placed to or from a particular telephone. Federal government attorneys and state and local police officers may apply for a court order authorizing the installation and use of a pen register and/or a trap and trace device upon certification that the information that it will provide is relevant to a pending criminal investigation.[2556]

An order authorizing installation and use of a pen register or trap and trace device must:

- specify
  - the person (if known) upon whose telephone line the device is to be installed,
  - the person (if known) who is the subject of the criminal investigation,
  - the telephone number, (if known) the location of the line to which the device is to be attached, and geographical range of the device,
  - a description of the crime to which the investigation relates;
- upon request, direct carrier assistance pursuant to section 3124;
- terminate within 60 days, unless extended;
- involve a report of particulars of the order's execution in Internet cases; and
- impose necessary nondisclosure requirements.[2557]

Senior Justice Department or state prosecutors may approve the installation and use of a pen register or trap and trace device prior to the issuance of court authorization in emergency cases that involve either an organized crime

---

[2555] "(2) A provider of electronic communication service or remote computing service shall disclose to a governmental entity the (A) name; (B) address; (C) local and long distance telephone connection records, or records of session times and durations; (D) length of service (including start date) and types of service utilized; (E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and (F) means and source of payment (including any credit car or bank account number), of a subscriber to or customer of such service, when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under paragraph (1). (3) A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer," 18 U.S.C. 2703(c)(2),(3).

[2556] 18 U.S.C. 3122 (text is appended).

[2557] 18 U.S.C. 3123 (text is appended).

conspiracy, an immediate danger of death or serious injury, a threat to national security, or a serious attack on a "protected computer."[2558]

Federal authorities have applied for court orders, under the Stored Communications Act (18 U.S.C. 2701-2712) and the trap and trace authority of 18 U.S.C. 3121-3127, seeking to direct communications providers to supply them with the information necessary to track cell phone users in conjunction with an ongoing criminal investigation. Thus far, their efforts have met with mixed success.[2559]

Foreign Intelligence Surveillance Act

The procedure for securing wiretapping court orders under the Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. 1801-1811, is the most distinctive of the wiretap-related procedures.[2560] First, its focus is different. It was designed to secure foreign intelligence information – not evidence of a crime.[2561] Second, it operates in a highly secretive manner. But its most individualistic feature is that the procedure is conducted entirely before members of an independent court convened for no other purpose. The Act operates in the field of foreign intelligence gathering, primarily through a Foreign Intelligence Surveillance Court whose judges grant or reject petitions for wiretap and electronic surveillance orders, orders authorizing physical searches and seizures, pen register and trap and trace orders, and orders relating to the surrender of tangible items.

[2558] 18 U.S.C. 3125 (text is appended).

[2559] E.g., In re Application of the United States, 534 F.Supp.2d 585 (W.D.Pa. 2008); In re Application of the United States, 497 F.Supp.2d 301 (D. P.R. 2007); In re United States, 441 F.3d 816 (S.D. Tex. 2006); In re Application of the United States, 416 F.Supp. 390 (D.Md. 2006); In re Application of the United States, 415 F.Supp.2d 211 (W.D.N.Y. 2006); In re Application of the United States, 412 F.Supp.2d 947 (E.D.Wis. 2006); In re Application of the United States, 407 F.Supp.2d 134 (D.D.C. 2006) (each denying the application); but see, In re Application of the United States, 632 F.Supp.2d 202 (E.D.N.Y. 2008); In re Application of the United States, 509 F.Supp.2d 76 (D.Mass. 2007); In re Application of the United States, 460 F.Supp.2d 448 (S.D.N.Y. 2006); In re Application of the United States, 433 F.Supp.2d 804 (S.D. Tex. 2006); In re Application of the United States, 411 F.Supp.2d 678 (W.D.La. 2006).

[2560] See generally, CRS Report RL30465, The Foreign Intelligence Surveillance Act: An Overview of the Statutory Framework and U.S. Foreign Intelligence Surveillance Court and U.S. Foreign Intelligence Surveillance Court of Review Decisions, by Elizabeth B. Bazan.

[2561] In its original form, gathering foreign intelligence was "the" purpose for which FISA surveillance orders were sought, 50 U.S.C. 1804(a)(7)(B) (1982 ed.). Although amended by the USA PATRIOT Act, gathering foreign intelligence must still provide a "significant" reason for seeking a FISA surveillance order, 50 U.S.C. 1804(a)(7)(B); In re Sealed Case, 310 F.3d 717, (F.I.S.Ct.Rev. 2002); United States v. Ning Wen, 477 F.3d 896, 897 (7th Cir. 2007).

The Foreign Intelligence Surveillance Court (FISC) is comprised of eleven federal court judges designated by the Chief Justice to sit on the FISC for a single seven year term.[2562] In the area of wiretaps and physical searches,[2563] the judges of the FISC individually receive and approve or reject requests,[2564] authorized by the Attorney General, to conduct the four specific types of electronic surveillance noted earlier[2565] of the communications and activities of foreign powers.[2566]

The contents of FISA application include:

- the identity of the individual submitting the application;
- the identity or a description of the person whose communications are to be intercepted;
- an indication of
    - why the person is believed to be a foreign power or the agent of a foreign power, and

---

[2562] 50 U.S.C. 1803(a),(b),(d) (text is appended).

[2563] The FISA procedures relating to wiretapping and electronic surveillance orders, 50 U.S.C. 1801-1811, and those relating to physical searches, 50 U.S.C. 1821-1829, are virtually identical and consequently are treated together here.

[2564] P.L. 110-261 explicitly granted the FISA court judges the authority to sit as a group on their own initiative or on the petition of the government when a majority of court concludes that a particular matter is exceptional significance or in order uniformity of interpretation among the members of the court, 50 U.S.C. 1803(a)(2).

[2565] 50 U.S.C. 1801(f)(text is appended). The courts have noted that, unlike surveillance under Title III/EPCA, silent video surveillance falls within the purview of FISA by virtue of subsection 1801(f)(4), United States v. Koyomejian, 970 F.2d 536, 540 (9th Cir. 1992); United States v. Mesa-Rincon, 911 F.2d 1433, 1438 (10th Cir. 1990); United States v. Biasucci, 786 F.2d 504, 508 (2d Cir. 1986).

[2566] "'Foreign power' means – (1) a foreign government or any component thereof, whether or not recognized by the United States; (2) a faction of a foreign nation or nations, not substantially composed of United States persons; (3) an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments; (4) a group engaged in international terrorism or activities in preparation therefor; (5) a foreign-based political organization, not substantially composed of United States persons; (6) an entity that is directed and controlled by a foreign government or governments; or an entity not substantially composed of United States persons that is engaged in the international proliferation of weapons of mass destruction," 50 U.S.C. 1801(a)(language in italics added in P.L. 110-261). Note that the definition of foreign power includes international terrorists groups regardless of whether any nexus to a foreign power can be shown, 50 U.S.C. 1801(a)(4) and includes agents of foreign powers that no longer exist, United States v. Squillacote, 221 F.3d 542, 554 (4th Cir. 2000) (agents of East Germany intercepted under an order granted after unification). Moreover, at least until it expires on December 31, 2009, the definition of "agent of foreign power" (50 U.S.C.1801(b)(1)(c)) includes international terrorists with no necessary to connection to a foreign power or group. The FISA physical search provisions adopt by cross reference the definitions of "foreign power" and "agent of a foreign power," 50 U.S.C. 1821(1).

    - why foreign powers or their agents are believed to use the targeted facilities or places;
- a summary of the minimization procedures[2567] to be followed;
- a description of the communications to be intercepted and the information sought;[2568]
- certification by a senior national security or senior defense official designed by the President that
    - the information sought is foreign intelligence information,
    - a significant purpose of interception is to secure foreign intelligence information,
    - the information cannot reasonably be obtained using alternative means,[2569]
- a summary statement of the means of accomplishing the interception (including whether a physical entry will be required);[2570]
- a history of past interception applications involving the same persons, places or facilities;
- the period of time during which the interception is to occur, whether it will terminate immediately upon obtaining the information sought, and if not, the reasons why interception thereafter is likely to be productively intercepted.[2571]

[2567] "Minimization procedures" are defined in 50 U.S.C. 1801(h). They are essentially those procedures designed to minimize the unnecessary acquisition, retention, and dissemination of information relating to U.S. persons (American citizens, permanent resident aliens, U.S. corporations, and organizations a substantial number of whose members are Americans). Like the procedures in Title III, they are crafted to minimize the amount of "innocent" communications captured with the communications which are the target of the order and require a good faith effort on the part of the government to avoid the capture and retention of irrelevant material, United States v. Hammoud, 381 F.3d 316, 334 (4th Cir. 2004), vac'd on other grounds, 543 U.S. 1097 (2004), reinstated in pertinent part after remand, 405 F.3d 1034 (4th Cir. 2005); United States v. Rosen, 447 F.Supp.2d 538, 550-51 (E.D.Va. 2006).

[2568] Section 104(a)(1)(c) of P.L. 110-261 eliminated the requirement of a "detailed" description.

[2569] Section 104(a)(1)(D) of P.L. 110-261 authorized the President to designate the Deputy Director of the Federal Bureau of Investigation as a certifying official as well.

[2570] Section 104(a)(1)(E) of P.L. 11-261 added that the statement need only be "summary."

[2571] 50 U.S.C. 1804 (text is appended). 50 U.S.C. 1823 relating to applications for a FISA physical search order is essentially the same. Section 104(a)(1)(A) of P.L. 110-261 eliminated the requirement that the application indicate that the Attorney General approved the application and that the President had authorized him to do so. It also eliminated the requirement that the application indicate whether more than one interception device was to be used and if so their range and the minimization procedures associated with each. Section 104(a)(2) of P.L. 110-261, however, repealed the language once found in 50 U.S.C. 1804(b) which, when the target of the surveillance was a foreign power, excused the inclusion of multiple device information, of a statement of the means of execution, of a statement relating to the basis for the "last resort" and

FISA court judges issue orders approving electronic surveillance or physical searches upon a finding that the application requirements have been met and that there is probable cause to believe that the target is a foreign power or the agent of a foreign power and that the targeted places or facilities are used by foreign powers of their agents.[2572]

Orders approving electronic surveillance must:

- specify
  - the identity or a description of the person whose communications are to be intercepted,
  - the nature and location of the targeted facilities or places, if known,
  - type of communications or activities targeted and the kind of information sought,
  - the means by which interception is to be accomplished and whether physical entry is authorized,
  - the tenure of the authorization, and
  - whether more than one device are to be used and if so their respective ranges and associated minimization procedures;
- require
  - that minimization procedures be adhered to,
  - upon request, that carriers and others provide assistance,[2573]
  - that those providing assistance observe certain security precautions, and be compensated;[2574]

---

foreign intelligence information certifications, and of a description of the information sought and the type of communications targeted.

[2572] 50 U.S.C. 1805(a) (text is appended); 50 U.S.C. 1824(a) is to the same effect with respect to physical search orders.

[2573] "An order approving an electronic surveillance under this section shall . . . (2) direct – (B) that, upon the request of the applicant, a specified communication or other common carrier, landlord, custodian, or other specified person, or in circumstances where the Court finds that the actions of the target of the application may have the effect of thwarting the identification of a specified person, such other persons, furnish the applicant forthwith all information, facilities, or technical assistance necessary to accomplish the electronic surveillance in such a manner as will protect its secrecy and produce a minimum of interference with the services that such carrier, landlord, custodian, or other person is providing that target of electronic surveillance," 50 U.S.C. 1805(c)(2)(B). By virtue of section 102(b) of the USA PATRIOT Improvement and Reauthorization Act, the language in italics expires on December 31, 2009, unless statutorily extended or made permanent, P.L. 109-177, §102(b), 120 Stat. 195 (2006).

[2574] 50 U.S.C. 1805(c)(2)(C),(D); 50 U.S.C. 1824(c)(2)(C),(D)(text is appended). FISA physical search orders must also direct "the federal officer conducting the physical search promptly report to the court the circumstances and results of the physical search," 50 U.S.C. 1824(c)(2)(E).

- direct the applicant to advise the court of the particulars relating to surveillance directed at additional facilities and places when the order permits surveillance although the nature and location of targeted facilities and places were unknown at the time of issuance;
- expire when its purpose is accomplished but not later than after 90 days generally (after 120 days in the case of certain foreign agents and after a year in the case of foreign governments or their entities or factions of foreign nations) unless extended (extensions may not exceed one year).[2575]

As in the case of law enforcement wiretapping and electronic eavesdropping, there is authority for interception and physical searches prior to approval in emergency situations,[2576] but there is also statutory authority for foreign intelligence surveillance interceptions and physical searches without the requirement of a court order when the targets are limited to communications among or between foreign powers or involve nonverbal communications from places under the open and exclusive control of a foreign power.[2577] The second of these is replete with reporting requirements to Congress and the FISA court.[2578] These and the twin war time exceptions[2579] may be subject to constitutional limitations, particularly when Americans are the surveillance targets.[2580]

The USA PATRIOT Act's amendments make it clear that those who provide such assistance are immune from civil suit, 18 U.S.C. 1805(i) ("No cause of action shall lie in any court against any provider of a wire or electronic communication service, landlord, custodian, or other persons (including any officer, employee, agent, or other specified person thereof) that furnishes any information, facilities, or technical assistance in accordance with a court order or request for emergency assistance under this Act for electronic surveillance or physical search"). As discussed at greater length later, P.L. 110-261 affords service providers retroactive protection for foreign intelligence assistance provided outside the confines of FISA.

[2575] 50 U.S.C. 1805(c); 1824(c) (text is appended).

[2576] 50 U.S.C. 1805(f); 1824(e) (text is appended). P.L. 110-261 extends the permissible length of emergency authorizations absent court approval from 72 hours to 7 days. It also removes earlier language which called for review of a FISA court denial of an application to approve an emergency authorization. Finally, it states that the Attorney General is to assess compliance with the statutory provisions which permit use of the information secured under an authorization which fails to secure judicial approval.

[2577] 50 U.S.C. 1802(a)(1),(4); 1822(a)(1), (4) (text is appended).

[2578] 50 U.S.C. 1802(a)(2),(3); 1822(a)(2), (3) (text is appended).

[2579] "Notwithstanding any other law, the President, through the Attorney General, may authorize electronic surveillance without a court order under this subchapter to acquire foreign intelligence information for a period not to exceed fifteen calendar days following a declaration of war by the Congress," 50 U.S.C. 1811.

"Notwithstanding any other provision of law, the President, through the Attorney General, may authorize physical searches without a court order under this subchapter to acquire foreign

FISA has detailed provisions governing the use of the information acquired through the use of its surveillance or physical search authority that include:

- confidentiality requirements, 50 U.S.C. 1806(a), 1825(a);
- notice of required Attorney General approval for disclosure, 50 U.S.C. 1806(b), 1825(b);
- notice to the "aggrieved" of the government's intention to use the results as evidence, 50 U.S.C. 1806(c),(d), 1825(c),(d);
- suppression procedures, 50 U.S.C. 1806(e), (f), (g), (h), 1825(e), (f), (g), (h);[2581]
- inadvertently captured information, 50 U.S.C. 1806(I), 1825(b);
- notification of emergency surveillance or search for which no FISA order was subsequently secured, 50 U.S.C. 1806(j), 1825(j); and
- clarification that those who execute FISA surveillance or physical search orders may consult with federal and state law enforcement officers, 50 U.S.C. 1806(k), 1825(k).

Both the surveillance and the physical search authorities are subject to Congressional oversight in the form of semiannual reports on the extent and circumstances of their use.[2582]

Pen Registers and Trap and Trace Devices

FISA pen register and trap and trace procedures, 50 U.S.C. 1841-1846, are similar to those of their law enforcement counterparts, but with many of the attributes of other FISA provisions. The orders may be issued either by a member of the FISA court or by a FISA magistrate upon the certification of a federal officer that the information sought is likely to be relevant to an investigation of international

---

intelligence information for a period not to exceed 15 calendar days following a declaration of war by the Congress," 50 U.S.C. 1829.

[2580] Over the years, however, the vast majority of courts have rejected the suggestion that FISA is vulnerable to constitutional attack on Fourth Amendment grounds or any other, In re Sealed Case, 310 F.3d 717, 737-46 (F.I.S.Ct.Rev. 2002); United States v. Damrah, 412 F.3d 618, 624-25 (6th Cir. 2005); United States v. Mubayyid, 521 F.Supp.2d 125, 135-36 (D. Mass. 2007); United States v. Benkahla, 437 F.Supp.2d 541, 554-55 (E.D.Va. 2006); contra, Mayfield v. United States, 504 F.Supp.2d 1023, 1036-43 (D. Ore. 2007).

[2581] Consideration of a motion to suppress occurs ex parte and in camera when the government files a notice that national security would otherwise be compromised, 50 U.S.C. 1806(f); In re Grand Jury Proceedings, 347 F.3d 197, 203 (7th Cir. 2003); United States v. Damrah, 412 F.3d 618, 623-24 (6th Cir. 2005); review is the same as that afforded by the FISA court, statutory compliance; there is no authority to "second guess the executive branches certification," In re Grand Jury Proceedings, 347 F.3d 197, 204-205 (7th Cir. 2003); United States v. Campa, 529 F.3d 980, 993 (11th Cir. 2008); United States v. Amawi, 531 F.Supp.2d 832, 837 (N.D. Ohio 2008); United States v. Abu-Jihaad, 531 F.Supp.2d 299, 312 (D.Conn. 2008).

[2582] 50 U.S.C. 1808, 1826.

terrorism or clandestine intelligence activities.[2583] The order may direct service providers to supply customer information related to the order.[2584] The statute allows the Attorney General to authorize emergency installation and use as long as an application is filed within 48 hours,[2585] and restricts the use of any resulting evidence if an order is not subsequently granted.[2586] The provisions for use of the information acquired run parallel to those that apply to FISA surveillance and physical search orders.[2587] The USA PATRIOT Improvement and Reauthorization Act increased the level of Congressional oversight by requiring that the semiannual report on the government's recourse to FISA pen register/trap and trace authority including statistical information on the extent of its use.[2588]

Tangible Items

FISA's tangible item orders, 50 U.S.C. 1861, are perhaps its most interesting feature. Prior to the USA PATRIOT Act, senior FBI officials could approve an application to a FISA judge or magistrate for an order authorizing common carriers, or public accommodation, storage facility, or vehicle rental establishments to release their business records based upon certification of a reason to believe that the records pertained to a foreign power or the agent of a foreign power.[2589] The USA PATRIOT Act and later the USA PATRIOT Improvement and Reauthorization Act temporarily rewrote the procedure. In its temporary form, it requires rather than authorizes access; it is predicated upon relevancy rather than probable cause; it applies to all tangible property (not merely records); and it applies to the tangible property of both individuals or organizations, commercial and otherwise.[2590] It is limited, however, to investigations conducted to secure foreign intelligence information or to protect against international terrorism or clandestine intelligence activities.[2591]

[2583] 50 U.S.C. 1842.

[2584] 50 U.S.C. 1842.(d)(2)(C).

[2585] 50 U.S.C. 1843.

[2586] 50 U.S.C. 1843(c)(2).

[2587] 50 U.S.C. 1845.

[2588] 50 U.S.C. 1846.

[2589] 50 U.S.C. 1862 (2000 ed.).

[2590] Unless legislative extended, the authority reverts to its pre-USA PATRIOT Act form on December 31, 2009, 50 U.S.C. 1861 note; P.L. 109-177, §102(b), 120 Stat. 195 (2006).

[2591] 50 U.S.C. 1861(a).

Recipients are prohibited from disclosing the existence of the order, but are expressly authorized to consult an attorney with respect to their rights and obligations under the order.[2592] They enjoy immunity from civil liability for good faith compliance.[2593] They may challenge the legality of the order and/or ask that its disclosure restrictions be lifted or modified.[2594] The grounds for lifting the secrecy requirements are closely defined, but petitions for reconsideration may be filed annually.[2595] The decision to set aside, modify or let stand either the disclosure restrictions of an order or the underlying order itself are subject to appellate review.[2596]

As addition safeguards, Congress has:

- insisted upon the promulgation of minimization standards, 50 U.S.C. 1861(g);
- established use restrictions, 50 U.S.C. 1861(h),
- required the approval of senior officials in order to seek orders covering the records of libraries and certain other types of records, 50 U.S.C. 1861(a)(3);
- confirmed and reinforced reporting requirements, 50 U.S.C. 1862; and
- directed the Justice Department's Inspector General to conduct an audit of the use of the FISA tangible item authority, P.L. 109-177, §106A, 120 Stat. 200-202 (2006).

Protect America Act (Expired)

The Protect America Act (Protect Act) granted the Attorney General and the Director of National Intelligence the power, under limited conditions, to authorize gathering foreign intelligence information,[2597] other than by electronic

---

[2592] 50 U.S.C. 1861(d).

[2593] 50 U.S.C. 1861(e).

[2594] 50 U.S.C. 1861(f).

[2595] 50 U.S.C. 1861(f)(2)(C)(iii).

[2596] 50 U.S.C. 1861(f)(3),(4),(5).

[2597] "'Foreign intelligence information' means – (1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against – (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power; (B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or (2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to – (A) the national defense or the security of the United States; or (B) the conduct of the foreign affairs of the United States," 50 U.S.C.

surveillance, (for up to a year) relating to persons believed to be overseas.[2598] In order to exercise that power, the Attorney General and the Director of National Intelligence were required to certify under oath that the collection effort involved:

- procedures reasonably calculated to assure that the information sought concerned a person outside the United States;
- communications to which service providers or others had access;
- a desire, at least in significant part, to gather foreign intelligence information;
- accompanying minimization procedures; and
- no electronic surveillance other than that directed at a person reasonably believed to be abroad, 50 U.S.C. 1805b(a)(expired).[2599]

That having been done or in emergency situations with their oral approval,[2600] the Attorney General and Director of National Intelligence might direct the communications providers, or others with access, to immediately assist in the gathering of the foreign intelligence information in a manner least disruptive of service to the target and under confidentiality restrictions imposed by the Attorney General and the Director of National Intelligence, 50 U.S.C. 1805b(e)(expired). The directive came with the promise of compensation at prevailing rates as well as immunity from civil liability and was enforceable through the contempt power of the FISA court, 50 U.S.C. 1805b(f), (g), (l)(expired). Recipients were entitled to seek judicial modification of a directive, issued contrary to the statute or otherwise unlawfully, in the FISA court under expedited procedures, 50 U.S.C. 1805b(h), (I), (j), (k) (expired).

1801(e)(language in italics added by P.L. 110-261 did not apply when the Protect Act was in effect).

[2598] P.L. 110-55, §§2, 3, 121 Stat. 552 (2007), 50 U.S.C. 1805a - 1805c. By operation of section 6(c) of the Public Law, sections 2, 3, 4, and 5 expired 180 days after enactment; the deadline was extended to 195 days on January 31, 2008, by P.L. 110-182, 122 Stat. 605 (2008); and the sections expired when the deadline ran out in mid-February. Section 6(b) of the Act provides that orders issued and extended under the authority of the Act remain in effect until they expire under the terms of the order, the Act, and the FISA provisions in effect when they were issued. See generally, CRS Report RL34143, P.L. 110-55, the Protect America Act of 2007: Modifications to the Foreign Intelligence Surveillance Act, by Elizabeth B. Bazan.

[2599] Section 1805b(a)(2) simply called for a determination that "the acquisition does not constitute electronic surveillance," but section 1805a had declared that "nothing in the definition of electronic surveillance under section 101(f)[which provides the definition of terms used in the subchapter in which section 1805b is found] shall be construed to encompass surveillance directed at a person reasonably believed to be located outside the United States."

[2600] In emergency situations, information gathering could begin prior certification under oral instructions as long as minimization procedures were followed and certification was provided within 72 hours, 50 U.S.C. 1805b(a), (d)(expired).

The FISA court was also tasked with the responsibility of reviewing the procedures crafted to ensure that the authority was only invoked with respect to persons reasonably believed to be found overseas, 50 U.S.C. 1805c(expired). Should the court have determined that the procedures were clearly erroneous, the government was free to amend them or to appeal the determination initially to the Foreign Intelligence Surveillance Court of Review and then to the Supreme Court, id.[2601]

Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008 (P.L. 110-261)

P.L. 110-261 (H.R. 6304), signed July 10, 2008, repeals the Protect America Act and addresses four FISA-related matters.[2602] First, in a manner reminiscent of the Protect Act, it provides temporary authority to gather foreign intelligence information from overseas targets.[2603] Second, it reasserts the exclusivity of FISA and Title III/ECPA as a basis for governmental electronic surveillance.[2604] Third, it instructs the Inspectors General in various agencies to conduct a review and report to Congress on the Terrorist Surveillance Program.[2605] Fourth, it seeks to protect those who assist government surveillance activities from civil liability.[2606]

Overseas Targets

P.L. 110-261 repeals the Protect Act.[2607] Yet like the Protect Act, it establishes a temporary set of three procedures to authorize the acquisition of foreign

---

[2601] The Foreign Intelligence Surveillance Court of Review found that the Protect America Act as applied satisfied Fourth Amendment reasonableness requirements, In re Directives [Redacted] Pursuant to Section 105B, 551 F.3d 1004, 1009-16 (F.I.S.C. Rev. 2008).

[2602] For a general discussion of the debate leading up to enactment see CRS Report RL34279, The Foreign Intelligence Surveillance Act: An Overview of Selected Issues, by Elizabeth B. Bazan.

[2603] 50 U.S.C. 1881-1881g.

[2604] 50 U.S.C. 1812 ("(a) Except as provided in subsection (b), the procedures of chapters 119, 121, and 206 of title 18, United States Code, and this Act shall be the exclusive means by which electronic surveillance and the interception of domestic wire, oral, or electronic communications may be conducted. (b) Only an express statutory authorization for electronic surveillance or the interception of domestic wire, oral, or electronic communications, other than as an amendment to this Act or chapters 119, 121, or 206 of title 18, United States Code, shall constitute an additional exclusive means for the purpose of subsection (a)").

[2605] P.L. 110-261, tit. III, 122 Stat. 2471 (2008).

[2606] P.L. 110-261, tit. II, 122 Stat. 2467 (2008); 50 U.S.C. 1885-1885c (text is appended). For a general discussion of the immunity provisions see CRS Report RL34600, Retroactive Immunity Provided by the FISA Amendments Act of 2008, by Edward C. Liu.

[2607] P.L. 110-261, §403(a)(1)(A), 122 Stat. 2473 (2008)(repealing 50 U.S.C. 1805a, 1985b, and 1805c).

intelligence information by targeting an individual or entity thought to be overseas.[2608] One, 50 U.S.C. 1881a, applies to the targeting of an overseas person or entity that is not a U.S. person.[2609] Another, 50 U.S.C. 1881b, covers situations when the American target is overseas but the gathering involves electronic communications or stored electronic communications or data acquired in this country.[2610] The third, 50 U.S.C. 1881c, applies to situations when the American target is overseas, but section 1881b is not available, either because acquisition occurs outside of the United States or because it involves something other than electronic surveillance or the acquisition of stored communications or data, e.g., a physical search.[2611]

In the case of targets who are not U.S. persons, section 1881a(a) declares "upon the issuance of an order in accordance with subsection (i)(3) or a determination under subsection (c)(2), the Attorney General and the Director of National Intelligence may authorize jointly, for a period of up to 1 year from the effective date of the authorization, the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information." It makes no mention of authorizing acquisition. It merely speaks of targeting with an eye to acquisition. Moreover, it gives no indication of whether the anticipated methods of acquisition include the capture of a target's communications, of communications relating to a target, of communications of a person or entity related to the target, or information concerning one of the three. The remainder of the section, however, seems to dispel some of the questions. Section 1881a is intended to empower the Attorney General and the Director of National Intelligence to authorize the acquisition of foreign intelligence information and the methods that may be used to the capture of communications and related information.

The procedure begins either with a certification presented to the FISA court for approval or with a determination by the two officials that exigent circumstances warrant timely authorization prior to court approval.[2612] In the certification process, they must assert in writing and under oath that:

[2608] Sections 1881a-1881g are repealed effective December 31, 2012, P.L. 110-261, §403(b)(1), 122 Stat. 2474 (2008).

[2609] "United States person" includes United States citizens, permanent resident aliens of the United States, corporations incorporated in the United States, and unincorporated associates made up of a substantial number of U.S. citizens, 50 U.S.C. 1881(a), 1801(j).

[2610] 50 U.S.C. 1881b.

[2611] 50 U.S.C. 1881c.

[2612] 50 U.S.C. 1881a(a), (i)(3), (c)(2).

- a significant purpose for the effort is the acquisition of foreign intelligence information
- the effort will involve the assistance of an electronic communication service provider
- the court has approved, or is being asked to approve, procedures designed to ensure that acquisition is limited to targeted persons found outside the U.S. and to prevent the capture of communications in which all the parties are within the U.S.
- minimization procedures, which the court has approved or is being asked to approve and which satisfy the requirements for such procedures in the case of FISA electronic surveillance and physical searches, will be honored
- guidelines to ensure compliance with limitations imposed in the section have been adopted and the limitations will be observed
- these procedures and guidelines are consistent with Fourth Amendment standards.[2613]

The certification is be accompanied by a copy of the targeting and minimization procedures, any supporting affidavits from senior national security officials, an indication of the effective date of the authorization, and a notification of whether pre-approval emergency authorization has been given.[2614] The certification, however, need not describe the facilities or places at which acquisition efforts will be directed.[2615]

The limitations preclude intentionally targeting a person in the U.S., "reverse targeting" (intentionally targeting a person overseas purpose of targeting a person within the U.S.), intentionally targeting a U.S. person outside the U.S., intentionally acquiring a communication in which all of the parties are in the U.S., or conducting the acquisition in a manner contrary to the demands of the Fourth Amendment.[2616]

The Attorney General, in consultation with the Director of National Intelligence, is obligated to promulgate targeting and minimization procedures and guidelines to ensure that the section's limitations are observed.[2617] The minimization procedures must satisfy the standards required for similar procedures required

---

[2613] 50 U.S.C. 1881a(g)(2).

[2614] Id.

[2615] 50 U.S.C. 1881a(g)(4).

[2616] 50 U.S.C. 1881a(b).

[2617] 50 U.S.C. 1881a(d), (e), (f).

for FISA electronic surveillance and physical searches.[2618] The targeting procedures must be calculated to avoid acquiring communications in which all of the parties are in the U.S. and to confine targeting to persons located outside the U.S.[2619] Both are subject to review by the FISA court for sufficiency when it receives the request to approve the certification.[2620] Copies of the guidelines, which also provide directions concerning the application for FISA court approval under the section, must be supplied to court and to the congressional intelligence and judiciary committees.[2621]

The Attorney General and Director of National Intelligence may instruct an electronic communications service provider to assist in the acquisition. Cooperative providers are entitled to compensation and are immune from suit for their assistance.[2622] They may also petition the FISA court to set aside or modify the direction for assistance, if it is unlawful.[2623] The Attorney General may petition the court to enforce a directive against an uncooperative provider.[2624] The court's decisions concerning certification approval, modification of directions for assistance, and enforcement of the directives are each appealable to the Foreign Intelligence Court of Review and on certiorari to the Supreme Court.[2625]

Except with respect to disclosure following a failure to secure court approval of an emergency authorization, section 1806, discussed earlier, governs the use of information obtained under the authority of section 1881a.[2626]

When the overseas target is an American individual or entity and acquisition is to occur in this country, the FISA court may authorize acquisition by electronic surveillance or by capturing stored electronic communications or data under section 1881b. The Attorney General must approve the application which must be made under oath and indicate:

[2618] 50 U.S.C. 1881a(e).

[2619] 50 U.S.C. 1881a(d).

[2620] 50 U.S.C. 1881a(d), (e), (i).

[2621] 50 U.S.C. 1881a(f).

[2622] 50 U.S.C. 1881(h)(1)-(3).

[2623] 50 U.S.C. 1881(h)(4).

[2624] 50 U.S.C. 1881(h)(5).

[2625] 50 U.S.C. 1881a(h)(6), (i).

[2626] 50 U.S.C. 1881e(a).

- the identity of the applicant
- the identity, if known, or description of the American target
- the facts establishing that reason to believe that the person is overseas and a foreign power or its agent, officer, or employee
- the applicable minimization procedures
- a description of the information sought and the type of communications or activities targeted
- certification by the Attorney General or a senior national security or defense official that
    - foreign intelligence information is to be sought
    - a significant purpose of the effort is to obtain such information
    - the information cannot otherwise reasonably be obtained (and the facts upon which this conclusion is based)
    - the nature of the information (e.g., relating to terrorism, sabotage, the conduct of U.S. foreign affairs, etc.)(and the facts upon which this conclusion is based)
- the means of acquisition and whether physical entry will be necessary
- the identity of the service providing assisting (targeted facilities and premises need not be identified)
- a statement of previous applications relating to the same American and actions taken
- the proposed tenure of the order (not to exceed 90 days), and
- any additional information the FISA court may require.[2627]

The court must issue an acquisition order upon a finding that the application satisfies statutory requirements, the minimization procedures are adequate, and there is probable cause to believe that the American target is located overseas and is a foreign power or its agent, officer or employee.[2628] The court must explain in writing any finding that the application's assertion of probable cause, minimization procedures, or certified facts is insufficient.[2629] Such findings are appealable to the Foreign Intelligence Surveillance Court of Review and under certiorari to the Supreme Court.[2630]

The court's order approving acquisition is to include the identity or description of the American target, the type of activities targeted, the nature of the information

---

[2627] 50 U.S.C. 1881b(b).

[2628] 50 U.S.C. 1881b(c)(1). An American may not be considered a foreign power or its agent, officer or employee based solely on activities protected by the First Amendment, 50 U.S.C. 1881b(c)(2).

[2629] 50 U.S.C. 1881b(c)(3).

[2630] 50 U.S.C. 1881b(f).

sought, the means of acquisition, and duration of the order.[2631] The order will also call for compliance with the minimization procedures, and when appropriate, for confidential, minimally disruptive provider assistance, compensated at a prevailing rate.[2632] Providers are immune from civil liability for any assistance they are directed to provide.[2633]

As in other instances, in emergency cases the Attorney General may authorize acquisition pending approval of the FISA court.[2634] The court must be notified of the Attorney General's decision and the related application must be filed within 7 days.[2635] If emergency acquisition is not judicially approved subsequently, no resulting evidence may be introduced in any judicial, legislative or regulatory proceedings unless the target is determined not to be an American, nor may resulting information be shared with other federal officials without the consent of the target, unless the Attorney General determines that the information concerns a threat of serious bodily injury.[2636] Except with respect to disclosure following a failure to court approval of an emergency authorization, section 1806, discussed earlier, governs the use of information obtained under the authority of section 1881a.[2637]

The second provision for targeting an American overseas in order to acquire foreign intelligence information, section 1881c, is somewhat unique. Both FISA and Title III/ECPA have been understood to apply only to interceptions within the United States. Neither has been thought to apply overseas. Section 1881c, however, may be used for acquisitions outside the United States. Moreover, it may be used for acquisitions inside the United States as long as the requirements that would ordinarily attend such acquisition are honored.[2638] Otherwise, section

---

[2631] 50 U.S.C. 1881b(c)(4).

[2632] 50 U.S.C. 1881b(c)(5).

[2633] 50 U.S.C. 1881b(e).

[2634] 50 U.S.C. 1881b(d)(1).

[2635] Id.

[2636] 50 U.S.C. 1881b(d)(4).

[2637] 50 U.S.C. 1881e(a).

[2638] 50 U.S.C. 1881c(a)(3)(B)("If an acquisition for foreign intelligence purposes is to be conducted inside the United States and could be authorized under section 703 [1881b], the acquisition may only be conducted if authorized under section 703 or in accordance with another provision of this Act other than this section"). 50 U.S.C. 1881d("(a) Joint applications and orders.– If an acquisition targeting a United States person under section 703 or 704 is proposed to be conducted both inside and outside the United States, a judge having jurisdiction under section 703(a)(1) or 704(a)(1) may issue simultaneously, upon the request of the Government in a

1881c features many of the same application, approval, and appeal provisions as section 1881b.

Otherwise, section 1881c features many of the same application, approval, and appeal provisions as section 1881b. Authorization is available under a FISA court order or in emergency circumstances under the order of the Attorney General.[2639] Acquisition activities must be discontinued during any period when the target is thought to be in the United States.[2640] Unlike 1881b, however, it is not limited to electronic surveillance or the acquisition of stored electronic information. Moreover, it declares that in the case of acquisition abroad recourse to a FISA court order need only be had when the target American, found overseas, has a reasonable expectation of privacy and a warrant would be required if the acquisition efforts had taken place in the United States and for law enforcement purposes.[2641]

Exclusivity

Title III/ECPA has long declared that it should not be construed to confine governmental activities authorized under FISA, but that the two – Title III/ECPA and FISA – are the exclusive authority under which governmental electronic surveillance may be conducted in this country.[2642] The Justice Department suggested, however, that in addition to the President's constitutional authority the Authorization for the Use of Military Force Resolution,[2643] enacted in response to the events of September 11, established an implicit exception to the

---

joint application complying with the requirements of sections 703(b) and 704(b), orders under sections 703(c) and 704(c), as appropriate. (b) Concurrent authorization– If an order authorizing electronic surveillance or physical search has been obtained under section 105 or 304, the Attorney General may authorize, for the effective period of that order, without an order under section 703 or 704, the targeting of that United States person for the purpose of acquiring foreign intelligence information while such person is reasonably believed to be located outside the United States").

[2639] 50 U.S.C. 1881c(a).

[2640] 50 U.S.C. 1881c(a)(3).

[2641] 50 U.S.C. 1881c(a)(2).

[2642] 18 U.S.C. 2511(2)(f).

[2643] Section 2(a), P.L. 107-40, 115 Stat. 224 (2001), 50 U.S.C. 1541 note ("That the President is authorized to use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks that occurred on September 11, 2001, or harbored such organizations or persons, in order to prevent any future acts of international terrorism against the United States by such nations, organizations or persons").

exclusivity requirement.[2644] Section 102 of P.L. 110-261 seeks to overcome the suggestion by establishing a second exclusivity section which declares that exceptions may only be created by explicit statutory language.[2645]

Inspector General Reviews

Section 301 of P.L. 110-261 instructs the Inspectors General of the Justice and Defense Departments, of the Office of the Director of National Intelligence, of the National Security Agency, and of any pertinent intelligence agency to conduct a comprehensive review of their agency's activities relating to presidentially authorized intelligence activities involving communications, including the Terrorist Surveillance Program.[2646] It further directs them to provide the Judiciary and Intelligence Committees with interim reports within 60 days of enactment and final reports within 1 year.[2647]

Immunity for Assistance

P.L. 110-261 bars the initiation or continuation of civil suits in either state or federal court based on charges that the defendant assisted any of the U.S. intelligence agencies.[2648] Dismissal is required upon the certification of the Attorney General that the person either:

- did not provide the assistance charged;
- provided the assistance under order of the FISA court;
- provided the assistance pursuant to a national security letter issued under 18 U.S.C. 2709;
- provided the assistance pursuant to 18 U.S.C. 2511(2)(a)(ii)(B) and 2518(7) under assurances from the Attorney General or a senior Justice

---

[2644] H.Rept. 110-373, at 9-10 (2007), citing a letter from Assistant Attorney General William E. Moschella.

[2645] 50 U.S.C. 1812 ("(a) Except as provided in subsection (b), the procedures of chapters 119, 121, and 206 of title 18, United States Code, and this Act shall be the exclusive means by which electronic surveillance and the interception of domestic wire, oral, or electronic communications may be conducted. (b) Only an express statutory authorization for electronic surveillance or the interception of domestic wire, oral, or electronic communications, other than as an amendment to this Act or chapters 119, 121, or 206 of title 18, United States Code, shall constitute an additional exclusive means for the purpose of subsection (a)").

[2646] P.L. 110-261, §301(b), (a)(3), 122 Stat. 2471(2008).

[2647] P.L. 110-261, §301(c), 122 Stat. 2471(2008).

[2648] 50 U.S.C. 1885a(a)("Notwithstanding any other provision of law, a civil action may not lie or be maintained in a Federal or State court against any person for providing assistance to an element of the intelligence community, and shall be promptly dismissed. . .").

Department official, empowered to approve emergency law enforcement wiretaps, that no court approval was required;
- provided the assistance in response to a directive from the President through the Attorney General relating to communications between or among foreign powers pursuant to 50 U.S.C. 1802(a)(4);
- provided the assistance in response to a directive from the Attorney General and the Director of National Intelligence relating to the acquisition of foreign intelligence information concerning persons believed to be overseas pursuant to 50 U.S.C. 1805b;
- provided the assistance in response to a directive from the Attorney General and the Director of National Intelligence relating to the acquisition of foreign intelligence information targeting non-U.S. persons thought to be overseas pursuant to 50 U.S.C. 1881a(h); or
- provided the assistance in connection with intelligence activities authorized by the President between September 11, 2001 and January 17, 2007 relating to terrorist attacks against the United States.[2649]

Only telecommunications carriers, electronic service providers, and other communication service providers may claim the protection afforded those who assisted activities authorized between 9/11 and January 17, 2007.[2650] The group which may claim protection for assistance supplied under other grounds is larger. It includes not only communication service providers but also any "landlord, custodian or other person" ordered or directed to provide assistance.[2651]

The Attorney General's certification is binding if supported by substantial evidence, and the court is to consider challenges and supporting evidence ex parte and in camera where the Attorney General asserts that disclosure would

---

[2649] 50 U.S.C. 1885a(a). On January 17, 2007, the Attorney General notified Congress that any subsequent electronic surveillance conducted as part of the Terrorist Surveillance Program would be conducted pursuant to FISA court approval, S.Rept. 110-209, at 4 (2007).

[2650] 50 U.S.C. 1885a(a)(4); 1885(6)("(A) a telecommunications carrier, as that term is defined in section 3 of the Communications Act of 1934 (47 U.S.C. 153); (B) a provider of electronic communication service, as that term is defined in section 2510 of title 18, United States Code; (C) a provider of a remote computing service, as that term is defined in section 2711 of title 18, United States Code; (D) any other communication service provider who has access to wire or electronic communications either as such communications are transmitted or as such communications are stored; (E) a parent, subsidiary, affiliate, successor, or assignee of an entity described in subparagraph (A), (B), (C), or (D); or (F) an officer, employee, or agent of an entity described in subparagraph (A), (B), (C), (D), or (E)").

[2651] 50 U.S.C. 1885a(a)(1)-(3), (5); 1885(7).

harm national security.[2652] Cases filed in state court may be removed to federal court.[2653]

The District Court, to which multi-district civil litigation over cases arising out of the National Security Agency program has been assigned, upheld the constitutionality of P.L. 110-261's immunity provision against attacks under the due process clause, the First Amendment, and separation of powers.[2654]

P.L. 11-261 also preempts state regulatory authority over communication service providers with respect to assistance provided to intelligence agencies.[2655] Moreover, it directs the Attorney General to report to the Judiciary and Intelligence Committees on implementation of the protective provisions.[2656]

Selected Bibliography

Books and Articles

Addicott & McCaul, The Protect America Act of 2007: A Framework for Improving Intelligence Collection in the War on Terror, 13 TEXAS REVIEW OF LAW & POLITICS 43 (2008)

Avery, The Constitutionality of Warrantless Electronic Surveillance of Suspected Foreign Threats to the National Security of the United States, 62 UNIVERSITY OF MIAMI LAW REVIEW 541 (2008)

Banks, The Death of FISA, 91 MINNESOTA LAW REVIEW 1209 (2007)

Bellia, & Freiwald, Fourth Amendment Protection for Stored E-mail, 2008 UNIVERSITY OF CHICAGO LEGAL FORUM 121

Brownell, The Public Security and Wire Tapping, 39 CORNELL LAW QUARTERLY 154 (1954)

[2652] 50 U.S.C. 1885a(b), (c).

[2653] 50 U.S.C. 1885a(g).

[2654] In re National Security Agency Telecommunications Records Litigation, 633 F.Supp.2d 949, 960-74 (N.D.Cal. 2009). The court also rejected a challenge under the Administrative Procedure Act, id. at 974-76.

[2655] 50 U.S.C. 1885b. The court found no Tenth Amendment violation in P.L. 110-261's pre-emption provision, In re National Security Agency Telecommunications Records Litigation, 630 F.Supp.2d 1092, 1100-103 (N.D.Cal. 2009).

[2656] 50 U.S.C. 1885c.

Burstein, Amending the ECPA to Enable a Culture of Cuybersecurity Research, 22 HARVARD JOURNAL OF LAW & TECHNOLOGY 167 (2008)

Caproni, Surveillance and Transparency, 11 LEWIS & CLARK LAW REVIEW 1087 (2007)

Carr & Bellia, THE LAW OF ELECTRONIC SURVEILLANCE (2001 & July, 2009 Supp.)

Casey, Electronic Surveillance and the Right to Be Secure, 41 UC DAVIS LAW REVIEW 977 (2008)

Chemerinsky, Losing Liberties: Applying a Foreign Intelligence Model to Domestic Law Enforcement, 51 UCLA LAW REVIEW 1619 (2004)

Cinquegrana, The Walls (and Wires) Have Ears: The Background and First Ten Years of the Foreign Intelligence Surveillance Act of 1978, 137 UNIVERSITY OF PENNSYLVANIA LAW REVIEW 793 (1989)

Dinger, Should Parents Be Allowed to Record a Child's Telephone Conversations When They Believe the Child Is in Danger?: A Examination of the Federal Wiretap Statute and the Doctrine of Vicarious Consent in the Context of a Criminal Prosecution, 28 SEATTLE UNIVERSITY LAW REVIEW 955 (2005)

Donnelly, Comments and Caveats on the Wiretapping Controversy, 63 YALE LAW JOURNAL 799 (1954)

Fishman & McKenna, WIRETAPPING AND EAVESDROPPING (3d ed.2007 & April, 2009 Supp.)

Freiwald, Online Surveillance: Remembering the Lessons of the Wiretap Act, 56 ALABAMA LAW REVIEW 9 (2004)

Froomkin, The Metaphor Is the Key: Cryptography, the Clipper Chip, and the Constitution, 143 UNIVERSITY OF PENNSYLVANIA LAW REVIEW 709 (1995)

Funk, Electronic Surveillance of Terrorism: The Intelligence/Law Enforcement Dilemma–A History, 11 LEWIS & CLARK LAW REVIEW 1099 (2007)

Garrie, Armstrong & Harris, Voice Over Internet Protocol and the Wiretap Act: Is Your Conversation Protected?, 29 SEATTLE UNIVERSITY LAW REVIEW 97 (2005)

Goldsmith & Balmforth, The Electronic Surveillance of Privileged Communications: A Conflict of Doctrines, 64 SOUTH CALIFORNIA LAW REVIEW 903 (1991)

Himma, Privacy Versus Security: Why Privacy Is Not an Absolute Value or Right, 44 SAN DIEGO LAW REVIEW 857 (2007)

Kastenmeier, Leavy & Beier, Communications Privacy: A Legislative Perspective, 1989 WISCONSIN LAW REVIEW 715

Katyal & Caplan, The Surprisingly Stronger Case for Legality of the NSA Surveillance Program: The FDR Precedent, 60 STANFORD LAW REVIEW 1023 (2008)

Lawson, What Lurks Beneath: NSA Surveillance and Executive Power, 88 BOSTON UNIVERSITY LAW REVIEW 375 (2008)

Maher, Tale of the Tape: Lawyers Recording Conversations, 15 PROFESSIONAL LAWYER 10 (2004)

Meason, The Foreign Intelligence Surveillance Act: Time for Reappraisal, 24 INTERNATIONAL LAWYER 1043 (1990)

National Commission for the Study of Federal and State Laws Relating to Wiretapping and Electronic Surveillance, FINAL REPORT (1976)

Robotti, Grasping the Pendulum: Coordination Between Law Enforcement and Intelligence Officers Within the Department of Justice in a Post-"Wall" Era, 64 NEW YORK UNIVERSITY ANNUAL SURVEY OF AMERICAN LAW 751 (2009)

Schwartz, Warrantless Wiretapping, FISA Reform, and the Lessons of Public Liberty: A Comment on Holmes's Jorde Lecture, 97 CALIFORNIA LAW REVIEW 407 (2009)

Seamon & Gardner, The Patriot Act and the Wall Between Foreign Intelligence and Law Enforcement, 28 HARVARD JOURNAL OF LAW & PUBLIC POLICY 319 (2005)

Simons, From Katz to Kyllo: A Blueprint for Adapting the Fourth Amendment to Twenty-First Century Technologies, 53 HASTINGS LAW JOURNAL 1303 (2002)

Spritzer, Electronic Surveillance by Leave of the Magistrate: The Case in Opposition, 118 UNIVERSITY OF PENNSYLVANIA LAW REVIEW 169 (1969)

Symposium, Surveillance, 75 UNIVERSITY OF CHICAGO LAW REVIEW 47 (2008)

- Kerr, Updating the Foreign Intelligence Surveillance Act, 75 UNIVERSITY OF CHICAGO LAW REVIEW 225 (2008)
- Posner, Privacy, Surveillance, and Law, 75 UNIVERSITY OF CHICAGO LAW REVIEW 245(2008)

- Schwartz, Reviving Telecommunications Surveillance Law, 75 UNIVERSITY OF CHICAGO LAW REVIEW 287 (2008)

Symposium, The Future of Internet Surveillance Law: A Symposium to Discuss Internet Surveillance, Privacy & the USA PATRIOT Act, 72 GEORGE WASHINGTON LAW REVIEW 1139 (2004)

- Kerr, Foreword: The Future of Internet Surveillance Law, 72 GEORGE WASHINGTON LAW REVIEW 1139 (2004)
- Howell, Seven Weeks: The Making of the USA PATRIOT Act, 72 GEORGE WASHINGTON LAW REVIEW 1145 (2004)
- Kerr, A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It, 72 GEORGE WASHINGTON LAW REVIEW 1208 (2004)
- Schwartz, Evaluating Telecommunications Surveillance in Germany: The Lessons of the Max Plank Institute's Study, 72 GEORGE WASHINGTON LAW REVIEW 1244 (2004)
- Solove, Reconstructing Electronic Surveillance Law, 72 GEORGE WASHINGTON LAW REVIEW 1264 (2004)
- Swire, The System of Foreign Intelligence Surveillance Law, 72 GEORGE WASHINGTON LAW REVIEW 1306 (2004)
- Bellia, Surveillance Law Through Cyberlaw's Lens, 72 GEORGE WASHINGTON LAW REVIEW 1375 (2004)
- Dempsey & Flint, Commercial Data and National Security, 72 GEORGE WASHINGTON LAW REVIEW 1459 (2004)
- Fishman, Technology and the Internet: The Impending Destruction of Privacy by Betrayers, Grudgers, Snoops, Spammers, Corporations, and the Media, 72 GEORGE WASHINGTON LAW REVIEW 1503 (2004)
- Mulligan, Reasonable Expectations in Electronic Communications; A Critical Perspective on the Electronic Communications Privacy Act, 72 GEORGE WASHINGTON LAW REVIEW 1557 (2004)
- Ohm, Parallel-Effect Statutes and E-Mail "Warrants": Reframing the Internet Surveillance Debate, 72 GEORGE WASHINGTON LAW REVIEW 1559 (2004)

Symposium, Spyware: The Latest Cyber-Regulatory Challenge, 20 BERKELEY TECHNOLOGY LAW JOURNAL 1269 (2005)

- Schwartz, Privacy Inalienability and the Regulation of Spyware, 20 BERKELEY TECHNOLOGY LAW JOURNAL 1269 (2005)
- Bellia, Spyware and the Limits of Surveillance Law, 20 BERKELEY TECHNOLOGY LAW JOURNAL 1283 (2005)
- Winn, Contracting Spyware by Contract, 20 BERKELEY TECHNOLOGY LAW JOURNAL 1345 (2005)
- Crawford, First Do No Harm: The Problem of Spyware, 20 BERKELEY TECHNOLOGY LAW JOURNAL 1433 (2005)

Tokson, The Content/Envelope Distinction in Internet Law, 50 WILLIAM & MARY LAW REVIEW 2105 (2009)

Turkington, Protections for Invasions of Conversational and Communications Privacy by Electronic Surveillance in Family, Marriage, and Domestic Disputes Under Federal and State Wiretap and Store Communications Acts and the Common Law Privacy Intrusion Tort, 82 NEBRASKA LAW REVIEW 693 (2004)

Whitehead & Aden, Forfeiting "Enduring Freedom" for "Homeland Security": A Constitutional Analysis of the USA PATRIOT Act and the Justice Department's Anti-Terrorism Initiatives, 51 AMERICAN UNIVERSITY LAW REVIEW 1081 (2002)

Notes and Comments

Attorney Private Eyes: Ethical Implications of a Private Attorney's Decision to Surreptitiously Record Conversations, 2003 UNIVERSITY OF ILLINOIS LAW REVIEW 1605 (2003)

The Case for Magic Lantern: September 11 Highlights the Need for Increased Surveillance, 15 HARVARD JOURNAL OF LAW & TECHNOLOGY 521 (2002)

Crying Wolf in the Digital Age: Voluntary Disclosure Under the Stored Communications Act, 39 COLUMBIA HUMAN RIGHTS LAW REVIEW 529 (2008)

Dirty Digit: The Collection of Post-Cut-Through Dialed Digits Under the Pen/Trap Statute, 74 BROOKLYN LAW REVIEW 1109 (2009)

Electronic Surveillance in the Internet Age: The Strange Case of Pen Registers, 41 AMERICAN CRIMINAL LAW REVIEW 1321 (2004)

Hijacking Civil Liberties: The USA PATRIOT Act of 2001, 33 LOYOLA UNIVERSITY OF CHICAGO LAW JOURNAL 933 (2002)

The Protect America Act: One Nation Under <<Strike Through>>God<<End Strike Through>> Surveillance, 29 LOYOLA OF LOS ANGELES ENTERTAINMENT LAW REVIEW (2008)

Qualified Immunity as a Defense to Federal Wiretap Act Claims, 68 UNIVERSITY OF CHICAGO LAW REVIEW 1369 (2001)

The Revamped FISA: Striking a Better Balance Between the Government's Need to Protect Itself and the 4th Amendment, 58 VANDERBILT LAW REVIEW 1671 (2005)

"The Right of the People": The NSA, the FISA Amendments Act of 2008, and Foreign Intelligence Surveillance of Americans Overseas, 78 FORDHAM LAW REVIEW 217 (2009)

Thirty-Eighth Annual Review of Criminal Procedure: Electronic Surveillance, 38 GEORGETOWN LAW JOURNAL ANNUAL REVIEW OF CRIMINAL PROCEDURE 142 (2009)

Warrantless Location Tracking 83 NEW YORK UNIVERSITY LAW REVIEW 1324 (2008)

ALR Notes

Applicability, in Civil Action, of Provisions of Omnibus Crime Control and Safe Streets Act of 1968, Prohibiting Interception of Communications (18 USCS §2511(1)), to Interceptions by Spouse, or Spouse's Agent, of Conversations of Other Spouse, 139 ALR FED. 517

Application of Extension Telephones of Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (18 USCS §§2510 et seq.) Pertaining to Interceptions of Wire Communications, 58 ALR FED. 594

Constitutionality of Secret Video Surveillance, 91 ALR 5th 585

Construction and Application of 18 USCS 2511(1)(a) and (b), Providing Criminal Penalty for Intercepting, Endeavoring to intercept, or Procuring Another to Intercept Wire, Oral or Electronic Communication, 122 ALR FED. 597

Construction and Application of Provision of Omnibus Crime and Safe Streets Act of 1968 (18 U.S.C.A. §2520) Authorizing Civil Cause of Action by Person Whose Wire, Oral, or Electronic Communication Is Intercepted, Disclosed, or Used in Violation of the Act, 164 ALR FED. 139 Construction and Application of State Statutes Authorizing Civil Cause of Action by Person Whose Wire or Oral Communications Is Intercepted, Disclosed, or Used in Violation of Statutes, 33 ALR 4TH 506

Eavesdropping and Wiretapping, What Constitutes "Device Which Is Primarily Useful for the Surreptitious Interception of Wire, Oral, or Electronic Communication," Under 18 USCS 2512(1)(b), Prohibiting Manufacture, Possession, Assembly, Sale of Such Device, 129 ALR FED.

Eavesdropping on Extension Telephone as Invasion of Privacy, 49 ALR 4TH 430

Interception of Telecommunications by or With Consent of Party as Exception Under 18 USCS §2511(2)(c) and (d), to Federal Proscription of Such Interceptions, 67 ALR FED. 429

Permissible Surveillance, Under State Communications Interception Statute, by Person Other than State or Local Law Enforcement Officer or One Acting in Concert with Officer, 24 ALR 4TH

Permissible Warrantless Surveillance, Under State Communications Interception Statute, by State or Local Law Enforcement Officer or One Acting in Concert with Officer, 27 ALR 4TH 449

Propriety of Attorney's Surreptitious Sound Recording of Statements by Others Who Are or May Become Involved in Litigation 32 ALR 5TH 715

Propriety of Monitoring of Telephone Calls to or From Prison Inmates Under Title III of Omnibus Crime Control and Safe Streets Act (18 USCS §§2510 et seq.) Prohibiting Judicially Unauthorized Interception of Wire or Oral Communications, 61 ALR FED. 825

Propriety of Governmental Eavesdropping on Communications Between Accused and His Attorney, 189 ALD FED. 419

Propriety, Under 18 USCS 2517(5), of Interception or Use of Communications Relating to Federal Offenses Which Were Not Specified in Original wiretap Order, 103 ALR FED. 422

Qualified Immunity as Defense in Suit Under Federal Wiretap Act (18 U.S.C.A. §§2510 et seq.), 178 ALR FED 1

State Regulation of Radio Paging Services, 44 ALR 4TH 216

Validity, Construction, and Application of Foreign Intelligence Surveillance Act of 1978 (50 USCS §§1801 et seq.) Authorizing Electronic Surveillance of Foreign Powers and Their Agents, 86 ALR FED. 782

What Constitutes Adequate Response by the Government, Pursuant to 18 U.S.C. 3504, Affirming or Denying Use of Unlawful Electronic Surveillance, 53 ALR Fed. 378

What Constitutes Compliance by Government Agents With Requirement of 18 U.S.C. 2518(5) that Wire Tapping and Electronic Surveillance Be Conduct in Such Manner as to Minimize Interception of Communications Not Otherwise Subject to Interception, 181 ALR Fed. 419

Who May Apply or Authorize Application for Order to Intercept Wire or Oral Communications Under Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (18 U.S.C. 2510 et seq.), 169 ALR Fed. 169

Appendix A: State Statutes Outlawing the Interception of Wire(w), Oral(o) and Electronic Communications(e)

Alabama

Ala.Code §§13A-11-30 to 13A-11-37(w/o)

Alaska

Alaska Stat. §§42.20.300 to 42.20.390 (w/o/e)

Arizona

Ariz.Rev.Stat.Ann. §§13-3001 to 13-3009 (w/o/e)

Arkansas

Ark.Code §§5-60-120, 23-17-107(w/o/e)

California

Cal.Penal Code §§631(w), 632(o), 632.7(e)

Colorado

Colo.Rev.Stat. §§18-9-301 to 18-9305(w/o/e)

Connecticut

Conn.Gen.Stat.Ann. §§53a-187 to 53a189, 54-41t (w/o)

Delaware

Del.Code tit.11 §§ 2401, 2402(w/o/e)

Florida

Fla.Stat.Ann. §§ 934.02, 934.03(w/o/e)

Georgia

Ga.Code §16-11-62 (w/o/e)

Hawaii

Hawaii Rev.Stat. §§ 711-1111, 803-41, 80342(w/o/e)

Idaho

Idaho Code §§ 18-6701, 18-6702(w/o/e)

Indiana

Ind.Code Ann. §§ 35-33.5-1-5, 35-33.5-55(w/e)

Iowa

Iowa Code Ann. §§272.8, 808B.2(w/o/e)

Kansas

Kan.Stat.Ann. §21-4001(w/o); 21-4002(w)

Kentucky

Ky.Rev.Stat. §§526.010, 526.020(w/o)

Louisiana

La.Rev.Stat.Ann. §§ 15:1302, 15:1303 (w/o/e)

Maine

Me.Rev.Stat.Ann. tit. 15 §§ 709, 710(w/o)

Maryland

Md.Cts. & Jud.Pro.Code Ann. §§ 10-401, 10-402(w/o/e)

Massachusetts

Mass.Gen.Laws Ann. ch.272 §99 (w/o)

Michigan

Mich.Comp.Laws Ann. §§750.539a, 750.539c(o); 750.540(w)

Minnesota

Minn.Stat.Ann. §§ 626A.01, 626A.02 (w/o/e)

Mississippi

Miss.Code §41-29-533(w/o/e)

Missouri

Mo.Ann.Stat. §§ 542.400 to 542.402 (w/o)

Montana

Mont.Code Ann. §45-8-213(w/o/e)

Nebraska

Neb.Rev.Stat. §§ 86-271 to 86-290 (w/o/e)

Nevada

Nev.Rev.Stat. §§ 200.610, 200.620(w), 200.650(o)

New Hampshire

N.H.Rev.Stat.Ann. §§ 570-A:1, 570A:2 (w/o)

New Jersey

N.J.Stat.Ann. §§ 2A:156A-2, 2A:156A3(w/o/e)

New Mexico

N.M.Stat.Ann. §30-12-1(w)

New York

N.Y.Penal Law §§ 250.00, 250.05(w/o/e)

North Carolina

N.C.Gen.Stat. §§ 15A-286, 15A287(w/o/e)

New Hampshire

N.H.Rev.Stat.Ann. §§ 570-A:1, 570-A:2 (w/o)

New Jersey

N.J.Stat.Ann. §§ 2A:156A-2, 2A:156A3(w/o/e)

New Mexico

N.M.Stat.Ann. §30-12-1(w)

New York

N.Y.Penal Law §§ 250.00, 250.05(w/o/e)

North Carolina

N.C.Gen.Stat. §§ 15A-286, 15A287(w/o/e)

North Dakota

N.D.Cent.Code §§12.1-15-02, 12.1-15-04 (w/o)

Ohio

Ohio Rev.Code §§ 2933.51, 2933.52 (w/o/e)

Oklahoma

Okla.Stat.Ann. tit.13 §§ 176.2, 176.3 (w/o/e)

Oregon

Ore.Rev.Stat. §§165.535 to 165.545 (w/o/e)

Pennsylvania

Pa.Stat.Ann. tit.18 §§ 5702, 5703 (w/o/e)

Rhode Island

R.I.Gen.Laws §§11-35-21(w/o/e)

South Carolina

S.C. Code Ann. §§16-17-470, 17-30-10 to 17-30-20 (w/o/e)

South Dakota

S.D.Cod.Laws §§ 23A-35A-1, 23A-35A-20 (w/o)

Tennessee

Tenn.Code Ann. §39-13-601(w/o/e)

Texas

Tex.Penal Code. § 16.02;
Tex. Crim. Pro. Code art. 18.20 (w/o/e)

Utah

Utah Code Ann. §§ 76-9-405, 77-23a-3, 77-23a-4 (w/o/e)

Virginia

Va.Code §§ 19.2-61, 19.2-62(w/o/e)

Washington

Wash.Rev.Code Ann.§9.73.030 (w/o)

West Virginia

W.Va.Code §§ 62-1D-2, 62-1D-3(w/o/e)

Wisconsin

Wis.Stat.Ann. §§ 968.27, 968.31(w/o/e)

Wyoming

Wyo.Stat. §§ 7-3-701, 7-3-702(w/o/e)

District of Columbia

D.C.Code §§ 23-541, 23-542(w/o).

Alabama: Ala.Code §13A-11-30 (one party consent)

Alaska: Alaska Stat. §§42.20.310, 42.20.330 (one party consent)

Arizona: Ariz.Rev.Stat.Ann. §13-3005 (one party consent)

Arkansas: Ark.Code §5-60-120 (one party consent)

California: Cal. Penal Code §§ 631, 632 (one party consent for police; all party consent otherwise), 632.7 (all party consent)

Colorado: Colo.Rev.Stat. §§18-9-303, 18-9-304 (one party consent)

Connecticut: Conn.Gen.Stat.Ann. §§53a-187, 53a-188 (criminal proscription: one party consent); §52-570d (civil liability: all party consent except for police)

Delaware: Del.Code tit.11 §2402 (one party consent)

Florida: Fla.Stat.Ann. §934.03 (one party consent for the police; all party consent for others)

Georgia: Ga.Code §16-11-66 (one party consent)

Hawaii: Hawaii Rev.Stat. §§ 711-1111, 803-42 (one party consent)

Idaho: Idaho Code §18-6702 (one party consent)

Illinois: Ill.Comp.Stat.Ann. ch.720 §§5/14-2, 5/14-3 (all party consent with law enforcement exceptions)

Indiana: Ind.Code Ann. §35-33.5-1-5 (one party consent)

Iowa: Iowa Code Ann. §808B.2 (one party consent)

Kansas: Kan.Stat.Ann. §§21-4001, 21-4002 (one party consent)

Kentucky: Ky.Rev.Stat. §526.010 (one party consent)

Louisiana: La.Rev.Stat.Ann. §15:1303 (one party consent)

Maine: Me.Rev.Stat.Ann. tit. 15 §709 (one party consent)

Maryland: Md.Cts. & Jud.Pro.Code Ann. §10-402 (all party consent)

Massachusetts: Mass.Gen.Laws Ann. ch.272 §99 (all parties must consent, except in some law enforcement cases)

Michigan: Mich.Comp.Laws Ann. §750.539c (proscription regarding eavesdropping on oral conversation: all party consent, except that the proscription does not apply to otherwise lawful activities of police officers)

Minnesota: Minn.Stat.Ann. §626A.02 (one party consent)

Mississippi: Miss.Code §41-29-531 (one party consent)

Missouri: Mo.Ann.Stat. §542.402 (one party consent)

Montana: Mont.Code Ann. §§45-8-213 (all party consent with an exception for the performance of official duties)

Nebraska: Neb.Rev.Stat. § 86-290 (one party consent)

Nevada: Nev.Rev.Stat. §§200.620, 200.650 (one party consent)

New Hampshire: N.H.Rev.Stat.Ann. §570-A:2 (all party consent)

New Jersey: N.J.Stat.Ann. §§2A:156A-4 (one party consent)

New Mexico: N.M.Stat.Ann. §§30-12-1 (one party consent)

New York: N.Y.Penal Law §250.00 (one party consent)

North Carolina: N.C.Gen.Stat. §15A-287 (one party consent)

North Dakota: N.D.Cent.Code §§12.1-15-02 (one party consent)

Ohio: Ohio Rev.Code §2933.52 (one party consent)

Oklahoma: Okla.Stat.Ann. tit.13 §176.4 (one party consent)

Oregon: Ore.Rev.Stat. §165.540 (one party consent for wiretapping and all parties must consent for other forms of electronic eavesdropping)

Pennsylvania: Pa.Stat.Ann. tit.18 §5704 (one party consent for the police; all parties consent otherwise)

Rhode Island: R.I.Gen.Laws §§11-35-21 (one party consent)

South Carolina: S.C. Code Ann. § 17-30-30 (one party consent)

South Dakota: S.D.Comp.Laws §§23A-35A-20 (one party consent)

Tennessee: Tenn.Code Ann. §39-13-601 (one party consent)

Texas: Tex.Penal Code §16.02 (one party consent)

Utah: Utah Code Ann. §§77-23a-4 (one party consent)

Virginia: Va.Code §19.2-62 (one party consent)

Washington: Wash.Rev.Code Ann. §9.73.030 (all parties must consent, except that one party consent is sufficient in certain law enforcement cases)

West Virginia: W.Va.Code §62-1D-3 (one party consent)

Wisconsin: Wis.Stat.Ann. §968.31 (one party consent)

Wyoming: Wyo.Stat. §7-3-702 (one party consent)

District of Columbia: D.C.Code §23-542 (one party consent).

Appendix C: Statutory Civil Liability for Interceptions Under State Law

Arizona

Ariz.Rev.Stat.Ann. §12-731

California

Cal. Penal Code §§ 637.2

Colorado

Colo.Rev.Stat. §18-9-309.5

Connecticut

Conn.Gen.Stat.Ann. §§54-41r, 52-570d

Delaware

Del.Code tit.11 §2409

Florida

Fla.Stat.Ann. §§934.10, 934.27

Hawaii

Hawaii Rev.Stat. §803-48

Idaho

Idaho Code §18-6709

Illinois

Ill.Comp.Stat.Ann. ch.720 §5/14-6

Indiana

Ind.Code Ann. §35-33.5-5-4

Iowa

Iowa Code Ann. §808B.8

Kansas

Kan.Stat.Ann. §22-2518

Louisiana

La.Rev.Stat.Ann. §15:1312

Maine

Me.Rev.Stat.Ann. ch.15 §711

Maryland

Md.Cts. & Jud.Pro.Code Ann. §§10-410, 10-4A-08

Massachusetts

Mass.Gen.Laws Ann. ch.272 §99

Michigan

Mich.Comp.Laws Ann. §750.539h

Mississippi

Miss. Code § 41-29-529

Minnesota

Minn.Stat.Ann. §§626A.02, 626A.13

Nebraska

Neb.Rev.Stat. § 86-297

Nevada

Nev.Rev.Stat. §200.690

New Hampshire

N.H.Rev.Stat.Ann. §570-A:11

New Jersey

N.J.Stat.Ann. §§2A:156A-24

New Mexico

N.M.Stat.Ann. §§30-12-11

North Carolina
N.C.Gen.Stat. §15A-296

Ohio
Ohio Rev.Code §2933.65

Oregon
Ore.Rev.Stat. §133.739

Pennsylvania
Pa.Stat.Ann. tit.18 §§5725, 5747

Rhode Island
R.I.Gen.Laws §12-5.1-13

South Carolina
S.C. Code Ann. § 17-30-135

Tennessee
Tenn.Code Ann. §39-13-603

Texas
Tex.Code Crim.Pro. art. 18.20

Utah
Utah Code Ann. §§77-23a-11; 77-23b-8

Virginia
Va.Code §19.2-69

Washington
Wash.Rev.Code Ann. §9.73.060

West Virginia

W.Va.Code §62-1D-12

Wisconsin

Wis.Stat.Ann. §968.31

Wyoming

Wyo.Stat. §7-3-710

District of Columbia

D.C.Code §23-554.

Appendix D: Court Authorized Interception Under State Law

Alaska

Alaska Stats. §§12.37.010 to 12.37.900

Arizona

Ariz.Rev.Stat.Ann. §§13-3010 to 13-3019

California

Cal.Penal Code §629.50 to 629.98

Colorado

Colo.Rev.Stat. §§16-15-101 to 16-15-104

Connecticut

Conn.Gen.Stat.Ann. §§54-41a to 54-41u

Delaware

Del.Code tit.11 §§2401 to 2412

Florida

Fla.Stat.Ann. §§934.02 to 934.43

Georgia

Ga.Code §16-11-64 to 16-11-69

Hawaii

Hawaii Rev.Stat. §§803-41 to 803-49

Idaho

Idaho Code §§18-6701 to 18-6709; 6719 to 6725

Illinois

Ill.Stat.Ann. ch.725 §§5/108A-1 to 108B-14

Indiana

Ind.Code §§35-33.5-1-1 to 35-33.5-5-6

Iowa

Iowa Code Ann. §§808B.3 to 808B.7

Kansas

Kan.Stat.Ann. §§ 22-2514 to 22-2519

Louisiana

La.Rev.Stat.Ann. §§15:1301 to 15:1316

Maryland

Md.Cts. & Jud.Pro.Code Ann. §§10-401 to 10410

Massachusetts

Mass.Gen.Laws Ann. ch.272 §99

Minnesota

Minn.Stat.Ann. §§626A.01 to 626.41

Mississippi

Miss.Code §§41-29-501 to 41-29-537

Missouri

Mo.Ann.Stat. §§542.400 to 542.422

Nebraska

Neb.Rev.Stat. §§ 86-271 to 86-2,115

Nevada

Nev.Rev.Stat. §§179.410 to 179.515

New Hampshire

N.H.Rev.Stat.Ann. §§570-A:1 to 570A:9

New Jersey

N.J.Stat.Ann. §§2A:156A-8 to 2A:156A-26

New Mexico

N.M.Stat.Ann. §§30-12-1 to 30-12-11

New York

N.Y.Crim.Pro. Law §§700.05 to 700.70

North Carolina

N.C.Gen.Stat. §§15A-286 to 15A-298

North Dakota

N.D.Cent.Code §§29-29.2-01 to 2929.2-05

Ohio

Ohio Rev.Code §§2933.51 to 2933.66

Oklahoma

Okla.Stat.Ann. tit.13 §§176.1 to 176.14

Oregon

Ore.Rev.Stat. §§133.721 to 133.739

Pennsylvania

Pa.Stat.Ann. tit.18 §§5701 to 5728

Rhode Island

R.I.Gen.Laws §§12-5.1-1 to 12-5.1-16

South Carolina

S.C. Code Ann. §§ 17-30-10 to 17-30145

South Dakota

S.D.Cod.Laws §§23A-35A-1 to 23A35A-34

Tennessee

Tenn.Code Ann. §§40-6-301 to 40-6-311

Texas

Tex.Crim.Pro. Code. art. 18.20

Utah

Utah Code Ann. §§77-23a-1 to 77-23a-16

Virginia

Va.Code §§19.2-61 to 19.2-70.3

Washington

Wash.Rev.Code Ann. §§9.73.040 to 9.73.250

West Virginia

W.Va.Code §§62-1D-1 to 62-1D-16

Wisconsin

Wis.Stat.Ann. §§968.27 to 968.33

Wyoming

Wyo.Stat. §§7-3-701 to 7-3-712

District of Columbia

D.C.Code §§23-541 to 23-556.

Appendix E: State Statutes Regulating Stored Electronic Communications (SE), Pen Registers (PR) and Trap and Trace Devices (T)

Alaska

Alaska Stats. §§12.37.200 (PR&T), 12.37.300(SE)

Arizona

Ariz.Rev.Stat.Ann. §§13-3016 (SE); 13-3005, 133017 (PR&T)

Arkansas

Ark. Code Ann. § 5-60-120(g) (PR&T)

Colorado

Colo. Rev. Stat. § 18-9-305 (PR&T)

Delaware

Del.Code tit.11 §§ 2401; 2421 to 2427 (SE); 2430 to 2434 (PR&T)

Florida

Fla.Stat.Ann. §§934.02; 934.21 to 934.28 (SE); 934.32 to 934.34(PR&T)

Georgia

Ga.Code Ann. §§16-11-60 to 16-11-64.2 (PR &T); § 16-9-109 (SE)

Hawaii

Hawaii Rev.Stat. §§803-41; 803-44.5, 803-44.6 (PR&T), 803-47.5 to 803.47.9 (SE)

Idaho

Idaho Code §§18-6719 to 18-6725 (PR&T)

Iowa

Iowa Code Ann. §§808B.1, 808B.10 to 808B.14 (PR&T)

Kansas

Kan.Stat.Ann. §§22-2525 to 22-2529 (PR&T)

Louisiana

La.Rev.Stat.Ann. §§15:1302, 15:1313 to 15:1316 (PR&T)

Maryland

Md.Cts. & Jud.Pro.Code Ann. §§10-4A-01 to 104A-08 (SE), 10-4B-01 to 10-4B-05 (PR&T)

Minnesota

Minn.Stat.Ann. §§626A.01; 626A.26 to 626A.34; (SE), 626A.35 to 636A.391 (PR&T)

Mississippi

Miss.Code §41-29-701(PR&T)

Missouri

Mo.Ann.Stat. §542.408 (PR)

Montana

Mont.Code Ann. §§46-4-401 to 46-4-405 (PR&T)

Nebraska

Neb.Rev.Stat. §§ 86-279, 86-2,104 to 86-2,110 (SE); 86-284, 86-287, 86-298 to 86-2,101 (PR&T)

Nevada

Nev.Rev.Stat. §§179.530 (PR&T), 205.492 to 205.513(SE)

New Hampshire

N.H.Rev.Stat.Ann. §§570-B:1 to 570-B:7 (PR&T)

New Jersey

N.J.Stat.Ann. §§2A:156A-27 to 2A:156A-34 (SE)

New York

N.Y.Crim.Pro.Law §§705.00 to 705.35 (PR&T)

North Carolina

N.C.Gen.Stat. §§15A-260 to 15A264 (PR&T)

North Dakota

N.D.Cent.Code §§29-29.3-01 to 29-29.3-05 (PR&T)

Ohio

Ohio Rev.Code §2933.76 (PR&T)

Oklahoma

Okla.Stat.Ann. tit.13 §177.1 to 177.5 (PR&T)

Oregon

Ore.Rev.Stat. §§165.657 to 165.673 (PR&T)

Pennsylvania

Pa.Stat.Ann. tit.18 §§5741 to 5749 (SE), 5771 to 5775 (PR&T)

Rhode Island

R.I.Gen.Laws §§12-5.2-1 to 12-5.2-5 (PR&T)

South Carolina

S.C.Code §§17-29-10 to 17-29-50, 17-30-45 to 17-30-50 (PR&T)

South Dakota

S.D.Cod.Laws §§23A-35A-22 to 23A-35A-34 (PR&T)

Tennessee

Tenn.Code Ann. §40-6-311 (PR&T)

Texas

Tex.Code Crim.Pro. art. 18.20, 18.21;
Tex. Penal Code §§ 16.03, 16.04 (SE, PR&T)

Utah

Utah Code Ann. §§77-23a-13 to 77-23a-15 (PR&T); 77-23b-1 to 77-23b-9(SE)

Virginia

Va.Code §§19.2-70.1, 19.2-70.2 (PR&T), 19.2-70.3 (SE)

Washington

Wash.Rev.Code Ann. §9.73.260 (PR&T)

West Virginia

W.Va.Code §§62-1D-2, 62-1D-10 (PR&T)

Wisconsin

Wis.Stat.Ann. §968.30 to 968.37 (PR&T)

Wyoming

Wyo.Stat. §§7-3-801 to 7-3-806 (PR&T).

Appendix F: State Computer Crime Statutes

Alabama

Ala.Code §§13A-8-100 to 13A-8-103

Alaska

Alaska Stat. §11.46.740

Arizona

Ariz.Rev.Stat.Ann. §§13-2316 to 132316.02

Arkansas

Ark.Code §§5-41-101 to 5-41-206

California

Cal.Penal Code §502

Colorado

Colo.Rev.Stat. §§18-5.5-101, 18-5.5102

Connecticut

Conn.Gen.Stat.Ann. §§53a-250 to 53a-261

Delaware

Del.Code tit.11 §§931 to 941

Florida

Fla.Stat.Ann. §§815.01 to 815.07

Georgia

Ga.Code §§16-9-92 to 16-9-94

Hawaii

Hawaii Rev.Stat. §708-890 to 708-895.7

Idaho

Idaho Code §§18-2201, 18-2202

Illinois

Ill.Stat.Ann. ch.720 §§5/16D-1 to 5/16D-7

Indiana

Ind.Code §§35-43-1-4 to 35-43-2-3

Iowa

Iowa Code Ann. §716.6B

Kansas

Kan.Stat.Ann. §21-3755

Kentucky

Ky.Rev.Stat. §§434.840 to 434.860

Louisiana

La.Rev.Stat.Ann. §§14:73.1 to 14:73.7

Maine

Me.Rev.Stat.Ann. tit. 17-A §§431 to 433

Maryland

Md.Code Ann., Crim. Law. §7-302

Massachusetts

Mass.Gen.Laws Ann. ch.266 §120F

Michigan

Mich.Comp.Laws Ann. §§752.791 to 752.797

Minnesota

Minn.Stat.Ann. §§609.87 to 609.893

Mississippi

Miss.Code §§97-45-1 to 97-45-29

Missouri

Mo.Ann.Stat. §§569.095 to 569.099

Montana

Mont.Code Ann. §§45-6-310, 45-6-311

Nebraska

Neb.Rev.Stat. §§28-1341 to 28-1348

Nevada

Nev.Rev.Stat. §§205.473 to 205.492; 205.509 to 205.513

New Hampshire

N.H.Rev.Stat.Ann. §638:16 to 638:19

New Jersey

N.J.Stat.Ann. §§2C:20-2, 2C:20-23 to 2C:20-34

New Mexico

N.M.Stat.Ann. §§30-45-1 to 30-45-7

New York

N.Y.Penal Law §§156.00 to 156.50

North Carolina

N.C.Gen.Stat. §§14-453 to 14-458

North Dakota

N.D.Cent.Code §12.1-06.1-08

Ohio

Ohio Rev.Code §§2909.01, 2909.07, 2913.01 to 2913.04, 2913.421

Oklahoma

Okla.Stat.Ann. tit.21 §§1951 to 1959

Oregon

Ore.Rev.Stat. §164.377

Pennsylvania

Pa.Stat.Ann. tit.18 §7611

Rhode Island

R.I.Gen.Laws §§11-52-1 to 11-52-8

South Carolina

S.C.Code §§16-16-10 to 16-16-40, 26-6-210

South Dakota

S.D.Cod.Laws §§43-43B-1 to 43-43B-8

Tennessee

Tenn.Code Ann. §§39-14-601 to 39-14-605

Texas

Tex.Penal Code. §§33.01 to 33.05

Utah

Utah Code Ann. §§76-6-702 to 76-6-705

Vermont

Vt. Stat. Ann. tit. 13, §§ 4101 to 4107

Virginia

Va.Code §§18.2-152.1 to 18.2-152.15, 19.2-249.2

Washington

Wash.Rev.Code Ann. §§9A.52.110 to 9A.52.130

West Virginia

W.Va.Code §§61-3C-1 to 61-3C-21

Wisconsin

Wis.Stat.Ann. §943.70

Wyoming

Wyo.Stat. §§6-3-501 to 6-3-505.

Appendix G: Spyware[2657]

Alaska

Alaska Stat. §§ 45.45.471 to 45.45.798

Arizona

Ariz. Rev. Stat. Ann. §§ 44-7301 to 44-7304

Arkansas

Ark. Code §§ 4-110-101 to 4-110-105

California

Cal. Bus. & Prof. Code §§ 22947 to 22947.6

Georgia

Ga. Code Ann. §§ 16-9-150 to 16-9-157

Indiana

Ind. Code Ann. §§ 24-4.8-1-1 to 24-4.8-3-2

Iowa

Iowa Code Ann. §§ 714F.1 to 714F.8

Louisiana

La. Rev. Stat. Ann. §§ 51:2006 to 51:2014

Nevada

Nev. Rev. Stat. Ann. §205.4737

New Hampshire

N.H. Rev. Stat. Ann. §§ 359-H:1 to 359-H:6

[2657] Depending upon the definition used, spyware has been outlawed under a host of federal and state laws; this appendix is limited to those state statutes that address "spyware" as such. For a general discussion of activities at the federal level see CRS Report RL32706, Spyware: Background and Policy Issues for Congress.

Texas

Tex. Bus. & Com. Code Ann. §§ 48.001 to 48.102

Utah

Utah Code Ann. §§ 13-40-101 to 13-40-401

Washington

Wash. Rev. Code Ann. §§19.270.010 to 19.270.900.

Electronic Communications Privacy Act (ECPA)

18 U.S.C. 2510. Definitions

As used in this chapter–

(1) "wire communication" means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce;

(2) "oral communication" means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication;

(3) "State" means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, and any territory or possession of the United States;

(4) "intercept" means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device;

(5) "electronic, mechanical, or other device" means any device or apparatus which can be used to intercept a wire, oral, or electronic communication other than–

(a) any telephone or telegraph instrument, equipment or facility, or any component thereof, (i) furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business; or

(ii) being used by a provider of wire or electronic communication service in the ordinary course of its business, or by an investigative or law enforcement officer in the ordinary course of his duties;

(b)a hearing aid or similar device being used to correct subnormal hearing to not better than normal;

(6) "person" means any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation;

(7) “Investigative or law enforcement officer” means any officer of the United States or of a State or political subdivision thereof, who is empowered by law to conduct investigations of or to make arrests for offenses enumerated in this chapter, and any attorney authorized by law to prosecute or participate in the prosecution of such offenses;

(8) “contents”, when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication;

(9) “Judge of competent jurisdiction” means–
(a) a judge of a United States district court or a United States court of appeals; and
(b) a judge of any court of general criminal jurisdiction of a State who is authorized by a statute of that State to enter orders authorizing interceptions of wire, oral, or electronic communications;

(10) “communication common carrier” has the meaning given the term in section 3 of the Communications Act of 1934;

(11) “aggrieved person” means a person who was a party to any intercepted wire, oral, or electronic communication or a person against whom the interception was directed;

(12) “electronic communication” means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include–
(A) any wire or oral communication;
(B) any communication made through a tone-only paging device;
(C) any communication from a tracking device (as defined in section 3117 of this title); or
(D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds;

(13) “user” means any person or entity who–
(A) uses an electronic communication service; and
(B) is duly authorized by the provider of such service to engage in such use;

(14) “electronic communications system” means any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications;

(15) “electronic communication service” means any service which provides to users thereof the ability to send or receive wire or electronic communications;

(16) “readily accessible to the general public” means, with respect to a radio communication, that such communication is not–
(A) scrambled or encrypted;
(B) transmitted using modulation techniques whose essential parameters have been withheld from the public with the intention of preserving the privacy of such communication;
(C) carried on a subcarrier or other signal subsidiary to a radio transmission;
(D) transmitted over a communication system provided by a common carrier, unless the communication is a tone only paging system communication; or
(E) transmitted on frequencies allocated under part 25, subpart D, E, or F of part 74, or part 94 of the Rules of the Federal Communications Commission, unless, in the case of a communication transmitted on a frequency allocated under part 74 that is not exclusively allocated to broadcast auxiliary services, the communication is a two-way voice communication by radio;

(17) “electronic storage” means–
(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and
(B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication;

(18) “aural transfer” means a transfer containing the human voice at any point between and including the point of origin and the point of reception.

(19) “foreign intelligence information”, for purposes of section 2517(6) of this title, means –
(A) information, whether or not concerning a United States person, that relates to the ability of the United States to protect against –
(i) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
(ii) sabotage or intentional terrorism by a foreign power or an agent of a foreign power; or
(iii) clandestine intelligence activities by and intelligence service or network of a foreign power or by an agent of a foreign power; or

• information, whether or not concerning a United States person, with respect to a foreign power or foreign territory that relates to –
• the national defense or the security of the United States; or
• the conduct of the foreign affairs of the United States.
• “protected computer” has the meaning set forth in section 1030; and
• “computer trespasser” –
• means a person who accesses a protected computer without authorization and thus has no reasonable expectation of privacy in any communication transmitted to, through, or from the protected computer; and
• does not include a person known by the owner or operator of the protected computer to have an existing contractual relationship with the owner or operator of the protected computer for access to all or part of the protected computer.

18 U.S.C. 2511. Interception and disclosure of wire, oral, or electronic communications prohibited

(1) Except as otherwise specifically provided in this chapter any person who–

(a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;

(b) intentionally uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when-

(i) such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication; or

(ii) such device transmits communications by radio, or interferes with the transmission of such communication; or

(iii) such person knows, or has reason to know, that such device or any component thereof has been sent through the mail or transported in interstate or foreign commerce; or

(iv) such use or endeavor to use

(A) takes place on the premises of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or

(B) obtains or is for the purpose of obtaining information relating to the operations of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or

(v) such person acts in the District of Columbia, the Commonwealth of Puerto Rico, or any territory or possession of the United States;

(c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;

(d) intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection; or

(e) (i) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, intercepted by means authorized by sections 2511(2)(a)(ii), 2511(2)(b)-(c), 2511(2)(e), 2516, and 2518 of this chapter, (ii) knowing or having reason to know that the information was obtained through the interception of such a communication in connection with a criminal investigation, (iii) having obtained or received the information in connection with a criminal investigation, and (iv) with intent to improperly obstruct, impede, or interfere with a duly authorized criminal investigation, shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).

(2)

(a)
(i) It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.
(ii) Notwithstanding any other law, providers of wire or electronic communication service, their officers, employees, and agents, landlords, custodians, or other persons, are authorized to provide information, facilities, or technical assistance to persons authorized by law to intercept wire, oral, or electronic communications or to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, if such provider, its officers, employees, or agents, landlord, custodian, or other specified person, has been provided with–

[Sec. 101(c)(1)]295 (A) a court order directing such assistance or a court order pursuant to section 704 of the Foreign Intelligence Surveillance Act of 1978 signed by the authorizing judge, [Sec.403(b)(2)(C)] Effective December 31, 2012 . . . (C) except as provided in section 404, section 2511(2)(A)(ii)(A) of title 28, United States Code, is amended by striking "or a court order pursuant to section 704 of the Foreign Intelligence Surveillance Act of 1978". [Sec. 404(b)(3)] Challenge of directives; protection from liability; use of information – Notwithstanding any other provision of this Act or of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) . . . (E) section 2511(2)(a)(ii)(A) of title 18, United States Code, as amended by section 101(c)(1), shall continue to apply to an order issued pursuant to section 704 of the Foreign Intelligence Surveillance Act of 1978, as added by section 101(a)[50 U.S.C. 1881c]; or
(B) a certification in writing by a person specified in section 2518(7) of this title or the Attorney General of the United States that no warrant or court order is required by law, that all statutory requirements have been met, and that the specified assistance is required, setting forth the period of time during which the provision of the information, facilities, or technical assistance is authorized and specifying the information, facilities, or technical assistance required. No provider of wire or electronic communication service, officer, employee, or agent thereof, or landlord, custodian, or other specified person shall disclose the existence of any interception or surveillance or the device used to accomplish the interception or surveillance with respect to which the person has been furnished a court order or certification under this chapter, except as may otherwise be required by legal process and then only after prior notification to the Attorney General or to the principal prosecuting attorney of a State or any political subdivision of a State, as may be appropriate. Any such disclosure, shall render such person liable for the civil damages provided for in section 2520. No cause of action shall lie in any court against any provider of wire or electronic

communication service, its officers, employees, or agents, landlord, custodian, or other specified person for providing information, facilities, or assistance in accordance with the terms of a court order, statutory authorization, or certification under this chapter.

[Sec. 102(c)(1)] (iii) If a certification under subparagraph (ii)(B) for assistance to obtain foreign intelligence information is based on statutory authority, the certification shall identify the specific statutory provision and shall certify that the statutory requirements have been met.

(b) It shall not be unlawful under this chapter for an officer, employee, or agent of the Federal Communications Commission, in the normal course of his employment and in discharge of the monitoring responsibilities exercised by the Commission in the enforcement of chapter 5 of title 47 of the United States Code, to intercept a wire or electronic communication, or oral communication transmitted by radio, or to disclose or use the information thereby obtained.

(c) It shall not be unlawful under this chapter for a person acting under color of law to intercept a wire, oral, or electronic communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception.

(d) It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.

(e) Notwithstanding any other provision of this title or section 705 or 706 of the Communications Act of 1934, it shall not be unlawful for an officer, employee, or agent of the United States in the normal course of his official duty to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, as authorized by that Act.

(f) Nothing contained in this chapter or chapter 121 or 206 of this title, or section 705 of the Communications Act of 1934, shall be deemed to affect the acquisition by the United States Government of foreign intelligence information from international or foreign communications, or foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic communications system, utilizing a means other than electronic surveillance as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, and procedures in this chapter or chapter 121 and the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which electronic surveillance, as defined in section 101 of such Act, and the interception of domestic wire, oral, and electronic communications may be conducted.

(g) It shall not be unlawful under this chapter or chapter 121 of this title for any person-

(i) to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public;

(ii) to intercept any radio communication which is transmitted–

(I) by any station for the use of the general public, or that relates to ships, aircraft, vehicles, or persons in distress;

(II) by any governmental, law enforcement, civil defense, private land mobile, or public safety communications system, including police and fire, readily accessible to the general public;

(III) by a station operating on an authorized frequency within the bands allocated to the amateur, citizens band, or general mobile radio services; or

(IV) by any marine or aeronautical communications system;

(iii) to engage in any conduct which-

(I) is prohibited by section 633 of the Communications Act of 1934; or

(II) is excepted from the application of section 705(a) of the Communications Act of 1934 by section 705(b) of that Act;

(iv) to intercept any wire or electronic communication the transmission of which is causing harmful interference to any lawfully operating station or consumer electronic equipment, to the extent necessary to identify the source of such interference; or

(v) for other users of the same frequency to intercept any radio communication made through a system that utilizes frequencies monitored by individuals engaged in the provision or the use of such system, if such communication is not scrambled or encrypted.

(h) It shall not be unlawful under this chapter–

(i) to use a pen register or a trap and trace device (as those terms are defined for the purposes of chapter 206 (relating to pen registers and trap and trace devices) of this title); or

(ii) for a provider of electronic communication service to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire or electronic communication, or a user of that service, from fraudulent, unlawful or abusive use of such service.

(i) It shall not be unlawful under this chapter for a person acting under color of law to intercept the wire or electronic communications of a computer trespasser transmitted to, through, or from the protected computer, if–

(I) the owner or operator of the protected computer authorizes the interception of the computer trespasser's communications on the protected computer;

(II) the person acting under color of law is lawfully engaged in an investigation;

(III) the person acting under color of law has reasonable grounds to believe that the contents of the computer trespasser's communications will be relevant to the investigation; and

(IV) such interception does not acquire communications other than those transmitted to or from the computer trespasser.

(3)
(a) Except as provided in paragraph (b) of this subsection, a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient.

- A person or entity providing electronic communication service to the public may divulge the contents of any such communication–
- as otherwise authorized in section 2511(2)(a) or 2517 of this title;
- with the lawful consent of the originator or any addressee or intended recipient of such communication;

(iii) to a person employed or authorized, or whose facilities are used, to forward such communication to its destination; or
(iv) which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency.

(4)(a) Except as provided in paragraph (b) of this subsection or in subsection (5), whoever violates subsection (1) of this section shall be fined under this title or imprisoned not more than five years, or both.

- Conduct otherwise an offense under this subsection that consists of or relates to the interception of a satellite transmission that is not encrypted or scrambled and that is transmitted–
- to a broadcasting station for purposes of retransmission to the general public; or
- as an audio subcarrier intended for redistribution to facilities open to the public, but not including data transmissions or telephone calls, is not an offense under this subsection unless the conduct is for the purposes of direct or indirect commercial advantage or private financial gain.

(c)[Redesignated (b)] (5)(a)(i) If the communication is–

(A) a private satellite video communication that is not scrambled or encrypted and the conduct in violation of this chapter is the private viewing of that communication and is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain; or
(B) a radio communication that is transmitted on frequencies allocated under subpart D of part 74 of the rules of the Federal Communications Commission that is not scrambled or encrypted and the conduct in violation of this chapter is not

for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain, then the person who engages in such conduct shall be subject to suit by the Federal Government in a court of competent jurisdiction.
(ii) In an action under this subsection–
(A) if the violation of this chapter is a first offense for the person under paragraph (a) of subsection (4) and such person has not been found liable in a civil action under section 2520 of this title, the Federal Government shall be entitled to appropriate injunctive relief; and
(B) if the violation of this chapter is a second or subsequent offense under paragraph (a) of subsection (4) or such person has been found liable in any prior civil action under section 2520, the person shall be subject to a mandatory $500 civil fine.
(b) The court may use any means within its authority to enforce an injunction issued under paragraph (ii)(A), and shall impose a civil fine of not less than $500 for each violation of such an injunction.

18 U.S.C. 2512. Manufacture, distribution, possession, and advertising of wire, oral, or electronic communication intercepting devices prohibited

(1) Except as otherwise specifically provided in this chapter, any person who intentionally–

(a) sends through the mail, or sends or carries in interstate or foreign commerce, any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications;
(b) manufactures, assembles, possesses, or sells any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications, and that such device or any component thereof has been or will be sent through the mail or transported in interstate or foreign commerce; or
(c) places in any newspaper, magazine, handbill, or other publication or disseminates by electronic means any advertisement of–
(i) any electronic, mechanical, or other device knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications; or
(ii) any other electronic, mechanical, or other device, where such advertisement promotes the use of such device for the purpose of the surreptitious interception of wire, oral, or electronic communications, knowing the content of the advertisement and knowing or having reason to know that such advertisement will be sent through the mail or transported in interstate or foreign commerce, shall be fined under this title or imprisoned not more than five years, or both.

(2) It shall not be unlawful under this section for–

(a) a provider of wire or electronic communication service or an officer, agent, or employee of, or a person under contract with, such a provider, in the normal course of the business of providing that wire or electronic communication service, or

(b) an officer, agent, or employee of, or a person under contract with, the United States, a State, or a political subdivision thereof, in the normal course of the activities of the United States, a State, or a political subdivision thereof, to send through the mail, send or carry in interstate or foreign commerce, or manufacture, assemble, possess, or sell any electronic, mechanical, or other device knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications.

(3) It shall not be unlawful under this section to advertise for sale a device described in subsection (1) of this section if the advertisement is mailed, sent, or carried in interstate or foreign commerce solely to a domestic provider of wire or electronic communication service or to an agency of the United States, a State, or a political subdivision thereof which is duly authorized to use such device.

18 U.S.C. 2513. Confiscation of wire, oral, or electronic communication interception devices

Any electronic, mechanical, or other device used, sent, carried, manufactured, assembled, possessed, sold, or advertised in violation of section 2511 or section 2512 of this chapter may be seized and forfeited to the United States. All provisions of law relating to (1) the seizure, summary and judicial forfeiture, and condemnation of vessels, vehicles, merchandise, and baggage for violations of the customs laws contained in title 19 of the United States Code, (2) the disposition of such vessels, vehicles, merchandise, and baggage or the proceeds from the sale thereof, (3) the remission or mitigation of such forfeiture, (4) the compromise of claims, and (5) the award of compensation to informers in respect of such forfeitures, shall apply to seizures and forfeitures incurred, or alleged to have been incurred, under the provisions of this section, insofar as applicable and not inconsistent with the provisions of this section; except that such duties as are imposed upon the collector of customs or any other person with respect to the seizure and forfeiture of vessels, vehicles, merchandise, and baggage under the provisions of the customs laws contained in title 19 of the United States Code shall be performed with respect to seizure and forfeiture of electronic, mechanical, or other intercepting devices under this section by such officers, agents, or other persons as may be authorized or designated for that purpose by the Attorney General.

18 U.S.C. 2515. Prohibition of use as evidence of intercepted wire or oral communications

Whenever any wire or oral communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding in or before any

court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof if the disclosure of that information would be in violation of this chapter.

18 U.S.C. 2516. Authorization for interception of wire, oral, or electronic communications

(1) The Attorney General, Deputy Attorney General, Associate Attorney General, or any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General or acting Deputy Assistant Attorney General in the Criminal Division or National Security Division specially designated by the Attorney General, may authorize an application to a Federal judge of competent jurisdiction for, and such judge may grant in conformity with section 2518 of this chapter an order authorizing or approving the interception of wire or oral communications by the Federal Bureau of Investigation, or a Federal agency having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of–

(a) any offense punishable by death or by imprisonment for more than one year under sections 2122 and 2274 through 2277 of title 42 of the United States Code (relating to the enforcement of the Atomic Energy Act of 1954), section 2284 of title 42 of the United States Code (relating to sabotage of nuclear facilities or fuel), or under the following chapters of this title: chapter 10 (relating to biological weapons) chapter 37 (relating to espionage), chapter 55 (relating to kidnapping), chapter 90 (relating to protection of trade secrets), chapter 105 (relating to sabotage), chapter 115 (relating to treason), chapter 102 (relating to riots), chapter 65 (relating to malicious mischief), chapter 111 (relating to destruction of vessels), or chapter 81 (relating to piracy);

(b) a violation of section 186 or section 501(c) of title 29, United States Code (dealing with restrictions on payments and loans to labor organizations), or any offense which involves murder, kidnapping, robbery, or extortion, and which is punishable under this title;

(c) any offense which is punishable under the following sections of this title: section 37 (relating to violence at international airports), section 43 (relating to animal enterprise terrorism), section 81 (arson within special maritime and territorial jurisdiction), section 201 (bribery of public officials and witnesses), section 215 (relating to bribery of bank officials), section 224 (bribery in sporting contests), subsection (d), (e), (f), (g), (h), or (i) of section 844 (unlawful use of explosives), section 1032 (relating to concealment of assets), section 1084 (transmission of wagering information), section 751 (relating to escape), section 832 (relating to nuclear and weapons of mass destruction threats), section 842 (relating to explosive materials), section 930 (relating to possession of weapons in Federal facilities), section 1014 (relating to loans and credit applications generally; renewals and discounts), section 1114 (relating to officers and employees of the United States), section 1116 (relating to protection of foreign officials), sections 1503, 1512, and 1513 (influencing or injuring an officer, juror, or witness generally), section 1510 (obstruction of criminal investigations),

section 1511 (obstruction of State or local law enforcement), section 1591 (sex trafficking of children by force, fraud, or coercion), section 1751 (Presidential and Presidential staff assassination, kidnapping, and assault), section 1951 (interference with commerce by threats or violence), section 1952 (interstate and foreign travel or transportation in aid of racketeering enterprises), section 1958 (relating to use of interstate commerce facilities in the commission of murder for hire), section 1959 (relating to violent crimes in aid of racketeering activity), section 1954 (offer, acceptance, or solicitation to influence operations of employee benefit plan), section 1955 (prohibition of business enterprises of gambling), section 1956 (laundering of monetary instruments), section 1957 (relating to engaging in monetary transactions in property derived from specified unlawful activity), section 659 (theft from interstate shipment), section 664 (embezzlement from pension and welfare funds), section 1343 (fraud by wire, radio, or television), section 1344 (relating to bank fraud), section 1992 (relating to terrorist attacks against mass transportation), sections 2251 and 2252 (sexual exploitation of children), section 2251A (selling or buying of children), section 2252A (relating to material constituting or containing child pornography), section 1466A (relating to child obscenity), section 2260 (production of sexually explicit depictions of a minor for importation into the United States), sections 2421, 2422, 2423, and 2425 (relating to transportation for illegal sexual activity and related crimes), sections 2312, 2313, 2314, and 2315 (interstate transportation of stolen property), section 2321 (relating to trafficking in certain motor vehicles or motor vehicle parts), section 2340A (relating to torture), section 1203 (relating to hostage taking), section 1029 (relating to fraud and related activity in connection with access devices), section 3146 (relating to penalty for failure to appear), section 3521(b)(3) (relating to witness relocation and assistance), section 32 (relating to destruction of aircraft or aircraft facilities), section 38 (relating to aircraft parts fraud), section 1963 (violations with respect to racketeer influenced and corrupt organizations), section 115 (relating to threatening or retaliating against a Federal official), section 1341 (relating to mail fraud), a felony violation of section 1030 (relating to computer fraud and abuse), section 351 (violations with respect to congressional, Cabinet, or Supreme Court assassinations, kidnapping, and assault), section 831 (relating to prohibited transactions involving nuclear materials), section 33 (relating to destruction of motor vehicles or motor vehicle facilities), section 175 (relating to biological weapons), section 175c (relating to variola virus), section 956 (conspiracy to harm persons or property overseas), section a felony violation of section 1028 (relating to production of false identification documentation), section 1425 (relating to the procurement of citizenship or nationalization unlawfully), section 1426 (relating to the reproduction of naturalization or citizenship papers), section 1427 (relating to the sale of naturalization or citizenship papers), section 1541 (relating to passport issuance without authority), section 1542 (relating to false statements in passport applications), section 1543 (relating to forgery or false use of passports), section 1544 (relating to misuse of passports), or section 1546 (relating to fraud and misuse of visas, permits, and other documents);

(d) any offense involving counterfeiting punishable under section 471, 472, or 473 of this title;
(e) any offense involving fraud connected with a case under title 11 or the manufacture, importation, receiving, concealment, buying, selling, or otherwise dealing in narcotic drugs, marihuana, or other dangerous drugs, punishable under any law of the United States;
(f) any offense including extortionate credit transactions under sections 892, 893, or 894 of this title;
(g) a violation of section 5322 of title 31, United States Code (dealing with the reporting of currency transactions), or section 5324 of title 31, United States Code (relating to structuring transactions to evade reporting requirement prohibited);
(h) any felony violation of sections 2511 and 2512 (relating to interception and disclosure of certain communications and to certain intercepting devices) of this title;
(i) any felony violation of chapter 71 (relating to obscenity) of this title;
(j) any violation of section 60123(b) (relating to destruction of a natural gas pipeline), section 46502 (relating to aircraft piracy), the second sentence of section 46504 (relating to assault on a flight crew with dangerous weapon), or section 46505(b)(3) or (c) (relating to explosive or incendiary devices, or endangerment of human life, by means of weapons on aircraft) of title 49;
(k) any criminal violation of section 2778 of title 22 (relating to the Arms Export Control Act);
(l) the location of any fugitive from justice from an offense described in this section;
(m) a violation of section 274, 277, or 278 of the Immigration and Nationality Act (8 U.S.C. 1324, 1327, or 1328) (relating to the smuggling of aliens);
(n) any felony violation of sections 922 and 924 of title 18, United States Code (relating to firearms);
(o) any violation of section 5861 of the Internal Revenue Code of 1986 (relating to firearms);
(p) a felony violation of section 1028 (relating to production of false identification documents), section 1542 (relating to false statements in passport applications), section 1546 (relating to fraud and misuse of visas, permits, and other documents, section 1028A (relating to aggravated identity theft)) of this title or a violation of section 274, 277, or 278 of the Immigration and Nationality Act (relating to the smuggling of aliens); or
(q) any criminal violation of section 229 (relating to chemical weapons): or sections 2332, 2332a, 2332b, 2332d, 2332f, 2332g, 2332h 2339, 2339A, 2339B, 2339C, or 2339D of this title (relating to terrorism);
(r) any criminal violation of section 1 (relating to illegal restraints of trade or commerce), 2 (relating to illegal monopolizing of trade or commerce), or 3 (relating to illegal restraints of trade or commerce in territories or the District of Columbia) of the Sherman Act (15 U.S.C. 1, , 3); or
(s) any conspiracy to commit any offense described in any subparagraph of this paragraph.

(2) The principal prosecuting attorney of any State, or the principal prosecuting attorney of any political subdivision thereof, if such attorney is authorized by a statute of that State to make application to a State court judge of competent jurisdiction for an order authorizing or approving the interception of wire, oral, or electronic communications, may apply to such judge for, and such judge may grant in conformity with section 2518 of this chapter and with the applicable State statute an order authorizing, or approving the interception of wire, oral, or electronic communications by investigative or law enforcement officers having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of the commission of the offense of murder, kidnapping, gambling, robbery, bribery, extortion, or dealing in narcotic drugs, marihuana or other dangerous drugs, or other crime dangerous to life, limb, or property, and punishable by imprisonment for more than one year, designated in any applicable State statute authorizing such interception, or any conspiracy to commit any of the foregoing offenses.

(3) Any attorney for the Government (as such term is defined for the purposes of the Federal Rules of Criminal Procedure) may authorize an application to a Federal judge of competent jurisdiction for, and such judge may grant, in conformity with section 2518 of this title, an order authorizing or approving the interception of electronic communications by an investigative or law enforcement officer having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of any Federal felony.

18 U.S.C. 2517. Authorization for disclosure and use of intercepted wire, oral, or electronic communications

- Any investigative or law enforcement officer who, by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents to another investigative or law enforcement officer to the extent that such disclosure is appropriate to the proper performance of the official duties of the officer making or receiving the disclosure.
- Any investigative or law enforcement officer who, by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication or evidence derived therefrom may use such contents to the extent such use is appropriate to the proper performance of his official duties.
- Any person who has received, by any means authorized by this chapter, any information concerning a wire, oral, or electronic communication, or evidence derived therefrom intercepted in accordance with the provisions of this chapter may disclose the contents of that communication or such derivative evidence while giving testimony under oath or affirmation in any proceeding held under the authority of the United States or of any State or political subdivision thereof.

- No otherwise privileged wire, oral, or electronic communication intercepted in accordance with, or in violation of, the provisions of this chapter shall lose its privileged character.
- When an investigative or law enforcement officer, while engaged in intercepting wire, oral, or electronic communications in the manner authorized herein, intercepts wire, oral, or electronic communications relating to offenses other than those specified in the order of authorization or approval, the contents thereof, and evidence derived therefrom, may be disclosed or used as provided in subsections (1) and (2) of this section. Such contents and any evidence derived therefrom may be used under subsection (3) of this section when authorized or approved by a judge of competent jurisdiction where such judge finds on subsequent application that the contents were otherwise intercepted in accordance with the provisions of this chapter. Such application shall be made as soon as practicable.
- Any investigative or law enforcement officer, or attorney for the Government, who by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents to any Federal law enforcement, intelligence, protective, immigration, national defense, or national security official to the extent that such contents include foreign intelligence or counterintelligence (as defined in section 3 of the National Security act of 1947 (50 U.S.C. 401a), or foreign intelligence information (as defined in subsection (19) of section 2510 of this title), to assist the official who is to receive that information in the performance of his official duties. Any Federal official who receives information pursuant to this provision may use that information only as necessary in the conduct of that person's official duties subject to any limitations on the unauthorized disclosure of such information.
- Any investigative or law enforcement officer, or other Federal official in carrying out official duties as such Federal official, who by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents or derivative evidence to a foreign investigative or law enforcement officer to the extent that such disclosure is appropriate to the proper performance of the official duties of the officer making or receiving the disclosure, and foreign investigative or law enforcement officers may use or disclose such contents or derivative evidence to the extent such use or disclosure is appropriate to the proper performance of their official duties.
- Any investigative or law enforcement officer, or other Federal official in carrying out official duties as such Federal official, who by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents or derivative evidence to any appropriate Federal, State, local, or foreign government official to the extent that such contents or derivative evidence reveals a threat of actual or potential

attack or other grave hostile acts of a foreign power of an agent of as foreign power, domestic or international sabotage, domestic or international terrorism, or clandestine intelligence gathering activities by an intelligence service or network of a foreign power or by an agent of a foreign power, within the United States or elsewhere, for the purpose of preventing or responding to such a threat. Any official who receives information pursuant to this provision may use that information only as necessary in the conduct of that person's official duties subject to any limitations on the unauthorized disclosure of such information, and any State, local, or foreign official who receives information pursuant to this provision may use that information only consistent with such guidelines as the Attorney General and Director of Central Intelligence shall jointly issue.

18 U.S.C. 2518. Procedure for interception of wire, oral, or electronic communications

(1) Each application for an order authorizing or approving the interception of a wire, oral, or electronic communication under this chapter shall be made in writing upon oath or affirmation to a judge of competent jurisdiction and shall state the applicant's authority to make such application. Each application shall include the following information:

(a) the identity of the investigative or law enforcement officer making the application, and the officer authorizing the application;

(b) a full and complete statement of the facts and circumstances relied upon by the applicant, to justify his belief that an order should be issued, including (i) details as to the particular offense that has been, is being, or is about to be committed, (ii) except as provided in subsection (11), a particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted, (iii) a particular description of the type of communications sought to be intercepted, (iv) the identity of the person, if known, committing the offense and whose communications are to be intercepted;

(c) a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous;

(d) a statement of the period of time for which the interception is required to be maintained. If the nature of the investigation is such that the authorization for interception should not automatically terminate when the described type of communication has been first obtained, a particular description of facts establishing probable cause to believe that additional communications of the same type will occur thereafter;

(e) a full and complete statement of the facts concerning all previous applications known to the individual authorizing and making the application, made to any judge for authorization to intercept, or for approval of interceptions of, wire, oral, or electronic communications involving any of the same persons, facilities or places specified in the application, and the action taken by the judge on each such application; and

(f) where the application is for the extension of an order, a statement setting forth the results thus far obtained from the interception, or a reasonable explanation of the failure to obtain such results.

(2) The judge may require the applicant to furnish additional testimony or documentary evidence in support of the application.

(3) Upon such application the judge may enter an ex parte order, as requested or as modified, authorizing or approving interception of wire, oral, or electronic communications within the territorial jurisdiction of the court in which the judge is sitting (and outside that jurisdiction but within the United States in the case of a mobile interception device authorized by a Federal court within such jurisdiction), if the judge determines on the basis of the facts submitted by the applicant that–
(a) there is probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense enumerated in section 2516 of this chapter;
(b) there is probable cause for belief that particular communications concerning that offense will be obtained through such interception;
(c) normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous;
(d) except as provided in subsection (11), there is probable cause for belief that the facilities from which, or the place where, the wire, oral, or electronic communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such person.

(4) Each order authorizing or approving the interception of any wire, oral, or electronic communication under this chapter shall specify-
(a) the identity of the person, if known, whose communications are to be intercepted;
(b) the nature and location of the communications facilities as to which, or the place where, authority to intercept is granted;
(c) a particular description of the type of communication sought to be intercepted, and a statement of the particular offense to which it relates;
(d) the identity of the agency authorized to intercept the communications, and of the person authorizing the application; and
(e) the period of time during which such interception is authorized, including a statement as to whether or not the interception shall automatically terminate when the described communication has been first obtained. An order authorizing the interception of a wire, oral, or electronic communication under this chapter shall, upon request of the applicant, direct that a provider of wire or electronic communication service, landlord, custodian or other person shall furnish the applicant forthwith all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference with the services that such service provider, landlord, custodian, or person is according the person whose communications are to be intercepted. Any provider

of wire or electronic communication service, landlord, custodian or other person furnishing such facilities or technical assistance shall be compensated therefor by the applicant for reasonable expenses incurred in providing such facilities or assistance. Pursuant to section 2522 of this chapter, an order may also be issued to enforce the assistance capability and capacity requirements under the Communications Assistance for Law Enforcement Act.

(5) No order entered under this section may authorize or approve the interception of any wire, oral, or electronic communication for any period longer than is necessary to achieve the objective of the authorization, nor in any event longer than thirty days. Such thirty-day period begins on the earlier of the day on which the investigative or law enforcement officer first begins to conduct an interception under the order or ten days after the order is entered. Extensions of an order may be granted, but only upon application for an extension made in accordance with subsection (1) of this section and the court making the findings required by subsection (3) of this section. The period of extension shall be no longer than the authorizing judge deems necessary to achieve the purposes for which it was granted and in no event for longer than thirty days. Every order and extension thereof shall contain a provision that the authorization to intercept shall be executed as soon as practicable, shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter, and must terminate upon attainment of the authorized objective, or in any event in thirty days. In the event the intercepted communication is in a code or foreign language, and an expert in that foreign language or code is not reasonably available during the interception period, minimization may be accomplished as soon as practicable after such interception. An interception under this chapter may be conducted in whole or in part by Government personnel, or by an individual operating under a contract with the Government, acting under the supervision of an investigative or law enforcement officer authorized to conduct the interception.

(6) Whenever an order authorizing interception is entered pursuant to this chapter, the order may require reports to be made to the judge who issued the order showing what progress has been made toward achievement of the authorized objective and the need for continued interception. Such reports shall be made at such intervals as the judge may require.

(7) Notwithstanding any other provision of this chapter, any investigative or law enforcement officer, specially designated by the Attorney General, the Deputy Attorney General, the Associate Attorney General, or by the principal prosecuting attorney of any State or subdivision thereof acting pursuant to a statute of that State, who reasonably determines that–

(a) an emergency situation exists that involves–

(i) immediate danger of death or serious physical injury to any person,

(ii) conspiratorial activities threatening the national security interest, or

(iii) conspiratorial activities characteristic of organized crime, that requires a wire, oral, or electronic communication to be intercepted before an order authorizing such interception can, with due diligence, be obtained, and

(b) there are grounds upon which an order could be entered under this chapter to authorize such interception, may intercept such wire, oral, or electronic communication if an application for an order approving the interception is made in accordance with this section within forty-eight hours after the interception has occurred, or begins to occur. In the absence of an order, such interception shall immediately terminate when the communication sought is obtained or when the application for the order is denied, whichever is earlier. In the event such application for approval is denied, or in any other case where the interception is terminated without an order having been issued, the contents of any wire, oral, or electronic communication intercepted shall be treated as having been obtained in violation of this chapter, and an inventory shall be served as provided for in subsection (d) of this section on the person named in the application.

(8)

(a) The contents of any wire, oral, or electronic communication intercepted by any means authorized by this chapter shall, if possible, be recorded on tape or wire or other comparable device. The recording of the contents of any wire, oral, or electronic communication under this subsection shall be done in such way as will protect the recording from editing or other alterations. Immediately upon the expiration of the period of the order, or extensions thereof, such recordings shall be made available to the judge issuing such order and sealed under his directions. Custody of the recordings shall be wherever the judge orders. They shall not be destroyed except upon an order of the issuing or denying judge and in any event shall be kept for ten years. Duplicate recordings may be made for use or disclosure pursuant to the provisions of subsections

(1) and (2) of section 2517 of this chapter for investigations. The presence of the seal provided for by this subsection, or a satisfactory explanation for the absence thereof, shall be a prerequisite for the use or disclosure of the contents of any wire, oral, or electronic communication or evidence derived therefrom under subsection (3) of section 2517.

(b) Applications made and orders granted under this chapter shall be sealed by the judge. Custody of the applications and orders shall be wherever the judge directs. Such applications and orders shall be disclosed only upon a showing of good cause before a judge of competent jurisdiction and shall not be destroyed except on order of the issuing or denying judge, and in any event shall be kept for ten years.

(c) Any violation of the provisions of this subsection may be punished as contempt of the issuing or denying judge.

(d) Within a reasonable time but not later than ninety days after the filing of an application for an order of approval under section 2518(7)(b) which is denied or the termination of the period of an order or extensions thereof, the issuing or denying judge shall cause to be served, on the persons named in the order or the application, and such other parties to intercepted communications as the judge

may determine in his discretion that is in the interest of justice, an inventory which shall include notice of–

- the fact of the entry of the order or the application;
- the date of the entry and the period of authorized, approved or disapproved interception, or the denial of the application; and
- the fact that during the period wire, oral, or electronic communications were or were not intercepted. The judge, upon the filing of a motion, may in his discretion make available to such person or his counsel for inspection such portions of the intercepted communications, applications and orders as the judge determines to be in the interest of justice. On an ex parte showing of good cause to a judge of competent jurisdiction the serving of the inventory required by this subsection may be postponed.

(9) The contents of any wire, oral, or electronic communication intercepted pursuant to this chapter or evidence derived therefrom shall not be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in a Federal or State court unless each party, not less than ten days before the trial, hearing, or proceeding, has been furnished with a copy of the court order, and accompanying application, under which the interception was authorized or approved. This ten-day period may be waived by the judge if he finds that it was not possible to furnish the party with the above information ten days before the trial, hearing, or proceeding and that the party will not be prejudiced by the delay in receiving such information.

(10)(a) Any aggrieved person in any trial, hearing, or proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, may move to suppress the contents of any wire or oral communication intercepted pursuant to this chapter, or evidence derived therefrom, on the grounds that

- the communication was unlawfully intercepted;
- the order of authorization or approval under which it was intercepted is insufficient on its face; or

(iii) the interception was not made in conformity with the order of authorization or

approval. Such motion shall be made before the trial, hearing, or proceeding unless there was no opportunity to make such motion or the person was not aware of the grounds of the motion. If the motion is granted, the contents of the intercepted wire or oral communication, or evidence derived therefrom, shall be treated as having been obtained in violation of this chapter. The judge, upon the filing of such motion by the aggrieved person, may in his discretion make available to the aggrieved person or his counsel for inspection such portions of the intercepted communication or evidence derived therefrom as the judge determines to be in the interests of justice.

- In addition to any other right to appeal, the United States shall have the right to appeal from an order granting a motion to suppress made under paragraph (a) of this subsection, or the denial of an application for an order of approval, if the United States attorney shall certify to the judge or other official granting such motion or denying such application that the appeal is not taken for purposes of delay. Such appeal shall be taken within thirty days after the date the order was entered and shall be diligently prosecuted.
- The remedies and sanctions described in this chapter with respect to the interception of electronic communications are the only judicial remedies and sanctions for nonconstitutional violations of this chapter involving such communications.
- The requirements of subsections (1)(b)(ii) and (3)(d) of this section relating to the specification of the facilities from which, or the place where, the communication is to be intercepted do not apply if–
- in the case of an application with respect to the interception of an oral communication-
- the application is by a Federal investigative or law enforcement officer and is approved by the Attorney General, the Deputy Attorney General, the Associate Attorney General, an Assistant Attorney General, or an acting Assistant Attorney General;
- the application contains a full and complete statement as to why such specification is not practical and identifies the person committing the offense and whose communications are to be intercepted; and

(iii) the judge finds that such specification is not practical; and

- in the case of an application with respect to a wire or electronic communication–
- the application is by a Federal investigative or law enforcement officer and is approved by the Attorney General, the Deputy Attorney General, the Associate Attorney General, an Assistant Attorney General, or an acting Assistant Attorney General;
- the application identifies the person believed to be committing the offense and whose communications are to be intercepted and the applicant makes a showing that there is probable cause to believe that the person's actions could have the effect of thwarting interception from a specified facility;

(iii) the judge finds that such showing has been adequately made; and

- the order authorizing or approving the interception is limited to interception only for such time as it is reasonable to presume that the person identified in the application is or was reasonably proximate to the instrument through which such communication will be or was transmitted.
- An interception of a communication under an order with respect to which the requirements of subsections (1)(b)(ii) and (3)(d) of this section do not apply by reason of subsection (11)(a) shall not begin until the place where the communication is to be intercepted is ascertained by the person

implementing the interception order. A provider of wire or electronic communications service that has received an order as provided for in subsection (11)(b) may move the court to modify or quash the order on the ground that its assistance with respect to the interception cannot be performed in a timely or reasonable fashion. The court, upon notice to the government, shall decide such a motion expeditiously.

18 U.S.C. 2519. Reports concerning intercepted wire, oral, or electronic communications

(1) Within thirty days after the expiration of an order (or each extension thereof) entered under section 2518, or the denial of an order approving an interception, the issuing or denying judge shall report to the Administrative Office of the United States Courts–

(a) the fact that an order or extension was applied for;

(b) the kind of order or extension applied for (including whether or not the order was an order with respect to which the requirements of sections 2518(1)(b)(ii) and 2518(3)(d) of this title did not apply by reason of section 2518(11) of this title);

(c) the fact that the order or extension was granted as applied for, was modified, or was denied;

(d) the period of interceptions authorized by the order, and the number and duration of any extensions of the order;

(e) the offense specified in the order or application, or extension of an order;

(f) the identity of the applying investigative or law enforcement officer and agency making the application and the person authorizing the application; and

(g) the nature of the facilities from which or the place where communications were to be intercepted.

(2) In January of each year the Attorney General, an Assistant Attorney General specially designated by the Attorney General, or the principal prosecuting attorney of a State, or the principal prosecuting attorney for any political subdivision of a State, shall report to the Administrative Office of the United States Courts–

(a) the information required by paragraphs (a) through (g) of subsection (1) of this section with respect to each application for an order or extension made during the preceding calendar year;

(b) a general description of the interceptions made under such order or extension, including (i) the approximate nature and frequency of incriminating communications intercepted, (ii) the approximate nature and frequency of other communications intercepted, (iii) the approximate number of persons whose communications were intercepted, (iv) the number of orders in which encryption was encountered and whether such encryption prevented law enforcement from obtaining the plain text of communications intercepted pursuant to such order, and (v) the approximate nature, amount, and cost of the manpower and other resources used in the interceptions;

(c) the number of arrests resulting from interceptions made under such order or extension, and the offenses for which arrests were made;
(d) the number of trials resulting from such interceptions;
(e) the number of motions to suppress made with respect to such interceptions, and the number granted or denied;
(f) the number of convictions resulting from such interceptions and the offenses for which the convictions were obtained and a general assessment of the importance of the interceptions; and
(g) the information required by paragraphs (b) through (f) of this subsection with respect to orders or extensions obtained in a preceding calendar year.

(3) In April of each year the Director of the Administrative Office of the United States Courts shall transmit to the Congress a full and complete report concerning the number of applications for orders authorizing or approving the interception of wire, oral, or electronic communications pursuant to this chapter and the number of orders and extensions granted or denied pursuant to this chapter during the preceding calendar year. Such report shall include a summary and analysis of the data required to be filed with the Administrative Office by subsections (1) and (2) of this section. The Director of the Administrative Office of the United States Courts is authorized to issue binding regulations dealing with the content and form of the reports required to be filed by subsections (1) and (2) of this section.

18 U.S.C. 2520. Recovery of civil damages authorized

(a) In general. –Except as provided in section 2511(2)(a)(ii), any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter may in a civil action recover from the person or entity other than the United States which engaged in that violation such relief as may be appropriate.

(b) Relief. –In an action under this section, appropriate relief includes–
(1) such preliminary and other equitable or declaratory relief as may be appropriate;
(2) damages under subsection (c) and punitive damages in appropriate cases; and
(3) a reasonable attorney's fee and other litigation costs reasonably incurred.

(c) Computation of damages. –
(1) In an action under this section, if the conduct in violation of this chapter is the private viewing of a private satellite video communication that is not scrambled or encrypted or if the communication is a radio communication that is transmitted on frequencies allocated under subpart D of part 74 of the rules of the Federal Communications Commission that is not scrambled or encrypted and the conduct is not for a tortious or illegal purpose or for purposes of direct or

indirect commercial advantage or private commercial gain, then the court shall assess damages as follows:

(A) If the person who engaged in that conduct has not previously been enjoined under section 2511(5) and has not been found liable in a prior civil action under this section, the court shall assess the greater of the sum of actual damages suffered by the plaintiff, or statutory damages of not less than $50 and not more than $500.

(B) If, on one prior occasion, the person who engaged in that conduct has been enjoined under section 2511(5) or has been found liable in a civil action under this section, the court shall assess the greater of the sum of actual damages suffered by the plaintiff, or statutory damages of not less than $100 and not more than $1000.

(2) In any other action under this section, the court may assess as damages whichever is the greater of–

(A) the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation; or

(B) statutory damages of whichever is the greater of $100 a day for each day of violation or $10,000.

(d) Defense. –A good faith reliance on-

(1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization;

(2) a request of an investigative or law enforcement officer under section 2518(7) of this title; or

(3) a good faith determination that section 2511(3) or 2511(2)(i) of this title permitted the conduct complained of; is a complete defense against any civil or criminal action brought under this chapter or any other law.

(e) Limitation. –A civil action under this section may not be commenced later than two years after the date upon which the claimant first has a reasonable opportunity to discover the violation.

(f) Administrative Discipline. – If a court or appropriate department or agency determines that the United States or any of its departments or agencies has violated any provision of this chapter, and the court finds that the circumstances surrounding the violation raise serious questions about whether or not an officer or employee of the United States acted willfully or intentionally with respect to the possible violation, the department or agency shall, upon receipt of a true and correct copy of the decision and findings of the court or appropriate department or agency promptly initiate a proceeding to determine whether disciplinary action against the officer or employee is warranted. If the head of the department or agency involved determines that disciplinary action is not warranted, he or she shall notify the Inspector General with jurisdiction over the department or agency concerned and shall provide the Inspector General with the reasons for such determination.

(g) Improper Disclosure Is Violation. – Any willful disclosure or use by an investigative or law enforcement officer or governmental entity of information beyond the extent permitted by section 2517 is a violation of this chapter for purposes of section 2510(a).

18 U.S.C. 2521. Injunction against illegal interception

Whenever it shall appear that any person is engaged or is about to engage in any act which constitutes or will constitute a felony violation of this chapter, the Attorney General may initiate a civil action in a district court of the United States to enjoin such violation. The court shall proceed as soon as practicable to the hearing and determination of such an action, and may, at any time before final determination, enter such a restraining order or prohibition, or take such other action, as is warranted to prevent a continuing and substantial injury to the United States or to any person or class of persons for whose protection the action is brought. A proceeding under this section is governed by the Federal Rules of Civil Procedure, except that, if an indictment has been returned against the respondent, discovery is governed by the Federal Rules of Criminal Procedure.

18 U.S.C. 2522. Enforcement of the Communications Assistance for Law Enforcement Act

(a) Enforcement by court issuing surveillance order. –If a court authorizing an interception under this chapter, a State statute, or the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) or authorizing use of a pen register or a trap and trace device under chapter 206 or a State statute finds that a telecommunications carrier has failed to comply with the requirements of the Communications Assistance for Law Enforcement Act, the court may, in accordance with section 108 of such Act, direct that the carrier comply forthwith and may direct that a provider of support services to the carrier or the manufacturer of the carrier's transmission or switching equipment furnish forthwith modifications necessary for the carrier to comply.

(b) Enforcement upon application by Attorney General. –The Attorney General may, in a civil action in the appropriate United States district court, obtain an order, in accordance with section 108 of the Communications Assistance for Law Enforcement Act, directing that a telecommunications carrier, a manufacturer of telecommunications transmission or switching equipment, or a provider of telecommunications support services comply with such Act.

(c) Civil penalty. –

(1) In general. – A court issuing an order under this section against a telecommunications carrier, a manufacturer of telecommunications transmission or switching equipment, or a provider of telecommunications support services may impose a civil penalty of up to $10,000 per day for each day in violation after the issuance of the order or after such future date as the court may specify.

(2) Considerations.– In determining whether to impose a civil penalty and in determining its amount, the court shall take into account–

(A) the nature, circumstances, and extent of the violation;

(B) the violator's ability to pay, the violator's good faith efforts to comply in a timely manner, any effect on the violator's ability to continue to do business, the degree of culpability, and the length of any delay in undertaking efforts to comply; and (c) such other matters as justice may require.

(d) Definitions.– As used in this section, the terms defined in section 102 of the Communications Assistance for Law Enforcement Act have the meanings provided, respectively, in such section.

18 U.S.C. 2701. Unlawful access to stored communications

(a) Offense.–Except as provided in subsection (c) of this section whoever–

(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or

(2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.

(b) Punishment. –The punishment for an offense under subsection (a) of this section is–

(1) if the offense is committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain, or in furtherance of any criminal or tortious act in violation of the constitution and laws of the United States or any state –

(A) a fine under this title or imprisonment for not more than 5 years, or both, in the case of a first offense under this subparagraph; and

(B) a fine under this title or imprisonment for not more than 10 years, or both, for any subsequent offense under this subparagraph; and

(2)

(A) a fine under this title or imprisonment for not more than 1 year or both, in the case of a first offense under this paragraph; and

(B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under this subparagraph that occurs after a conviction of another offense under this section.

(c) Exceptions. –Subsection (a) of this section does not apply with respect to conduct authorized–

(1) by the person or entity providing a wire or electronic communications service;

(2) by a user of that service with respect to a communication of or intended for that user; or

(3) in section 2703, 2704 or 2518 of this title.

18 U.S.C. 2702. Voluntary disclosure of customer communications or records

(a) Prohibitions. –Except as provided in subsection (b) or (c) –

(1) a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; and

(2) a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service–

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service;

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing; and

(3) a provider of remote computing service or electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by paragraph (1) or (2)) to any governmental entity.

(b) Exceptions for disclosure of communications. – A provider described in subsection (a) may divulge the contents of a communication-

(1) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient;

(2) as otherwise authorized in section 2517, 2511(2)(a), or 2703 of this title;

(3) with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;

(4) to a person employed or authorized or whose facilities are used to forward such communication to its destination;

(5) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;

(6) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 227 of the Victims of Child Abuse Act of 1990 (42 U.S.C. 13032);

(7) to a law enforcement agency–

(A) if the contents–

(i) were inadvertently obtained by the service provider; and

(ii) appear to pertain to the commission of a crime; or [(B) Repealed. P.L. 108-21, Title V, § 508(b)(1)(A), Apr. 30, 2003, 117 Stat. 684] [(C) Repealed. P.L. 107-296, Title II, § 225(d)(1)(C), Nov. 25, 2002, 116 Stat. 2157]

(8) to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency.

(c) Exceptions for disclosure of customer records. –A provider described in subsection (a) may divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a)(1) or (a)(2)) –
(1)as otherwise authorized in section 2703;
(2) with the lawful consent of the customer or subscriber;
(3) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;
(4) to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency;
(5) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 227 of the Victims of Child Abuse Act of 1990 (42 U.S.C. 13032); or
(6) to any person other than a governmental entity.

(d) Reporting of emergency disclosures. –On an annual basis, the Attorney General shall submit to the Committee on the Judiciary of the House of Representatives and the Committee on the Judiciary of the Senate a report containing–
(1) the number of accounts from which the Department of Justice has received voluntary disclosures under subsection (b)(8); and
(2) a summary of the basis for disclosure in those instances where-–
(A) voluntary disclosures under subsection (b)(8) were made to the Department of Justice; and
(B) the investigation pertaining to those disclosures was closed without the filing of criminal charges.

18 U.S.C. 2703. Required disclosure of customer communications or records

(a) Contents of wire or electronic communications in electronic storage. –A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in a wire or electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section. (b)(1) Contents of electronic communications in a remote computing service. –
(1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection–

(A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant; or

(B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity–

(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or

(ii) obtains a court order for such disclosure under subsection (d) of this section; except that delayed notice may be given pursuant to section 2705 of this title.

(2) Paragraph (1) is applicable with respect to any wire or electronic communication that is held or maintained on that service–

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

(c) Records concerning electronic communication service or remote computing service. –

(1)

(A) A government entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications).

(B) A provider of electronic communication service or remote computing service shall disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a) or (b) of this section) to a governmental entity only when the governmental entity-

(A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant;

(B) obtains a court order for such disclosure under subsection (d) of this section;

(C) has the consent of the subscriber or customer to such disclosure; or

(D) submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud for the name, address, and place of business of a subscriber or customer of such provider, which subscriber or customer is engaged in telemarketing (as such term is defined in section 2325 of this title); or

(E) seeks information under paragraph (2).

(2) A provider of electronic communication service or remote computing service shall disclose to a governmental entity the (A) name; (B) address; (C) local and long distance telephone connection records, or records of session times and durations; (D) length of service (including start date) and types of service utilized; (E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and (F) means and source of payment (including any credit car or bank account number), of a subscriber to or customer of such service, when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under paragraph (1).
(3) A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer.

(d) Requirements for court order. –A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.

(e) No cause of action against a provider disclosing information under this chapter. –No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order, warrant, subpoena , statutory authorization, or certification under this chapter.

(f) Requirement to preserve evidence. –
(1) In general. – A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.
(2) Period of retention. – Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90-day period upon a renewed request by the governmental entity.

(g) Presence of Officer not Required. – Notwithstanding section 3105 of this title, the presence of an officer shall not be required for service or execution of a search warrant issued in accordance with this chapter requiring disclosure by a provider of electronic communications service or remote computing service of the contents

of communications or records or other information pertaining to a subscriber to or customer of such service.

18 U.S.C. 2704. Backup preservation

(a) Backup preservation. –

(1) A governmental entity acting under section 2703(b)(2) may include in its subpoena or court order a requirement that the service provider to whom the request is directed create a backup copy of the contents of the electronic communications sought in order to preserve those communications. Without notifying the subscriber or customer of such subpoena or court order, such service provider shall create such backup copy as soon as practicable consistent with its regular business practices and shall confirm to the governmental entity that such backup copy has been made. Such backup copy shall be created within two business days after receipt by the service provider of the subpoena or court order.

(2) Notice to the subscriber or customer shall be made by the governmental entity within three days after receipt of such confirmation, unless such notice is delayed pursuant to section 2705(a).

(3) The service provider shall not destroy such backup copy until the later of–

(A) the delivery of the information; or

(B) the resolution of any proceedings (including appeals of any proceeding) concerning the government's subpoena or court order.

(4) The service provider shall release such backup copy to the requesting governmental entity no sooner than fourteen days after the governmental entity's notice to the subscriber or customer if such service provider–

(A) has not received notice from the subscriber or customer that the subscriber or customer has challenged the governmental entity's request; and

(B) has not initiated proceedings to challenge the request of the governmental entity.

(5) A governmental entity may seek to require the creation of a backup copy under subsection (a)(1) of this section if in its sole discretion such entity determines that there is reason to believe that notification under section 2703 of this title of the existence of the subpoena or court order may result in destruction of or tampering with evidence. This determination is not subject to challenge by the subscriber or customer or service provider.

(b) Customer challenges. –

(1) Within fourteen days after notice by the governmental entity to the subscriber or customer under subsection (a)(2) of this section, such subscriber or customer may file a motion to quash such subpoena or vacate such court order, with copies served upon the governmental entity and with written notice of such challenge to the service provider. A motion to vacate a court order shall be filed in the court which issued such order. A motion to quash a subpoena shall be filed in the appropriate United States district court or State court. Such motion or application shall contain an affidavit or sworn statement-

(A) stating that the applicant is a customer or subscriber to the service from which the contents of electronic communications maintained for him have been sought; and

(B) stating the applicant's reasons for believing that the records sought are not relevant to a legitimate law enforcement inquiry or that there has not been substantial compliance with the provisions of this chapter in some other respect.

(2) Service shall be made under this section upon a governmental entity by delivering or mailing by registered or certified mail a copy of the papers to the person, office, or department specified in the notice which the customer has received pursuant to this chapter. For the purposes of this section, the term "delivery" has the meaning given that term in the Federal Rules of Civil Procedure.

(3) If the court finds that the customer has complied with paragraphs (1) and (2) of this subsection, the court shall order the governmental entity to file a sworn response, which may be filed in camera if the governmental entity includes in its response the reasons which make in camera review appropriate. If the court is unable to determine the motion or application on the basis of the parties' initial allegations and response, the court may conduct such additional proceedings as it deems appropriate. All such proceedings shall be completed and the motion or application decided as soon as practicable after the filing of the governmental entity's response.

(4) If the court finds that the applicant is not the subscriber or customer for whom the communications sought by the governmental entity are maintained, or that there is a reason to believe that the law enforcement inquiry is legitimate and that the communications sought are relevant to that inquiry, it shall deny the motion or application and order such process enforced. If the court finds that the applicant is the subscriber or customer for whom the communications sought by the governmental entity are maintained, and that there is not a reason to believe that the communications sought are relevant to a legitimate law enforcement inquiry, or that there has not been substantial compliance with the provisions of this chapter, it shall order the process quashed.

(5) A court order denying a motion or application under this section shall not be deemed a final order and no interlocutory appeal may be taken therefrom by the customer.

18 U.S.C. 2705. Delayed notice

(a) Delay of notification. –

(1) A governmental entity acting under section 2703(b) of this title may–

(A) where a court order is sought, include in the application a request, which the court shall grant, for an order delaying the notification required under section 2703(b) of this title for a period not to exceed ninety days, if the court determines that there is reason to believe that notification of the existence of the court order may have an adverse result described in paragraph (2) of this subsection; or

(B) where an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury subpoena is obtained, delay the notification required under section 2703(b) of this title for a period not to exceed ninety days

upon the execution of a written certification of a supervisory official that there is reason to believe that notification of the existence of the subpoena may have an adverse result described in paragraph (2) of this subsection.

(2) An adverse result for the purposes of paragraph (1) of this subsection is-

(A) endangering the life or physical safety of an individual;

(B) flight from prosecution;

(C) destruction of or tampering with evidence;

(D) intimidation of potential witnesses; or

(E) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

(3) The governmental entity shall maintain a true copy of certification under paragraph (1)(B).

(4) Extensions of the delay of notification provided in section 2703 of up to ninety days each may be granted by the court upon application, or by certification by a governmental entity, but only in accordance with subsection (b) of this section.

(5) Upon expiration of the period of delay of notification under paragraph (1) or (4) of this subsection, the governmental entity shall serve upon, or deliver by registered or first-class mail to, the customer or subscriber a copy of the process or request together with notice that-

(A) states with reasonable specificity the nature of the law enforcement inquiry; and

(B) informs such customer or subscriber--

(i) that information maintained for such customer or subscriber by the service provider named in such process or request was supplied to or requested by that governmental authority and the date on which the supplying or request took place;

(ii) that notification of such customer or subscriber was delayed;

(iii) what governmental entity or court made the certification or determination pursuant to which that delay was made; and

(iv) which provision of this chapter allowed such delay.

(6) As used in this subsection, the term "supervisory official" means the investigative agent in charge or assistant investigative agent in charge or an equivalent of an investigating agency's headquarters or regional office, or the chief prosecuting attorney or the first assistant prosecuting attorney or an equivalent of a prosecuting attorney's headquarters or regional office.

(b) Preclusion of notice to subject of governmental access. –

A governmental entity acting under section 2703, when it is not required to notify the subscriber or customer under section 2703(b)(1), or to the extent that it may delay such notice pursuant to subsection (a) of this section, may apply to a court for an order commanding a provider of electronic communications service or remote computing service to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order. The court shall enter such an order if it determines that there is reason to believe that notification of the existence of the warrant, subpoena, or court order will result in–

(1) endangering the life or physical safety of an individual;
(2) flight from prosecution;
(3) destruction of or tampering with evidence;
(4) intimidation of potential witnesses; or
(5) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

18 U.S.C. 2706. Cost reimbursement

(a) Payment. –Except as otherwise provided in subsection (c), a governmental entity obtaining the contents of communications, records, or other information under section 2702, 2703, or 2704 of this title shall pay to the person or entity assembling or providing such information a fee for reimbursement for such costs as are reasonably necessary and which have been directly incurred in searching for, assembling, reproducing, or otherwise providing such information. Such reimbursable costs shall include any costs due to necessary disruption of normal operations of any electronic communication service or remote computing service in which such information may be stored.

(b) Amount. –The amount of the fee provided by subsection (a) shall be as mutually agreed by the governmental entity and the person or entity providing the information, or, in the absence of agreement, shall be as determined by the court which issued the order for production of such information (or the court before which a criminal prosecution relating to such information would be brought, if no court order was issued for production of the information).

(c) Exception. –The requirement of subsection (a) of this section does not apply with respect to records or other information maintained by a communications common carrier that relate to telephone toll records and telephone listings obtained under section 2703 of this title. The court may, however, order a payment as described in subsection (a) if the court determines the information required is unusually voluminous in nature or otherwise caused an undue burden on the provider.

18 U.S.C. 2707. Civil action

(a) Cause of action. –Except as provided in section 2703(e), any provider of electronic communication service, subscriber, or other person aggrieved by any violation of this chapter in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind may, in a civil action, recover from the person or entity other than the United States which engaged in that violation such relief as may be appropriate.

(b) Relief. –In a civil action under this section, appropriate relief includes-
(1) such preliminary and other equitable or declaratory relief as may be appropriate;
(2) damages under subsection (c); and

(3) a reasonable attorney's fee and other litigation costs reasonably incurred.

(c) Damages. – The court may assess as damages in a civil action under this section the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation, but in no case shall a person entitled to recover receive less than the sum of $1,000. If the violation is willful or intentional, the court may assess punitive damages. In the case of a successful action to enforce liability under this section, the court may assess the costs of the action, together with reasonable attorney fees determined by the court.

(d) Administrative Discipline. – If a court or appropriate department or agency determines that the United States or any of its departments or agencies has violated any provision of this chapter, and the court or appropriate department or agency finds that the circumstances surrounding the violation raise serious questions about whether or not an officer or employee of the United States acted willfully or intentionally with respect to the possible violation, the department or agency shall, upon receipt of a true and correct copy of the decision and findings of the court or appropriate department or agency promptly initiate a proceeding to determine whether disciplinary action against the officer or employee is warranted. If the head of the department or agency involved determines that disciplinary action is not warranted, he or she shall notify the Inspector General with jurisdiction over the department or agency concerned and shall provide the Inspector General with the reasons for such determination.

(e) Defense. –A good faith reliance on–
(1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization (including a request of a governmental entity under section 2703(f) of this title);
(2) a request of an investigative or law enforcement officer under section 2518(7) of this title; or
(3) a good faith determination that section 2511(3) of this title permitted the conduct complained of; is a complete defense to any civil or criminal action brought under this chapter or any other law.

(f) Limitation. – A civil action under this section may not be commenced later than two years after the date upon which the claimant first discovered or had a reasonable opportunity to discover the violation.

(g) Improper Disclosure Is Violation. – Any willful disclosure of a "record", as that term is defined in section 552a(a) of title 5, United States Code, obtained by an investigative or law enforcement officer, or governmental entity, pursuant to section 2703 of this title, or from a device installed pursuant to section 3123 or 3125 of this title, that is not a disclosure made in the proper performance of the official duties of the officer or governmental entity making the disclosure, is a violation of this chapter. This provision shall not apply to information previously lawfully disclosed (prior to the commencement of any civil or administrative

proceeding under this chapter) to the public by a Federal, State, or local governmental entity or by the plaintiff in a civil action under this chapter.

18 U.S.C. 2708. Exclusivity of remedies

The remedies and sanctions described in this chapter are the only judicial remedies and sanctions for nonconstitutional violations of this chapter.

18 U.S.C. 2709. Counterintelligence access to telephone toll and transactional records

(a) Duty to provide–A wire or electronic communication service provider shall comply with a request for subscriber information and toll billing records information, or electronic communication transactional records in its custody or possession made by the Director of the Federal Bureau of Investigation under subsection (b) of this section.

(b) Required certification–The Director of the Federal Bureau of Investigation, or his designee in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge in a Bureau field office designated by the Director, may–

(1) request the name, address, length of service, and local and long distance toll billing records of a person or entity if the Director (or his designee) certifies in writing to the wire or electronic communication service provider to which the request is made that the name, address, length of service, and toll billing records sought are relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment to the Constitution of the United States; and

(2) request the name, address, and length of service of a person or entity if the Director (or his designee) certifies in writing to the wire or electronic communication service provider to which the request is made that the information sought is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution of the United States.

(c) Prohibition of certain disclosure–

(1) If the Director of the Federal Bureau of Investigation, or his designee in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge in a Bureau field office designated by the Director, certifies that otherwise there may result a danger to the national security of the United States, interference with a criminal, counter terrorism, or counterintelligence investigation, interference with diplomatic relations, or danger to the life or physical safety of any person, no wire or electronic communications service provider, or officer, employee, or agent thereof, shall

disclose to any person (other than those to whom such disclosure is necessary to comply with the request or an attorney to obtain legal advice or legal assistance with respect to the request) that the Federal Bureau of Investigation has sought or obtained access to information or records under this section.
(2) The request shall notify the person or entity to whom the request is directed of the nondisclosure requirement under paragraph (1).
(3) Any recipient disclosing to those persons necessary to comply with the request or to an attorney to obtain legal advice or legal assistance with respect to the request shall inform such person of any applicable nondisclosure requirement. Any person who receives a disclosure under this subsection shall be subject to the same prohibitions on disclosure under paragraph (1).
(4) At the request of the Director of the Federal Bureau of Investigation or the designee of the Director, any person making or intending to make a disclosure under this section shall identify to the Director or such designee the person to whom such disclosure will be made or to whom such disclosure was made prior to the request, except that nothing in this section shall require a person to inform the Director or such designee of the identity of an attorney to whom disclosure was made or will be made to obtain legal advice or legal assistance with respect to the request under subsection (a).

(d) Dissemination by bureau–The Federal Bureau of Investigation may disseminate information and records obtained under this section only as provided in guidelines approved by the Attorney General for foreign intelligence collection and foreign counterintelligence investigations conducted by the Federal Bureau of Investigation, and, with respect to dissemination to an agency of the United States, only if such information is clearly relevant to the authorized responsibilities of such agency.

(e) Requirement that certain congressional bodies be informed–On a semiannual basis the Director of the Federal Bureau of Investigation shall fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate, and the Committee on the Judiciary of the House of Representatives and the Committee on the Judiciary of the Senate, concerning all requests made under subsection (b) of this section.

(f) Libraries–A library (as that term is defined in section 213(1) of the Library Services and Technology Act (20 U.S.C. 9122(1)), the services of which include access to the Internet, books, journals, magazines, newspapers, or other similar forms of communication in print or digitally by patrons for their use, review, examination, or circulation, is not a wire or electronic communication service provider for purposes of this section, unless the library is providing the services defined in section 2510(15) (“electronic communication service”) of this title.

18 U.S.C. 2711. Definitions for chapter

As used in this chapter–

- the terms defined in section 2510 of this title have, respectively, the definitions given such terms in that section;
- • the term "remote computing service" means the provision to the public of computer storage or processing services by means of an electronic communications system;
- the term "court of competent jurisdiction" has the meaning assigned by section 3127, and includes any Federal court within that definition, without geographic limitation.
- the term "governmental entity" means a department or agency of the United States or State or political subdivision thereof.

18 U.S.C. 2712. Civil Action against the United States

(a) In General.– Any person who is aggrieved by any willful violation of this chapter or of chapter 119 of this title or of sections 106(a), 305(a), or 405(a) of the Foreign Intelligence Surveillance Act (50 U.S.C. 1801 et seq.) may commence an action in United States District Court against the United States to recover money damages. In any such action, if a person who is aggrieved successfully establishes a violation of this chapter or of chapter 119 of this title or of the above special provisions of title 50, the Court may assess as damages–

(1) actual damages, but not less than $10,000, whichever amount is greater; and
(2) litigation costs, reasonably incurred.

(b) Procedures. –
(1) Any action against the United States under this section may be commenced only after a claim is presented to the appropriate department or agency under the procedures of the Federal Tort Claims Act, as set forth in title 28, United States Code.
(2) Any action against the United States under this section shall be forever barred unless it is presented in writing to the appropriate Federal agency within 2 years after such claim accrues or unless action is begun within 6 months after the date of mailing, by certified or registered mail, of notice of final denial of the claim by the agency to which it was presented. The claim shall accrue on the date upon which the claimant first has a reasonable opportunity to discover the violation.
(3) Any action under this section shall be tried in the court without a jury.
(4) Notwithstanding any other provision of law, the procedures set forth in section 106(f), 305(g), or 405(f) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) shall be the exclusive means by which materials governed by those sections may be reviewed.
(5) An amount equal to any award against the United States under this section shall be reimbursed by the department or agency concerned to the fund described in section 1304 of title 31, United States Code, out of any appropriation, fund, or other account (excluding any part of such appropriation, fund, or account that is

available for the enforcement of any Federal law) that is available for the operating expenses of the department or agency concerned.

(c) Administrative Discipline. –
If a court or appropriate department or agency determines that the United States or any of the departments or agencies has violated any provision of this chapter, and the court or appropriate department or agency finds that the circumstances surrounding the violation raise serious questions about whether or not an officer or employee of the United States acted willfully or intentionally with respect to the possible violation, the department or agency shall, upon receipt of a true and correct copy of the decision and findings of the court or appropriate department or agency promptly initiate a proceeding to determine whether disciplinary action against the officer or employee is warranted. If the head of the department or agency involved determines that disciplinary action is not warranted, he or she shall notify the Inspector General with jurisdiction over the department or agency concerned and shall provide the Inspector General with the reasons for such determination.

(d) Exclusive Remedy. –
Any action against the United States under this subsection shall be the exclusive remedy against the United States for any claims within the purview of this section.

(e) Stay of Proceedings. –
(1) Upon the motion of the united States, the curt shall stay any action commenced under this section f the court determines that civil discovery will adversely affect the ability of the Government to conduct a related investigation or the prosecution of a related criminal case. Such a stay shall toll the limitations periods of paragraph (2) of subsection (b).
(2) In this subsection, the terms "related criminal case" and "related investigation" means an actual prosecution or investigation in progress at the time at which the request for the stay or any subsequent motion to lift the stay is made. In determining whether any investigation or a criminal case is related to an action commenced under this section, the court shall consider the degree of similarity between the parties, witnesses, facts, and circumstances involved in the 2 proceedings, without requiring that nay one or more factors be identical.
(3) In requesting a stay under paragraph (1), the Government may, in appropriate cases submit evidence ex parte in order to avoid disclosing any matter that may adversely affect a related investigation or a related criminal case. If the Government makes such an ex parte submission, the plaintiff shall be given an opportunity to make a submission to the court, not ex parte, and the court may, in its discretion, request further information from either party.

18 U.S.C. 3121. General prohibition on pen register and tape and trace device use; exception

(a) In general–Except as provided in this section, no person may install or use a pen register or a trap and trace device without first obtaining a court order under section 3123 of this title or under the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.).

(b) Exception–The prohibition of subsection (a) does not apply with respect to the use of a pen register or a trap and trace device by a provider of electronic or wire communication service–
(1) relating to the operation, maintenance, and testing of a wire or electronic communication service or to the protection of the rights or property of such provider, or to the protection of users of that service from abuse of service or unlawful use of service; or
(2) to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire communication, or a user of that service, from fraudulent, unlawful or abusive use of service; or
(3) where the consent of the user of that service has been obtained.

(c) Limitation–A government agency authorized to install and use a pen register or trap and trace device under this chapter or under State law shall use technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to the dialing, routing, addressing, and signaling information utilized in identifying the origination or destination of wire or electronic communications.

(d) Penalty–Whoever knowingly violates subsection (a) shall be fined under this title or imprisoned not more than one year, or both.

18 U.S.C. 3122. Application for an order for a pen register or a trap and trace device

(a) Application.
(1) An attorney for the Government may make application for an order or an extension of an order under section 3123 of this title authorizing or approving the installation and use of a pen register or a trap and trace device under this chapter, in writing under oath or equivalent affirmation, to a court of competent jurisdiction.
(2) Unless prohibited by State law, a State investigative or law enforcement officer may make application for an order or an extension of an order under section 3123 of this title authorizing or approving the installation and use of a pen register or a trap and trace device under this chapter, in writing under oath or equivalent affirmation, to a court of competent jurisdiction of such State.

(b) Contents of application–An application under subsection (a) of this section shall include-

(1) the identity of the attorney for the Government or the State law enforcement or investigative officer making the application and the identity of the law enforcement agency conducting the investigation; and
(2) a certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency.

18 U.S.C. 3123. Issuance of an order for a pen register or a trap and trace device

(a) In general.
(1) Upon an application made under section 3122(a)(1) of this title, the court shall enter an ex parte order authorizing the installation and use of a pen register or a trap and trace device if the court finds, based on facts contained in the application, that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation. Such order shall, upon service of such order, apply to any entity providing wire or electronic communication service in the United States whose assistance may facilitate the execution of the order.
(2) Upon an application made under section 3122(a)(2) of this title, the court shall enter an ex parte order authorizing the installation and use of a pen register or a trap and trace device within the jurisdiction of the court if the court finds, based on facts contained in the application, that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation.
(3)
(A) Where the law enforcement agency implementing an ex part order under this subsection seeks to do so by installing and using its own pen register or trap and trace device on a packet-switched data network of a provider of electronic communication service to the public the agency shall ensure that a record will be maintained which will identify –

- any officer or officers who installed the device and any officer or officers who accessed the device to obtain information from the network;
- the date and time the device was installed, the date and time the device was uninstalled, and the date, time, and duration of each time the device is accessed to obtain information;

(iii) the configuration of the device at the time of its installation and any subsequent modification thereof; and
(iv) any information which has been collected by the device. To the extent that the pen register or trap and trace device can be set automatically to record this information electronically, the record shall be maintained electronically throughout the installation and use of the such device.
(B) The record maintained under subparagraph (A) shall be provided ex parte and under seal to the court which entered the ex parte order authorizing the installation and use of the device within 30 days after termination of the order (including any extensions thereof).

(b) Contents of order–An order issued under this section–
(1) shall specify–
(A) the identity, if known, of the person to whom is leased or in whose name is listed the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied;
(B) the identity, if known, of the person who is the subject of the criminal investigation;
(C) the attributes of the communications to which the order applies, including the number or other identifier and, if known, the location of the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied, and, in the case of an order authorizing installation and use of a trap and trace device under subsection (a)(2), the geographic limits of the order; and
(D) a statement of the offense to which the information likely to be obtained by the pen register or trap and trace device relates; and
(2) shall direct, upon the request of the applicant, the furnishing of information, facilities, and technical assistance necessary to accomplish the installation of the pen register or trap and trace device under section 3124 of this title.

(c) Time period and extensions–
(1) An order issued under this section shall authorize the installation and use of a pen register or a trap and trace device for a period not to exceed sixty days.
(2) Extensions of such an order may be granted, but only upon an application for an order under section 3122 of this title and upon the judicial finding required by subsection (a) of this section. The period of extension shall be for a period not to exceed sixty days.

(d) Nondisclosure of existence of pen register or a trap and trace device
An order authorizing or approving the installation and use of a pen register or a trap and trace device shall direct that-
(1) the order be sealed until otherwise ordered by the court; and
(2) the person owning or leasing the line or other facility to which the pen register or a trap and trace device is attached, or applied, or who is obligated by the order to provide assistance to the applicant, not disclose the existence of the pen register or trap and trace device or the existence of the investigation to the listed subscriber, or to any other person, unless or until otherwise ordered by the court.

18 U.S.C. 3124. Assistance in installation and use of a pen register or a trap and trace device

(a) Pen registers–Upon the request of an attorney for the Government or an officer of a law enforcement agency authorized to install and use a pen register under this chapter, a provider of wire or electronic communication service, landlord, custodian, or other person shall furnish such investigative or law enforcement officer forthwith all information, facilities, and technical assistance necessary to accomplish the installation of the pen register unobtrusively and with a minimum of interference with the services that the person so ordered by

the court accords the party with respect to whom the installation and use is to take place, if such assistance is directed by a court order as provided in section 3123(b)(2) of this title.

(b) Trap and trace device–Upon the request of an attorney for the Government or an officer of a law enforcement agency authorized to receive the results of a trap and trace device under this chapter, a provider of a wire or electronic communication service, landlord, custodian, or other person shall install such device forthwith on the appropriate line or other facility and shall furnish such investigative or law enforcement officer all additional information, facilities and technical assistance including installation and operation of the device unobtrusively and with a minimum of interference with the services that the person so ordered by the court accords the party with respect to whom the installation and use is to take place, if such installation and assistance is directed by a court order as provided in section 3123(b)(2) of this title. Unless otherwise ordered by the court, the results of the trap and trace device shall be furnished, pursuant to section 3123(b) or section 3125 of this title, to the officer of a law enforcement agency, designated in the court order, at reasonable intervals during regular business hours for the duration of the order.

(c) Compensation–A provider of a wire or electronic communication service, landlord, custodian, or other person who furnishes facilities or technical assistance pursuant to this section shall be reasonably compensated for such reasonable expenses incurred in providing such facilities and assistance.

(d) No cause of action against a provider disclosing information under this chapter–No cause of action shall lie in any court against any provider of a wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with a court order under this chapter or request pursuant to section 3125 of this title.

(e) Defense–A good faith reliance on a court order under this chapter, a request pursuant to section 3125 of this title, a legislative authorization, or a statutory authorization is a complete defense against any civil or criminal action brought under this chapter or any other law.

(f) Communications assistance enforcement orders–Pursuant to section 2522, an order may be issued to enforce the assistance capability and capacity requirements under the Communications Assistance for Law Enforcement Act.

18 U.S.C. 3125. Emergency pen register and trap and trace device installation

(a) Notwithstanding any other provision of this chapter, any investigative or law enforcement officer, specially designated by the Attorney General, the Deputy Attorney General, the Associate Attorney General, any Assistant Attorney

General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General, or by the principal prosecuting attorney of any State or subdivision thereof acting pursuant to a statute of that State, who reasonably determines that-

(1) an emergency situation exists that involves–

(A) immediate danger of death or serious bodily injury to any person; or

(B) conspiratorial activities characteristic of organized crime;

(C) an immediate threat to a national security interest; or

(D) an ongoing attack on a protected computer (as defined in section 1030) that constitutes a crime punishable by a term of imprisonment greater than one year; that requires the installation and use of a pen register or a trap and trace device before an order authorizing such installation and use can, with due diligence, be obtained, and

(2) there are grounds upon which an order could be entered under this chapter to authorize such installation and use; may have installed and use a pen register or trap and trace device if, within forty-eight hours after the installation has occurred, or begins to occur, an order approving the installation or use is issued in accordance with section 3123 of this title.

(b) In the absence of an authorizing order, such use shall immediately terminate when the information sought is obtained, when the application for the order is denied or when forty-eight hours have lapsed since the installation of the pen register or trap and trace device, whichever is earlier.

(c) The knowing installation or use by any investigative or law enforcement officer of a pen register or trap and trace device pursuant to subsection (a) without application for the authorizing order within forty-eight hours of the installation shall constitute a violation of this chapter.

(d) A provider of a wire or electronic service, landlord, custodian, or other person who furnished facilities or technical assistance pursuant to this section shall be reasonably compensated for such reasonable expenses incurred in providing such facilities and assistance.

18 U.S.C. 3126. Reports concerning pen registers and trap and trace devices

The Attorney General shall annually report to Congress on the number of pen register orders and orders for trap and trace devices applied for by law enforcement agencies of the Department of Justice, which report shall include information concerning–

- the period of interceptions authorized by the order, and the number and duration of any extensions of the order;
- the offense specified in the order or application, or extension of an order;
- the number of investigations involved;
- the number and nature of the facilities affected; and

- the identity, including district, of the applying investigative or law enforcement agency making the application and the person authorizing the order.

18 U.S.C. 3127. Definitions for chapter

As used in this chapter–

- the terms “wire communication”, “electronic communication”, “electronic communication service” and “contents” have the meanings set forth for such terms in section 2510 of this title;
- the term “court of competent jurisdiction” means–
- any district court of the United States (including a magistrate of such a court) or a United States Court of Appeals having jurisdiction over the offense being investigated; or
- a court of general criminal jurisdiction of a State authorized by the law of that State to enter orders authorizing the use of a pen register or a trap and trace device;
- the term “pen register” means a device or process which records or decodes or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication, but such term does not include any device or process used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device or process used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business;
- the term “trap and trace device” means a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication;
- the term “attorney for the Government” has the meaning given such term for the purposes of the Federal Rules of Criminal Procedure; and
- the term “State” means a State, the District of Columbia, Puerto Rico, and any other possession or territory of the United States.

Foreign Intelligence Surveillance Act (FISA) (OMITTED)

[**INTELLIGENCELAW.COM EDITOR'S NOTE:** FISA is discussed thoroughly in the materials for Title 50 of the U.S. Code so it has been excluded from Title 18 materials]

18 U.S.C. CHAPTER 121: STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS (18 U.S.C. §§ 2701-2712)

National Security Letters

National Security Letters in Foreign Intelligence Investigations: A Glimpse of the Legal Background and Recent Amendments, RS22406 (September 8, 2009)

CHARLES DOYLE, CONGRESSIONAL RESEARCH SERV., NATIONAL SECURITY LETTERS IN FOREIGN INTELLIGENCE INVESTIGATIONS: A GLIMPSE OF THE LEGAL BACKGROUND AND RECENT AMENDMENTS (2009), , *available at* http://www.intelligencelaw.com/library/secondary/crs/pdf/RS22406_9-8-2009.pdf.

Charles Doyle

Senior Specialist in American Public Law

September 8, 2009

Congressional Research Service

7-5700
www.crs.gov
RS22406

Summary

Five statutory provisions vest government agencies responsible for certain foreign intelligence investigations (principally the Federal Bureau of Investigation [FBI]) with authority to issue written commands comparable to administrative subpoenas. These National Security Letters (NSLs) seek customer and consumer transaction information in national security investigations from communications providers, financial institutions, and credit agencies.

The USA PATRIOT Act expanded the circumstances under which an NSL could be used. Subsequent press accounts suggested that their use had become widespread. Two lower federal courts found the uncertainties, practices, and policies associated with the use of NSL authority contrary to the First Amendment right of freedom of speech. The USA PATRIOT Improvement and Reauthorization Act, P.L. 109-177, and P.L. 109-178, amend the NSL statutes and related law to address some of the concerns raised by critics and the courts. Following amendment, an appellate court dismissed one of the earlier cases as moot and remanded the second for reconsideration in light of the amendments. On remand, the lower federal court again held the NSLs constitutionally suspect. The Court of Appeals, however, ruled that the amended statutes could withstand constitutional scrutiny, if the government confines itself to a procedure which requires (1) notice to the recipient of its option to object to a secrecy requirement; (2) upon recipient objection, prompt judicial review at the government's petition and burden; and (3) meaningful judicial review without conclusive weight afforded a government certification of risk. Using this procedure, the district upheld continuation of the Doe nondisclosure requirement following an ex parte, in camera hearing and granted the plaintiff's motion for an unclassified, redacted summary of the government declaration on which the court's decision was based.

A report of the Department of Justice's Inspector General found that in its early use of its expanded USA PATRIOT Act authority the FBI had "used NSLs in violation of applicable NSL statutes, Attorney General Guidelines, and internal FBI policies," but that no criminal laws had been broken. A year later, a second IG report confirmed the findings of the first, and noted the corrective measures taken in response.

This is an abridged version of CRS Report RL33320, National Security Letters in Foreign Intelligence Investigations: Legal Background and Recent Amendments, without the footnotes, appendices, and most of the citations to authority found in the longer report.

Background

The ancestor of the first NSL letter provision is an exception to privacy protections afforded by the Right to Financial Privacy Act (RFPA). Its history is not particularly instructive and consists primarily of a determination that the exception in its original form should not be too broadly construed. But the exception was just that, an exception. It was neither an affirmative grant of authority to request information nor a command to financial institutions to provide information when asked. It removed the restrictions on the release of customer information imposed on financial institutions by the RFPA, but it left them free to decline to comply when asked to do so.

> *[I]n certain significant instances, financial institutions [had] declined to grant the FBI access to financial records in response to*

> *requests under Section 1114(a). The FBI informed the Committee that the problem occurs particularly in States which have State constitutional privacy protection provisions or State banking privacy laws. In those States, financial institutions decline to grant the FBI access because State law prohibits them from granting such access and the RFPA, since it permits but does not mandate such access, does not override State law. In such a situation, the concerned financial institutions which might otherwise desire to grant the FBI access to a customer's record will not do so, because State law does not allow such cooperation, and cooperation might expose them to liability to the customer whose records the FBI sought access. (H.Rept. 99-690, at 15-6 [1986].)*

Congress responded with passage of the first NSL statute as an amendment to the RFPA, affirmatively giving the FBI access to financial institution records in certain foreign intelligence cases. At the same time, in the Electronic Communications Privacy Act, it afforded the FBI comparable access to telephone company and other communications service provider customer information. Together, the two NSL provisions afforded the FBI access to communications and financial business records under limited circumstances—customer and customer transaction information held by telephone carriers and banks pertaining to a foreign power or its agents relevant to a foreign counterintelligence investigation. Both the communications provider section and the RFPA section contained nondisclosure provisions and limitations on further dissemination, except pursuant to guidelines promulgated by the Attorney General. Neither had an express enforcement mechanism nor identified penalties for failure to comply with either the NSL or the nondisclosure instruction.

In the mid-1990s, Congress added two more NSL provisions—one permits NSL use in connection with the investigation of government employee leaks of classified information under the National Security Act; the other grants the FBI access to credit agency records pursuant to the Fair Credit Reporting Act, under much the same conditions as apply to the records of financial institutions. The FBI asked for the Fair Credit Reporting Act amendment as a threshold mechanism to enable it to make more effective use of its bank record access authority:

> *FBI's right of access under the Right of Financial Privacy Act cannot be effectively used, however, until theFBI discovers which financial institutions arebeing utilized by the subject of a counterintelligence investigation. Consumer reports maintained by credit bureaus are a ready source of such information, but, although such report[s] are readily available to the private sector, they are not available to FBI counterintelligence investigators....*
>
> *FBI has made a specific showing ... that the effort to identify financial institutions in order to make use of FBI authority under*

> *the Right to Financial Privacy Act can not only be time-consuming and resource-intensive, but can also require the use of investigative techniques— such as physical and electronic surveillance, review of mail covers, and canvassing of all banks in an area—that would appear to be more intrusive than the review of credit reports. (H.Rept. 104-427, at 36 [1996].)*

The National Security Act NSL provision authorizes access to credit and financial institution records of federal employees with security clearances who were required to give their consent as a condition for clearance. Passed in the wake of the Ames espionage case, it is limited to investigations of classified information leaks.

Both the Fair Credit Reporting Act section and the National Security Act section contain dissemination restrictions, as well as safe harbor (immunity) and nondisclosure provisions. Neither has an explicit penalty for improper disclosure of the request, but the Fair Credit Reporting Act section expressly authorizes judicial enforcement.

The USA PATRIOT Act amended three of the four existing NSL statutes and added a fifth. In each of the three NSL statutes available exclusively to the FBI—the Electronic Communications Privacy Act section, the Right to Financial Privacy Act section, and the Fair Credit Reporting Act section—section 505 of the USA PATRIOT Act:

- expanded FBI issuing authority beyond FBI headquarter officials to include the heads of the FBI field offices (i.e., Special Agents in Charge [SACs]);
- eliminated the requirement that the record information sought pertain to a foreign power or the agent of a foreign power;
- required instead that the NSL request be relevant to an investigation to protect against international terrorism or foreign spying; and
- added the caveat that no such investigation of an American can be predicated exclusively on First Amendment-protected activities.

The amendments allowed NSL authority to be employed more quickly (without the delays associated with prior approval from FBI headquarters) and more widely (without requiring that the information pertain to a foreign power or its agents).

Subsection 358(g) of the USA PATRIOT Act amended the Fair Credit Reporting Act to add a fifth and final NSL section, and the provision had one particularly noteworthy feature: it was available not merely to the FBI but to any government agency investigating or analyzing international terrorism:

> *Notwithstanding section 1681b of this title or any other provision of this subchapter, a consumer reporting agency shall furnish a*

> *consumer report of a consumer and all other information in a consumer's file to a government agency authorized to conduct investigations of, or intelligence or counterintelligence activities or analysis related to, international terrorism when presented with a written certification by such government agency that such information is necessary for the agency's conduct or such investigation, activity or analysis.*

Although the subsection's legislative history treats it as a matter of first impression, Congress's obvious intent was to provide other agencies with the national security letter authority comparable to that enjoyed by the FBI under the Fair Credit Reporting Act. The new section had a nondisclosure and a safe harbor subsection, but no express means of judicial enforcement or penalties for improper disclosure of a request under the section.

NSL Amendments in the 109th Congress

Both USA PATRIOT Act reauthorization statutes—P.L. 109-177(H.R. 3199) and P.L. 109-178 (S. 2271)—amended the NSL statutes. They provided for judicial enforcement of the letter requests and for judicial review of both the requests and accompanying nondisclosure requirements. They established specific penalties for failure to comply or to observe the nondisclosure requirements. They made it clear that the nondisclosure requirements do not preclude a recipient from consulting an attorney. They provided a mechanism to lift the nondisclosure requirement. Finally, they expanded congressional oversight and called for an Inspector General's audit of use of the authority.

Inspector General's Reports

The USA PATRIOT Improvement and Reauthorization Act instructed the Department of Justice's Inspector General to review and report on the FBI's use of NSLs. In early March 2007, the Inspector General released the first of two required reports that covered calendar years 2003 through 2005. The second, covering the time period through the end of calendar year 2006, was released in March 2008.

The initial report noted that FBI use of NSLs had increased dramatically, expanding from 8,500 requests in 2000 to 47,000 in 2005. Seventy-four percent were issued in conjunction with counterterrorism investigations, most of the rest in connection with counterintelligence investigations, and less than 1 percent as part of a foreign computer intrusion investigation. During the three years under review, the percentage of NSLs used to investigate Americans ("U.S. persons") increased from 39% in 2003 to 53% in 2005. A substantial majority of the requests involve records relating to telephone or e-mail communications. The report is somewhat critical of the FBI's initial performance:

> *[W]e found that the FBI used NSLs in violation of applicable NSL statutes, Attorney General Guidelines, and internal FBI policies. In addition, we found that the FBI circumvented the requirements of the ECPA NSL statute when it issued at least 739 "exigent letters" to obtain telephone toll billing records and subscriber information from three telephone companies without first issuing NSLs.*

The second IG Report reviewed the FBI's use of national security letter authority during calendar year 2006 and the corrective measures taken following the issuance of the IG's first report. The second Report concluded that the FBI's use of national security letters in 2006 continued the upward trend previously identified; the percentage of NSL requests generated from investigations of U.S. persons increased from 39% of all NSL requests in 2003 to 57% in 2006; the FBI and DoJ are committed to correcting the problems identified in IG Report I and have made significant progress; and it is too early to say whether the corrective measures will resolve the problems previously identified.

NSLs in Court

Prior to amendment, two lower federal court cases had indicated that the NSLs and practices surrounding their use were contrary to the requirements of the First Amendment. On appeal, one was dismissed as moot and the other sent back for reconsideration in light of the amendments. Following remand and amendment of the NSL statutes, the District Court for the Southern District of New York again concluded that the amended NSL secrecy requirements violated both First Amendment free speech.

The Court of Appeals was similarly disposed, but concluded that the government could invoke the secrecy and judicial review authority of the 18 U.S.C. 2709 and 18 U.S.C. 3511 in a limited, but constitutionally permissible manner. It stated that:

> *If the Government uses the suggested reciprocal notice procedure as a means of initiating judicial review, there appears to be no impediment to the Government's including notice of a recipient's opportunity to contest the nondisclosure requirement in an NSL. If such notice is given, time limits on the nondisclosure requirement pending judicial review, as reflected in Freedman, would have to be applied to make the review procedure constitutional. We would deem it to be within our judicial authority to conform subsection 2709(c) to First Amendment requirements, by limiting the duration of the nondisclosure requirement, absent a ruling favorable to the Government upon judicial review, to the 10-day period in which the NSL recipient decides whether to contest the nondisclosure requirement, the 30-day period in which the Government considers whether to seek judicial review, and a further period of 60 days in which a court must adjudicate the*

> *merits, unless special circumstances warrant additional time. If the NSL recipient declines timely to precipitate Government-initiated judicial review, the nondisclosure requirement would continue, subject to the recipient's existing opportunities for annual challenges to the nondisclosure requirement provided by subsection 3511(b). If such an annual challenge is made, the standards and burden of proof that we have specified for an initial challenge would apply, although the Government would not be obliged to initiate judicial review.*

Given the possibility of constitutional application, the court saw no reason to invalidate sections 2709(c) and 3511(b) in toto. The exclusive presumptions of section 3511 cannot survive, the court declared, but the First Amendment finds no offense in the remainder of the two sections except, the court observed, "to the extent that they fail to provide for Government-initiated judicial review. The Government can respond to this partial invalidation ruling by using the suggested reciprocal notice procedure."

On remand under the procedure suggested by the Court of Appeals, the government submitted the declaration of the senior FBI official concerning the continued need for secrecy concerning the NSL. Following an ex parte, in camera hearing, the district court concluded the government had met its burden, but granted the plaintiff's motion for a unclassified, redacted summary of the FBI declaration.

Author Contact Information

Charles Doyle
Senior Specialist in American Public Law
cdoyle@crs.loc.gov, 7-6968

National Security Letters in Foreign Intelligence Investigations: Legal Background and Recent Amendments, RL33320 (September 8, 2009).

CHARLES DOYLE, CONGRESSIONAL RESEARCH SERV., NATIONAL SECURITY LETTERS IN FOREIGN INTELLIGENCE INVESTIGATIONS: LEGAL BACKGROUND AND RECENT AMENDMENTS (2009), , *available at* http://www.intelligencelaw.com/library/secondary/crs/pdf/RL33320_9-8-2009.pdf.

Charles Doyle
Senior Specialist in American Public Law

September 8, 2009

7-5700
www.crs.gov
RL33320

Summary

Five federal statutes authorize intelligence officials to request certain business record information in connection with national security investigations. The authority to issue these national security letters (NSLs) is comparable to the authority to issue administrative subpoenas. The USA PATRIOT Act expanded the authority under four of the NSL statutes and created the fifth. Thereafter, the authority has been reported to have been widely used. Prospects of its continued use dimmed, however, after two lower federal courts held the lack of judicial review and the absolute confidentiality requirements in one of the statutes rendered it constitutionally suspect.

A report by the Department of Justice's Inspector General (IG) found that in its pre-amendment use of expanded USA PATRIOT Act authority the FBI had "used NSLs in violation of applicable NSL statutes, Attorney General Guidelines, and internal FBI policies," but that no criminal laws had been broken. A year later, a second IG report confirmed the findings of the first, and noted the corrective measures taken in response.

The USA PATRIOT Improvement and Reauthorization Act (H.R. 3199), P.L. 109-177, and its companion P.L. 109-178, amended the five NSL sections to expressly provide for judicial review of both the NSLs and the confidentiality requirements that attend them. The sections have also been made explicitly judicially enforceable and sanctions recognized for failure to comply with an NSL request or to breach NSL confidentiality requirements with the intent to obstruct justice. The use of the authority has been made subject to greater congressional

oversight. Following amendment, an appellate court dismissed one of the earlier cases as moot and remanded the second for reconsideration in light of the amendments. On remand, the lower court found the amended procedure contrary to the demands of the First Amendment. The Court of Appeals, however, ruled that the amended statutes could withstand constitutional scrutiny, if the government confined itself to a procedure which requires (1) notice to the recipient of its option to object to a secrecy requirement; (2) upon recipient objection, prompt judicial review at the government's petition and burden; and (3) meaningful judicial review without conclusive weight afforded a government certification of risk. Using this procedure, the district court upheld continuation of the Doe nondisclosure requirement following an ex parte, in camera hearing and granted the plaintiff's motion for an unclassified, redacted summary of the government declaration on which the court's decision was based.

The text of the five provisions—section 1114(a)(5) of the Right to Financial Privacy Act (12 U.S.C. 3414(a)(5)); sections 626 and 627 of the Fair Credit Reporting Act (15 U.S.C. 1681u, 1681v); section 2709 of title 18 of the United States Code; and section 802 of the National Security Act (50 U.S.C. 436)—in their amended form have been appended. This report is available abridged—without footnotes, appendices, and most of the citations to authority—as CRS Report RS22406, National Security Letters in Foreign Intelligence Investigations: A Glimpse of the Legal Background and Recent Amendments, by Charles Doyle.

Introduction

Five statutory provisions vest government agencies responsible for certain foreign intelligence investigations (principally the Federal Bureau of Investigation (FBI)) with authority to issue written commands comparable to administrative subpoenas.[2658] A National Security Letter (NSL) seeks customer and consumer transaction information in national security investigations from communications providers, financial institutions and credit agencies. Section 505 of the USA PATRIOT Act expanded the circumstances under which an NSL could be used.[2659] Subsequent press accounts suggested that their use had become wide-spread.[2660] Two lower federal courts, however, found the uncertainties,

---

[2658] 18 U.S.C. 2709; 12 U.S.C. 3414; 15 U.S.C. 1681v; 15 U.S.C. 1681u; 50 U.S.C. 436; the text of each is appended.

Federal administrative subpoena authority is discussed in U.S. Department of Justice, Office of Legal Policy, Report to Congress on the Use of Administrative Subpoena Authorities by Executive Branch Agencies and Entities [2002], available on March 6, 2006 at http://www.usdoj.gov/olp/intro.pdf; see also CRS Report RL33321, Administrative Subpoenas in Criminal Investigations: A Brief Legal Analysis, abridged as CRS Report RS22407, Administrative Subpoenas in Criminal Investigations: A Sketch, both by Charles Doyle.

[2659] P.L. 1-7-56, 115 Stat. 365 (2001).

[2660] From calendar year 2003 through 2005, the FBI issued approximately 44,000 NSLs containing 143,074 requests. In one investigation, it issued 9 NSLs requesting information

practices and policies associated with the use of NSL authority contrary to the First Amendment right of freedom of speech, and thus brought into question the extent to which NSL authority could be used in the future.[2661] The USA PATRIOT Improvement and Reauthorization Act,[2662] and P.L. 109-178 (S. 2271) amended the NSL statutes and related law to address some of the concerns raised by critics and the courts.[2663] As a consequence, the Second Circuit dismissed one of the lower court cases as moot and remanded the other for reconsideration in light of the amendments.[2664] On reconsideration, the district court opinion continued to be troubled by the First Amendment implications of the nondisclosure features of 18 U.S.C. 2709, even as amended.[2665] The appellate court was comparable concerned, but concluded that the government might invoke the authority of 18 U.S.C. 2709 and 18 U.S.C. 3511 in a limited but constitutionally acceptable manner.[2666] On remand under the procedure envisioned by the Second Circuit panel, the district court found a continuing need to maintain the original secrecy order, but ordered the government to provide the plaintiffs with an unclassified, redacted summary of the declaration upon which the court's decision was based.[2667]

---

relating to 11,000 telephone numbers. U.S. Department of Justice, Office of the Inspector General, *A Review of the Federal Bureau of Investigation's Use of National Security Letters* (IG Report I) at xviii-xix (March 2007), available on Sept. 3, 2009 at http://www.usdoj.gov/oig/special/s0703b/ final.pdf. It issued another 49, 425 requests in 2006 for a total 192,499 requests over the four year period from 2003 through 2006, U.S. Department of Justice, Office of the Inspector General, *A Review of the Federal Bureau of Investigation's Use of National Security Letters* (IG Report II) at 9 (March 2008), available on Sept. 3, 2009 at http://www.usdoj.gov/oig/special/s0803b/final.pdf.

[2661] *Doe v. Ashcroft*, 334 F.Supp.2d 471, 526-27 (S.D.N.Y. 2004)("the Court concludes that the compulsory, secret, and unreviewable production of information required by the FBI's application of 18 U.S.C. 2709 violates the Fourth Amendment and that the non-disclosure provision of 18 U.S.C. 2709(c) violates the First Amendment"); *Doe v. Gonzales*, 386 F.Supp.2d 66, 78-82 (D.Conn. 2005)(the court did not reach the Fourth Amendment issue). Justice Ginsburg declined to lift the stay of Connecticut court's injunction pending appeal in the Second Circuit, 126 S.Ct. 1 (2005).

[2662] P.L. 109-177 (H.R. 3199), 120 Stat. 192 (2006).

[2663] The appended statutes note the amendments and additions.

[2664] *Doe v. Gonzalez*, 449 F.3d 415 (2d Cir. 2006).

[2665] *Doe v. Gonzalez*, 500 F.Supp.2d 379 (S.D.N.Y. 2007).

[2666] *John Doe, Inc. v. Mukasey*, 549 F.3d 861 (2d Cir. 2008).

[2667] *Doe v. Holder*, _____ F.Supp.2d _____ (2009 WL 2432320) (S.D.N.Y. Aug. 5, 2009).

Background

The ancestor of the first NSL letter provision is a statutory exception to privacy protections afforded by the Right to Financial Privacy Act (RFPA).[2668] Its history is not particularly instructive and consists primarily of a determination that the exception in its original form should not be too broadly construed.[2669] But the exception was just that, an exception. It was neither an affirmative grant of authority to request information nor a command to financial institutions to provided information when asked. It removed the restrictions on the release of customer information imposed on financial institutions by the Right to Financial Privacy Act, but it left them free to decline to comply when asked to do so.

> *[I]n certain significant instances, financial institutions [had] declined to grant the FBI access to financial records in response to requests under Section 1114(a). The FBI informed the Committee that the problem occurs particularly in States which have State constitutional privacy protection provisions or State banking privacy laws. In those States, financial institutions decline to grant the FBI access because State law prohibits them from granting such access and the RFPA, since it permits but does not mandate such access, does not override State law. In such a situation, the concerned financial institutions which might otherwise desire to grant the FBI access to a customer's record will not do so, because State law does not allow such cooperation, and cooperation might expose them to liability to the customer whose records the FBI sought access. H.Rept. 99-690, at 15-6 (1986).*

Congress responded with passage of the first NSL statute as an amendment to the Right to Financial Privacy Act, affirmatively giving the FBI access to financial institution records in certain foreign intelligence cases.[2670] At the same time in

---

[2668] Section 1114, P.L. 95-630, 92 Stat. 3706 (1978); now codified at 12 U.S.C. 3414(a)(1) (A), (B): "Nothing in this chapter (except sections 3415, 3417, 3418, and 3421 of this title) shall apply to the production and disclosure of financial records pursuant to requests from – (A) a Government authority authorized to conduct foreign counter- or foreign positive- intelligence activities for purposes of conducting such activities; [or] (B) the Secret Service for the purpose of conducting its protective functions (18 U.S.C. 3056; 3 U.S.C. 202, P.L.90-331, as amended)."

[2669] "Section 1114 provides for special procedures in the case of foreign intelligence ... though the committee believes that some privacy protections may well be necessary for financial records sought during a foreign intelligence investigation, there are special problems in this area which make consideration of such protections in other congressional forums more appropriate. Nevertheless, the committee intends that this exemption be used only for legitimate foreign intelligence investigations: investigations proceeding only under the rubric of "national security" do not qualify. Rather this exception is available only to those U.S. Government officials specifically authorized to investigate the intelligence operations of foreign governments," H.Rept. 95-1383, at 55 (1978).

[2670] P.L. 99-569, §404, 100 Stat. 3197 (1986); 12 U.S.C. 3414(a)(5)(A)(1988 ed.).

the Electronic Communications Privacy Act, it afforded the FBI comparable access to the telephone company and other communications service provider customer information.[2671] Together the two NSL provisions afforded the FBI access to communications and financial business records under limited circumstances—customer and customer transaction information held by telephone carriers and banks pertaining to a foreign power or its agents relevant to a foreign counter-intelligence investigation.[2672]

Both the communications provider section and the Right to Financial Privacy Act section contained nondisclosure provisions[2673] and limitations on further dissemination except pursuant of guidelines promulgated by the Attorney General.[2674] Neither had an express enforcement mechanism nor identified penalties for failure to comply with either the NSL or the nondisclosure instruction.

In the mid-1990s, Congress added two more NSL provisions—one permits NSL use in connection with the investigation of government employee leaks of classified information under the National Security Act;[2675] and the other grants the FBI access to credit agency records pursuant to the Fair Credit Reporting Act, under much the same conditions as apply to the records of financial institutions.[2676] The FBI asked for the Fair Credit Reporting Act amendment as a threshold mechanism to enable it to make more effective use of its bank record access authority:

> *FBI's right of access under the Right of Financial Privacy Act cannot be effectively used, however, until the FBI discovers which financial institutions are being utilized by the subject of a counterintelligence investigation. Consumer reports maintained by credit bureaus are a ready source of such information, but,*

[2671] 18 U.S.C. 2709 (1988 ed.); see also, S.Rept. 99-541, at 43 (1986)("This provision is substantially the same as language recently reported by the Intelligence Committee as section 503 of the Intelligence Authorization Act for Fiscal Year 1987, [P.L. 99-569]").

[2672] 18 U.S.C. 2709 (1988 ed.); 12 U.S.C. 3414(a)(5)(A)(1988 ed.).

[2673] 18 U.S.C. 2709(c)("No wire or electronic communication service provider, or officer, employee, or agent thereof, shall disclose to any person that the Federal Bureau of Investigation has sought or obtained access to information or records under this section"); see also, 12 U.S.C. 3414(a)(5)(D). Note that unlike section 3486, the prohibition is neither temporary nor judicially supervised.

[2674] 18 U.S.C. 2709(d)(1988 ed.); 12 U.S.C. 3414(a)(5)(B)(1988 ed.).

[2675] 50 U.S.C. 436.

[2676] 15 U.S.C. 1681u.

> *although such report[s] are readily available to the private sector, they are not available to FBI counterintelligence investigators....*
>
> *FBI has made a specific showing ... that the effort to identify financial institutions in order to make use of FBI authority under the Right to Financial Privacy Act can not only be time-consuming and resource-intensive, but can also require the use of investigative techniques— such as physical and electronic surveillance, review of mail covers, and canvassing of all banks in an area—that would appear to be more intrusive than the review of credit reports. H.Rept. 104-427, at 36 (1996).*[2677]

The National Security Act NSL provision authorized access to credit and financial institution records of federal employees with security clearances who were required to give their consent as a condition for clearance.[2678] Passed in the wake of the Ames espionage case, it is limited to investigations of classified information leaks. As noted at the time, "The Committee believes section 801 will serve as a deterrent to espionage for financial gain without burdening investigative agencies with unproductive recordkeeping or subjecting employees to new reporting requirements.... The Committee recognizes that consumer credit records have been notoriously inaccurate, and expects that information obtained pursuant to this section alone will not be the basis of an action or decision adverse to the interest of the employee involved."[2679]

Both the Fair Credit Reporting Act section and the National Security Act section contain dissemination restrictions;[2680] as well as safe harbor (immunity),[2681] and nondisclosure provisions.[2682] Neither has an explicit penalty for improper disclosure of the request, but the Fair Credit Reporting Act section expressly authorizes judicial enforcement.[2683]

[2677] The Senate Intelligence Committee had made similar observations in a prior Congress when considering legislation that ultimately became the National Security Amendment, H.Rept. 103-256, at 17-22 (1994).

[2678] 50 U.S.C. 456 (1994 ed.).

[2679] H.Rep.No.103-541 at 53-4 (1994).

[2680] 15 U.S.C. 1681u(f), 50 U.S.C. 436(e).

[2681] 15 U.S.C. 1681u(k), 50 U.S.C. 436(c).

[2682] 15 U.S.C. 1681u(d); 50 U.S.C. 436(b).

[2683] 15 U.S.C. 1681u(c).

The USA PATRIOT Act amended three of the four existing NSL statutes and added a fifth. In each of the three NSL statutes available exclusively to the FBI—the Electronic Communications Privacy Act section (18 U.S.C. 2709), the Right to Financial Privacy Act section (12 U.S.C. 3414(a)(5)), and the Fair Credit Reporting Act section (15 U.S.C. 1681u)—Section 505 of the USA PATRIOT Act:

- expanded FBI issuing authority beyond FBI headquarter officials to include the heads of the FBI field offices (i.e., Special Agents in Charge (SAC));
- eliminated the requirement that the record information sought pertain to a foreign power or the agent of a foreign power;
- required instead that the NSL request be relevant to an investigation to protect against international terrorism or foreign spying;
- added the caveat that no such investigation of an American can be predicated exclusively of First Amendment protected activities.[2684]

The amendments allowed NSL authority to be employed more quickly (without the delays associated with prior approval from FBI headquarters) and more widely (without requiring that the information pertain to a foreign power or its agents).[2685]

[2684] P.L. 107-56, §505, 115 Stat. 365-66 (2001).

[2685] "The information acquired through NSLs is extremely valuable to national security investigations…. Unfortunately, however, NSLs were of limited utility prior to the PATRIOT Act. While records held by third parties may generally be subpoenaed by a grand jury in a criminal investigation so long as those records are relevant, the standard for obtaining such records through an NSL was much higher before October of 2001.

"The FBI had to have specific and articulable facts that the information requested pertained to a foreign power or an agent of a foreign power. This requirement often prohibited the FBI from using NSLs to develop evidence at the early stage of an investigation, which is precisely when they are the most useful.

"The prior standard, Mr. Chairman, put the cart before the horse. Agents trying to determine whether or not there were specific and articulable facts that a certain individual was a terrorist or spy were precluded from using an NSL in this inquiry because, in order to use an NSL, they first had to be in possession of such facts.

"Suppose, for example, investigators were tracking a known al-Qaeda operative and saw him having lunch with three individuals. A responsible agent would want to conduct a preliminary investigation of those individuals and find out, among other things, with whom they had recently been in communication.

"Before the passage of the PATRIOT Act, however, the FBI could not have issued an NSL to obtain such information. While investigators could have demonstrated that this information was relevant to an ongoing terrorism investigation, they could not have demonstrated sufficient specific, and articulable facts that the individuals in question were agents of a foreign power," Material Witness Provisions of the Criminal Code, and the Implementation of the USA PATRIOT Act: Section 505 That Addresses National Security Letters, and Section 804 That Addresses Jurisdiction Over Crimes Committed at U.S. Facilities Abroad: Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Security of the House Comm. on the Judiciary, 109th Cong., 1st Sess. at 9-10 (2005) (testimony of Matthew Berry, Office of Legal Policy, U.S. Department of Justice).

Subsection 358(g) of the USA PATRIOT Act amended the Fair Credit Reporting Act to add a fifth and final NSL section; the provision had one particularly noteworthy feature, it was available not merely to the FBI but to any government agency investigating or analyzing international terrorism:

> *Notwithstanding section 1681b of this title or any other provision of this subchapter, a consumer reporting agency shall furnish a consumer report of a consumer and all other information in a consumer's file to a government agency authorized to conduct investigations of, or intelligence or counterintelligence activities or analysis related to, international terrorism when presented with a written certification by such government agency that such information is necessary for the agency's conduct or such investigation, activity or analysis.*[2686]

Although the subsection's legislative history treats it as a matter of first impression,[2687] Congress's obvious intent was to provide other agencies with the national security letter authority comparable to that enjoyed by the FBI under the Fair Credit Reporting Act. The new section had a nondisclosure and a safe harbor subsection, 15 U.S.C. 1681v(c), (e), but no express means of judicial enforcement or penalties for improper disclosure of a request under the section.

In the 108th Congress, the scope of the Right to Financial Privacy Act NSL was enlarged by defining the financial institutions subject to the authority to include not only banks and credit unions but also car dealers, jewelers, and real estate agents, among others.[2688] The same Congress saw a number of proposals

---

[2686] P.L. 107-56, §358(g), 115 Stat. 327 (2001).

[2687] E.g., H.Rept. 107-250, at 60-1 ("This section facilitates government access to information contained in suspected terrorists' credit reports when the government inquiry relates to an investigation, of or intelligence activity or analysis relating to, domestic or international terrorism. Even though private entities such as lender and insurers can access an individual's credit history, the government is strictly limited in its ability under current law to obtain the information. This section would permit those investigating suspected terrorists prompt access to credit histories that may reveal key information about the terrorist's plan or source of refunding – without notifying the target").

[2688] P.L. 108-177, §374, 117 Stat. 2628 (2004), 12 U.S.C. 3414(d), adopts the definition of financial institution found in 31 U.S.C. 5312(a)(2), (c)(1), i.e.: "(A) an insured bank (as defined in 12 U.S.C. 1813(h)); (B) a commercial bank or trust company; (C) a private banker; (D) an agency or branch of a foreign bank in the United States; (E) any credit union; (F) a thrift institution; (G) a broker or dealer registered with the Securities and Exchange Commission; (H) a broker or dealer in securities or commodities; (I) an investment banker or investment company; (J) a currency exchange; (K) an issuer, redeemer, or cashier of travelers' checks, checks, money orders, or similar instruments; (L) an operator of a credit card system; (M) an insurance company; (N) a dealer in precious metals, stones, or jewels; (O) a pawnbroker; (P) a loan or finance company; (Q)

introduced to exempt libraries from the reach of the communications NSL,[2689] to increase congressional oversight over the use of NSL authority,[2690] and to add the USA PATRIOT Act section 505 NSL amendments to the list of those temporary sections scheduled to expire on December 31, 2005.[2691] The 108th also witnessed the introduction of proposals that ultimately evolved into the NSL amendments in the USA PATRIOT Improvement and Reauthorization Act. H.R. 3179, introduced by Representative Sensenbrenner. They would have reinforced the five national security letter provisions with explicit authority for judicial enforcement[2692] and with criminal penalties for improper disclosure of the issuance of such letters. The penalties were to be the same as those proposed under the general administrative subpoena bills offered in the 108th—imprisonment for not more than five years when committed with the intent to obstruct and for not more than one year otherwise, proposed 18 U.S.C. 1510(e). A Justice Department witness explained that, "Oftentimes, the premature disclosure of an ongoing terrorism investigation can lead to a host of negative repercussions, including the destruction of evidence, the flight of suspected terrorists, and the frustration of efforts to identify additional terrorist conspirators. For these reasons, the FBI has forgone using NSLs in some investigations for fear that the recipients of those NSLs would compromise an

---

a travel agency; (R) a licensed sender of money or any other person who engages as a business in the transmission of funds, including any person who engages as a business in an informal money transfer system or any network of people who engage as a business in facilitating the transfer of money domestically or internationally outside of the conventional financial institutions system; (S) a telegraph company; (T) a business engaged in vehicle sales, including automobile, airplane, and boat sales; (U) persons involved in real estate closings and settlements; (V) the United States Postal Service; (W) an agency of the United States Government or of a State or local government carrying out a duty or power of a business described in this paragraph; (X) a casino, gambling casino, or gaming establishment with an annual gaming revenue of more than $1,000,000 which – (i) is licensed as a casino, gambling casino, or gaming establishment under the laws of any State or any political subdivision of any State; or (ii) is an Indian gaming operation conducted under or pursuant to the Indian Gaming Regulatory Act other than an operation which is limited to class I gaming (as defined in section 4(6) of such Act); (Y) any business or agency which engages in any activity which the Secretary of the Treasury determines, by regulation, to be an activity which is similar to, related to, or a substitute for any activity in which any business described in this paragraph is authorized to engage; (Z) any other business designated by the Secretary whose cash transactions have a high degree of usefulness in criminal, tax, or regulatory matters; [or (AA)] any futures commission merchant, commodity trading advisor, or commodity pool operator registered, or required to register, under the Commodity Exchange Act."

[2689] H.R. 3352, §5 (Rep. Otter); S. 1158, §3 (Sen. Boxer); S. 1507, §2 (Sen. Feingold); S. 1552, §4(b) (Sen. Murkowski); and S. 1709, §5 (Sen. Craig).

[2690] S. 436, §3 (Sen. Leahy).

[2691] H.R. 3171, §4 (Rep. Kucinich); H.R. 3352, §7 (Rep. Otter); S. 1695, §2 (Sen. Leahy); and S. 1709, §6 (Sen. Craig).

[2692] In *Doe v. Ashcroft*, 334 F.Supp.2d 471, 496-501 (S.D.N.Y. 2004), the Government argued unsuccessfully that the NSL statutes should be understood to include an implicit judicial enforcement component.

investigation by disclosing the fact that they had been sent an NSL."[2693] The enforcement provision would have been backed by the court's contempt power, proposed 18 U.S.C. 2332h.[2694] It had no explicit provisions, however, to permit the recipient to file a motion to quash or modify the NSL request.

Pre-amendment Judicial Action

Proponents of legislative proposals in the 108th Congress did not enjoy the benefit of two court decisions that colored the debate over NSL authority during the 109th Congress. *Doe v. Ashcroft*,[2695] reached much the same conclusion on the First Amendment issue: narrowly defined, the government's and *Doe v. Gonzales*[2696] suggested that the NSL statutes could not withstand constitutional scrutiny unless more explicit provisions were made for judicial review and permissible disclosure by recipients. In essence, *Doe v. Ashcroft* found that the language of 18 U.S.C. 2709 and the practices surrounding its use offended (1) the Fourth Amendment because "in all but the exceptional case it [had] the effect of authorizing coercive searches effectively immune from any judicial process," 334 F.Supp.2d at 506, and (2) the First Amendment because its sweeping, permanent secrecy order feature applied "in every case, to every person, in perpetuity, with no vehicle for the ban to ever be lifted from the recipient or other persons affected under any circumstances, either by the FBI itself, or pursuant to judicial process," id. at 476.

NSL Amendments in the 109th Congress

[2693] Anti-Terrorism Intelligence Tools Improvement Act of 2003: Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Security (House Hearing), 108th Cong., 2nd Sess., 7-8 (2004)(prepared statement of United States Assistant Attorney General Daniel J. Bryant).

[2694] Proposed 18 U.S.C. 2332h ("In the case of a refusal to comply with a request for records, a report, or other information made to any person under section 2709(b) of this title, section 625 (a) or (b) or 626 of the Fair Credit Reporting Act [15 U.S.C. 1681u, 1681v], section 1114(a)(5)A) of the right to Financial Privacy Act [12 U.S.C. 3414, or section 802(a) of the National Security Act of 1947 [50 U.S.C. 436(a)], the Attorney General may invoke the aid of any court of the United States within the jurisdiction of which the investigation is carried on or the person resides, carries on business, or may be found, to compel compliance with the request. The court may issue an order requiring the person to comply with the request. Any failure to obey the order of the court may be punished by the court as contempt thereof. Any process under this section may be served in any judicial district in which the person may be found").

[2695] 334 F.Supp.2d 471 (S.D.N.Y. 2004), vac'd and remanded, 449 F.3d 415 (2d Cir. 2006), after remand, 500 F.Supp.2d 379 (S.D.N.Y. 2007), aff'd in part, rev'd in part and remanded, 549 F.3d 861 (2d Cir. 2008), after remand, _____ F.Supp.2d _____ (2009 WL 2432320)(S.D.N.Y. Aug. 5, 2009).

[2696] 386 F.Supp.2d 66 (D.Conn. 2005), dism'd as moot, 449 F.3d 415 (2d Cir. 2006).

Both USA PATRIOT Act reauthorization statutes—P.L. 109-177(H.R. 3199) and P.L. 109-178 (S. 2271)[2697]—amended each of the NSL statutes. They

- created a judicial enforcement mechanism and a judicial review procedure for both the requests and accompanying nondisclosure requirements;[2698]
- established specific penalties for failure to comply or to observe the nondisclosure requirements;[2699]
- made it clear that the nondisclosure requirements did not preclude a recipient from consulting an attorney;[2700]
- provided a process to ease the nondisclosure requirement;[2701]
- expanded congressional oversight;[2702]
- called for an Inspector General's audit of use of the authority.[2703]

Post-Amendment NSL Attributes

Addressees and Certifying Officials

The five NSL statutes share a number of common attributes, although each has its own individual features as well. They are most distinctive with respect to the nature of the businesses to whom they may be addressed. The Electronic Communication Privacy Act NSLs are addressed to communications providers.[2704] Those issued under the authority of the Right to Financial Privacy Act may be directed to any financial institution, which as noted earlier, includes not only banks and credit unions, but credit card companies, car dealers, jewelers and a number of entities that are likely the scene of large cash transactions.[2705] The Fair Credit Reporting Act NSLs may be addressed to consumer credit reporting agencies.[2706] Recipients of the National Security Act NSLs may include

---

[2697] 120 Stat. 192 (2006) and 120 Stat. 278 (2006), respectively.

[2698] 28 U.S.C. 3511.

[2699] 28 U.S.C. 3511(c), 18 U.S.C. 1510(e).

[2700] 12 U.S.C. 3414((a)(3)(A); 15 U.S.C. 1681v(c)(1), 1681u(d)(1); 18 U.S.C. 2709(c)(1); 50 U.S.C. 436(B)(1).

[2701] 28 U.S.C. 3511(b).

[2702] P.L. 109-177, §118.

[2703] P.L. 109-177, §119.

[2704] 18 U.S.C. 2709.

[2705] 12 U.S.C. 3414(a), (d).

[2706] 15 U.S.C. 1681u(a), 1681v(a).

either financial institutions or consumer credit reporting agencies as well as any commercial entity with information concerning an agency employee's travel.[2707]

FBI officials are authorized to provide the initial certification required for issuance of an NSL under any of the five statutes. In three instances, the authority is exclusive; in the other two, it is enjoyed by other federal officials as well. In the case of the Electronic Communications Privacy Act NSL section, the Right to Financial Privacy Act section, and one of the Fair Credit Report Act NSL sections, issuance requires the certification of either the Director of the FBI, a senior FBI official (no lower than the Deputy Assistant Director), or the Special Agent in Charge of an FBI field office.[2708]

Certifying officials under the other statutes are described more broadly. The National Security Act NSL section contemplates certification by officials from a wider range of agencies; the second Fair Credit Reporting Act NSL section allows certification by both a wider range of agencies and a wider range of officials. Senior officials no lower than Assistant Secretary or Assistant Director of an agency whose employee with access to classified material is under investigation may certify a National Security Act NSL request.[2709] A designated supervisory official of any agency "authorized to conduct investigations of, or intelligence or counterintelligence activities and analysis related to, international terrorism" may certify a NSL request under the second, more recent Fair Credit Reporting Act section.[2710]

Purpose, Standards, Information Covered

Although variously phrased, the purpose for each of the NSLs is to acquire information related to the requesting agency's national security concerns. The most common statement of purpose is "to protect against international terrorism or clandestine intelligence activities."[2711] The more recent of the Fair Credit Reporting Act NSL sections simply indicates that the information must be sought for the requesting intelligence agency's investigation, activity or analysis.[2712] The National Security Act NSL authority is available to conduct law enforcement

---

[2707] 50 U.S.C. 436(a).

[2708] 18 U.S.C. 2709 (b); 12 U.S.C. 3414(a)(5)(A); 15 U.S.C. 1681u(b).

[2709] 50 U.S.C. 436 (a)(3).

[2710] 15 U.S.C. 1681v(a).

[2711] 18 U.S.C. 2709(b); 12 U.S.C. 3414(a)(5)(A); 15 U.S.C. 1681u(b).

[2712] 15 U.S.C. 1681v(a).

investigations, counterintelligence inquiries, and security determinations.[2713] As to standards, the Electronic Communications Privacy Act authorizes NSLs for relevant information.[2714] The same standard may apply to the others which are a little more cryptic, authorizing NSLs when the information is "sought for"[2715] or "is necessary"[2716] for the statutory purpose.

The communications NSL provision and the earlier of the two credit agency NSL statutes are fairly specific in their descriptions of the information that may be requested through an NSL. An Electronic Communications Privacy Act NSL may request a customer's name, address, length of service and billing records.[2717] The older of the two Fair Credit Report Act sections authorizes a NSL to acquire name, address or former address, place or former place of employment, and the name and address of any financial institution with which the consumer has or once had an account.[2718] The Right to Financial Privacy Act NSL provision covers the financial records of a financial institution's customers;[2719] the second and more recent Fair Credit Reporting Act NSL provision covers a consumer reporting agency's consumer reports and "all other" consumer information in its files.[2720] The National Security Act provision is at once the most inclusive and the most restricted. It authorizes NSLs for financial information and records and consumer reports held by any financial agency, institution, holding company or consumer reporting agency, and for travel information held by any commercial entity.[2721] On the other hand, it is the only provision that limits the information provided to that pertaining to the target of the agency's investigation and to information of a kind whose disclosure the target has previously approved.[2722]

Confidentiality

[2713] 50 U.S.C. 436(a)(1).

[2714] 18 U.S.C. 2709(b).

[2715] 15 U.S.C. 1681u(a); 12 U.S.C. 3414(a)(5)(A).

[2716] 15 U.S.C. 1681v; 50 U.S.C. 436(a).

[2717] 18 U.S.C. 2709(b).

[2718] 15 U.S.C. 1681u(a),(b).

[2719] 12 U.S.C. 3414(a)(5)(A).

[2720] 15 U.S.C. 1681v(a).

[2721] 50 U.S.C. 436(a)(1).

[2722] 50 U.S.C. 436(a)(2),(3).

Prior to their amendment in the 109th Congress, the NSL statutes generally featured an open ended confidentiality clause. The communications NSL provision for example declared, "No wire or electronic communication service provider, or officer, or employee, or agent thereof, shall disclose to any person that the Federal Bureau of Investigation has sought or obtained access to information or records under this section."[2723] The statutes did not indicate whether a recipient might consult an attorney in order to ascertain his rights and obligations nor whether it might ever be lifted. It was this silence in the face of a seemingly absolute, permanent nondisclosure command that the early Doe courts found constitutionally unacceptable[2724] and that perhaps led to the reconstruction of the NSL confidentiality requirements in their current form.

As NSL statutes now read, secrecy is not absolutely required. Instead NSL recipients are bound to secrecy only upon the certification of the requesting agency that disclosure of the request or response may result in a danger to national security; may interfere with diplomatic relations or with a criminal, counterterrorism, or counterintelligence investigation; or may endanger the physical safety of an individual. A recipient may disclose the request to those necessary to comply with the request and to an attorney the recipient consults for related legal advice or assistance. In doing so, the recipient must advise them of the secrecy requirements. Aside from its attorney and at the agency's election, the recipient must also identify those to whom it has disclosed the request. A recipient may petition the court to modify or extinguish any NSL secrecy requirement within a year of issuance.[2725] Thereafter, it may petition to have the veil of secrecy lifted, although it may resubmit a rejected request only once a year.[2726] In all instances, section 3511 declares conclusive and warranting continued secrecy the certification by certain officials that disclosure might create a danger to national security, interfere with diplomatic relations or ongoing investigations, or jeopardize personal safety.[2727] A breach of a confidentiality requirement committed knowingly and with the intent to obstruct an investigation or related judicial proceedings is punishable by imprisonment for

---

[2723] 18 U.S.C. 2709(c) (2000 ed.); see also, 12 U.S.C. 3414(a)(5)(D) (2000 ed.); 15 U.S.C. 1681u(d) (2000 ed.); 15 U.S.C. 1681v(c) (2002 Supp.); 50 U.S.C. 436(b) (2000 ed.).

[2724] *Doe v. Ashcroft*, 334 F.Supp.2d 471, 522 (S.D.N.Y. 2004). and *Doe v. Gonzales*, 386 F.Supp.2d 66, 78-81 (D.Conn. 2005).

[2725] 28 U.S.C. 3511(b)(2). As construed by the Second Circuit, the government is obliged to advise a recipient that the recipient has a period of time within which to decide if he would like the government to seek judicial review of its determination of the need for secrecy, *John Doe, Inc.v. Mukasey*, 549 F.3d 861, 883 (2d Cir. 2008).

[2726] 28 U.S.C. 3511(b)(3).

[2727] 28 U.S.C. 3511(b)(2), (3). The Second Circuit has declared this component of the procedure unconstitutional, *John Doe, Inc.v. Mukasey*, 549 F.3d at 883.

not more than five years and/or a fine of not more than $250,000 (not more than $500,000 for an organization).[2728]

Judicial Review and Enforcement

In addition to authority to review and set aside NSL nondisclosure requirements, the federal courts also enjoy jurisdiction to review and enforce the underlying NSL requests. Recipients may petition and be granted an order modifying or setting aside an NSL, if the court finds that compliance would be unreasonable, oppressive, or otherwise unlawful.[2729] Subpoenas issued under the Federal Rules of Criminal Procedure may be modified or quashed if compliance would be unreasonable or oppressive.[2730] The Rule affords protection against undue burdens and protects privileged communications.[2731] Compliance with a particular NSL might be unduly burdensome in some situations, but the circumstances under which NSLs are used suggest few federally recognized privileges. The Rule also imposes a relevancy requirement, but in the context of an investigation a motion to quash will be denied unless it can be shown that "there is no reasonable possibility that the category of materials the Government seeks will produce information relevant" to the investigation.[2732] The authority to modify or set aside a NSL that is unlawful affords the court an opportunity to determine whether the NSL in question complies with the statutory provisions under which it was issued. On the other hand, the court's authority may be invoked to enforce the NSL against a recalcitrant recipient and failure to comply thereafter is punishable as contempt of court.[2733]

Dissemination

Attorney General guidelines govern the sharing of information acquired in response to NSLs under two statutes.[2734] A third, the older of the two Fair Credit

---

[2728] 18 U.S.C. 1510(e), 3571, 3559.

[2729] 28 U.S.C. 3511.

[2730] F.R.Crim.P. 17(c)(2).

[2731] 2 WRIGHT, FEDERAL PRACTICE AND PROCEDURE §275 (Crim. 3d ed. 2000).

[2732] *United States v. R. Enterprises, Inc.*, 498 U.S. 292, 301 (1991).

[2733] 28 U.S.C. 3511(c).

[2734] 12 U.S.C. 3414(a)(5)(B)("The Federal Bureau of Investigation may disseminate information obtained pursuant to this paragraph only as provided in guidelines approved by the Attorney General for foreign intelligence collection and foreign counterintelligence investigations conducted by the Federal Bureau of Investigation, and, with respect to dissemination to an agency of the United States, only if such information is clearly relevant to the authorized responsibilities of such agency"); see also, 18 U.S.C. 2709(d).

Report Act sections, limits dissemination to sharing within the FBI, with other agencies to the extent necessary to secure approval of a foreign counterintelligence investigation, or with military investigators when the information concerns a member of the Armed Forces.[2735] The National Security Act authorizes dissemination of NSL information to the agency of the employee under investigation, to the Justice Department for law enforcement or counterintelligence purposes, or to another federal agency if the information is clearly relevant to its mission.[2736] The more recent Fair Credit Reporting Act NSL section has no explicit provision on restricting dissemination.[2737]

Liability, Fees and Oversight

Since judicial enforcement is a feature new to all but one of the NSL statutes,[2738] they might be expected to include other incentives to overcome recipient resistance. Three do offer immunity from civil liability for recipients who comply in good faith,[2739] and two offer fees or reimbursement to defer the costs of compliance.[2740]

The confidentiality that necessarily surrounds NSL requests could give rise to concerns of governmental overreaching. Consequently, regular reports on the use of NSL authority must be made to the congressional intelligence and judiciary committees and in some instances to the banking committees.[2741] Moreover, section 119 of the USA PATRIOT Improvement and Reauthorization Act instructs the Inspector General of the Department of Justice to audit and to report to the judiciary and intelligence committees as to the Department's use of the authority in the years following expansion of the authority in the USA PATRIOT Act. The section also directs the Attorney General and the Director of National Intelligence to report to Congress on the feasibility of establishing minimization requirements for the NSLs.

[2735] 15 U.S.C. 1681u(f).

[2736] 50 U.S.C. 436(e).

[2737] 15 U.S.C. 1681v.

[2738] In addition to the newly added judicial enforcement mechanism in 28 U.S.C. 3511, the earlier Fair Credit Report Act NSL sections had a limited judicial enforcement subsection, as it had for some time, 15 U.S.C. 1681u(c).

[2739] 15 U.S.C. 1681u(k), 1681v(e); 50 U.S.C. 436(c)(2).

[2740] 15 U.S.C. 1681u(e); 50 U.S.C. 4356(d).

[2741] P.L. 109-177, §118(a)(adding the judiciary committees as recipients of all NSL required reports); 12 U.S.C. 3414(a)(5)(C)(intelligence committees); 18 U.S.C. 2709 (intelligence and judiciary committees); 15 U.S.C. 1681u(h)(intelligence and banking committees), 1681v(judiciary, intelligence, and banking committees).

Inspector General's Reports

IG Report I

Section 119 of the USA PATRIOT Improvement and Reauthorization Act, P.L. 109-177, 120 Stat. 219 (2006), instructed the Department of Justice's Inspector General to review and report on the FBI's use of NSLs. In early March 2007, the Inspector General released the first of two required reports that covered calendar years 2003 through 2005. The second, covering the time period through the end of calendar year 2006, was released in March 2008.

The initial report notes that FBI use of NSLs has increased dramatically, expanding from 8,500 requests in 2000 to 47,000 in 2005, IG Report I at 120. Seventy-four percent were issued in conjunction with counterterrorism investigations, most of the rest in connection with counterintelligence investigations, and less than 1 percent as part of a foreign computer intrusion investigation, Id. During the three years under review, the percentage of NSLs used to investigate Americans ("U.S. persons") increased from 39% in 2003 to 53% in 2005.[2742] A substantial majority of the requests involve records relating to telephone or e-mail communications, IG Report I at 120.

The report is somewhat critical of the FBI's initial performance:

> *[W]e found that the FBI used NSLs in violation of applicable NSL statutes, Attorney General Guidelines, and internal FBI policies. In addition, we found that the FBI circumvented the requirements of the ECPA NSL statute when it issued at least 739 "exigent letters" to obtain telephone toll billing records and subscriber information from three telephone companies without first issuing NSLs. Moreover, in a few other instances, the FBI sought or obtained telephone toll billing records in the absence of a national security investigation, when it sought and obtained consumer full credit reports in a counterintelligence investigation, and when it sought and obtained financial records and telephone toll billing records without first issuing NSLs. Id. at 124.*

More specifically, the Report found that:

[2742] Id. A "U.S. person" is generally understood to mean "a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 1101(a)(2) of title 8), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in subsection(a)(1), (2), or (3) of this section," 50 U.S.C. 1801.

- a "significant number of NSL-related possible violations are not being identified or reported" as required
- the only FBI data collection system produced "inaccurate" results
- a "significant number of NSL-related possible violations are not being identified or reported" as required
- the FBI issued over 700 exigent letters acquiring information in a manner that "circumvented the ECPA NSL statute and violated the Attorney General's Guidelines … and internal FBI policy"
- the FBI's Counterterrorism Division initiated over 300 NSLs in a manner that precluded effective review prior to approval
- 60% of the individual files examined showed violations of FBI internal control policies
- the FBI did not retain signed copies of the NSLs it issues
- the FBI had not provided clear guidance on the application of the Attorney General's least-intrusive-feasible-investigative-technique standard in the case of NSLs
- the precise interpretation of toll billing information as it appears in the ECPA NSL statute is unclear
- SAC supervision of the attorneys responsible for review of the legal adequacy of proposed NSLs made some of the attorneys reluctant to question the adequacy of the underlying investigation previously approved by the SAC
- there was no indication that the FBI's misuse of NSL authority constituted criminal conduct
- personnel both at FBI headquarters and in the field consider NSL use indispensable
- information generated by NSLs is fed into a number of FBI systems. IG Report I at 121-24.

Exigent Letters

Prior to enactment of the ECPA, the Supreme Court held that customers had no Fourth Amendment protected privacy rights in the records the telephone company maintained relating to their telephone use.[2743] Where a recognized expectation of privacy exists for Fourth Amendment purposes, the Amendment's usual demands such as those of probable cause, particularity, and a warrant may be eased in the face of exigent circumstances. For example, the Fourth Amendment requirement that officers must knock and announce their purpose before forcibly entering a building to execute a warrant can be eased in the presence of certain exigent circumstances such as the threat of the destruction of

[2743] Smith v. Maryland, 442 U.S. 735, 745 (1979).

evidence or danger to the officers.[2744] Satisfying Fourth Amendment requirements, however, does not necessary satisfy statutory demands.

The ECPA prohibits communications service providers from supplying information concerning customer records unless one of the statutory exceptions applies.[2745] There are specific exceptions for disclosure upon receipt of a grand jury subpoena[2746] or an NSL.[2747] A service provider who knowingly or intentionally violates the prohibition is subject to civil liability,[2748] but there are no criminal penalties for the breach.

The Inspector General found that contrary to assertions that "the FBI would obtain telephone records only after it served NSLs or grand jury subpoenas, the FBI obtained telephone bill records and subscriber information prior to serving NSLs or grand jury subpoenas" by use "exigent letters."[2749] The FBI responded that it had barred the use of exigent letters, but emphasized that the term "exigent letter" does not include emergency disclosures under the exception now found in 18 U.S.C. 2702(c) (4). Thus, the FBI might request that a service provider invoke that exception to the record disclosure bar "if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person justifies disclosure of the information," 18 U.S.C. 2702(c)(4).

IG Report II

The second IG Report reviewed the FBI's use of national security letter authority during calendar year 2006 and the corrective measures taken following the issuance of the IG's first report. The second Report concluded that:

- "the FBI's use of national security letters in 2006 continued the upward trend ... identified ... for the period covering 2003 through 2006"
- "the percentage of NSL requests generated from investigations of U.S. persons continued to increase significantly, from approximately 39% of all NSL requests issued in 2003 to approximately 57% of all NSL requests issued in 2006"

[2744] Richards v. Wisconsin, 520 U.S. 385, 391 (1997); Wilson v. Arkansas, 514 U.S. 927, 936 (1995).

[2745] 18 U.S.C. 2702(c).

[2746] 18 U.S.C. 2703(c)(2).

[2747] 18 U.S.C. 2709(a).

[2748] 18 U.S.C. 2707(a).

[2749] IG Report I at 90.

- the FBI and DoJ are committed to correcting the problems identified in IG Report I and "have made significant progress in addressing the need to improve compliance in the FBI's use of NSLs"
- "it is too early to definitively state whether the new systems and controls developed by the FBI and the Department will eliminate fully the problems with NSLs that we identified," IG Report II at 8-9.

Post-Amendment Judicial Action

Following the 2006 USA PATRIOT Act amendments, the District Court for the Southern District of New York revisited the issue anew and concluded that the revised NSL procedures violated both First Amendment and separation of powers principles.[2750] It enjoined Justice Department officials from issuing NSLs under section 2709 or from enforcing compliance with existing orders.[2751] However, it stayed the order pending appeal.[2752] The Court of Appeals was similarly disposed, but concluded that the government could invoke the secrecy and judicial review authority of the 18 U.S.C. 2709 and 18 U.S.C. 3511 in a limited, but constitutionally permissible manner.[2753]

The issues before the Court of Appeals were (1) whether the nondisclosure features of section 2709(c) should be subject to First Amendment strict scrutiny and (2) whether judicial review subject to the conclusive weight of an executive branch certification under section 3511 posed constitutional concerns.

The pre-amendment Doe cases had concluded that section 2709(c), which then broadly prohibited disclosure of receipt of an NSL, "work[ed] as both a prior restraint on speech and a content-based restriction, and hence, [was] subject to strict scrutiny."[2754] "Under strict scrutiny review," the Supreme Court has explained, "the Government must demonstrate that the nondisclosure requirement is narrowly tailored to promote a compelling Government interest."[2755] Moreover, there can be "no less restrictive alternatives that would be at least as effective in achieving the legitimate purpose that the statute was

---

[2750] *Doe v. Gonzalez*, 500 F.Supp.2d 379 (S.D.N.Y. 2007), *aff'd in part, rev'd in part, and remanded, sub nom.*, *John Doe, Inc. v. Mukasey*, 549 F.861 (2d Cir. 2008).

[2751] *Doe v. Gonzalez* at 425-26.

[2752] Id. at 426.

[2753] *John Doe, Inc. v. Mukasey*, 549 F.3d at 883-84.

[2754] Doe v. Ashcroft, 334 F.Supp.2d 471, 511 (S.D.N.Y. 2004); Doe v. Gonzales, 386 F.Supp.2d 66, 75 (D.Conn. 2005)("Section 2709(c) is subject to strict scrutiny not only because it is a prior restraint, but also because it is a content-based restriction").

[2755] Playboy Entertainment 529 U.S. 803, 813 (2000).

enacted to serve."[2756] When a suspect prior restraint comes in the form of a licensing scheme, under which expression is banned for want government permission as in Freedman v. Maryland, the scheme must include prompt judicial review at the petition and burden of the regulator.[2757]

Yet, the courts have been unwilling to classify as constitutionally suspect all instances of apparent prior restraint. The government in its presentation to the Second Circuit point to a number of instances where withstanding an apparent prior restraint regulators were held to a less demanding standard—citing cases involving pre-trial discovery gag orders, grand jury secrecy, the confidentiality surrounding inquiry into judicial misconduct, and the secrecy agreements signed by national security employees.[2758]

In fact when the Supreme Court assessed the First Amendment validity of a pre-trial discovery gag order, it concluded that the relevant questions were two: first, "whether the practice in question furthers an important or substantial governmental interest unrelated to the suppression of expression;" and second, "whether the limitation of First Amendment freedoms is no greater than is necessary or essential to the protection of the particular governmental interest involved."[2759]

The members of the Second Circuit panel could not agree on whether section 2709(c), as amended, constituted a prior restraint subject to strict scrutiny analysis, or should be judged by a somewhat less demanding standard. The lack of consensus proved of little consequence, because the government conceded that strict scrutiny analysis was appropriate,[2760] and because the panel agreed the result would be the same under the factor common to both standards—is the

---

[2756] Reno v. ACLU, 521 U.S. 844, 874 (1997).

[2757] *FW/PHS, Inc. v. Dallas*, 493 U.S. 215, (1990)("In Freedman, we determined that the following three procedural safeguards were necessary to ensure expeditious decisionmaking by the motion picture censorship board: (1) any restraint prior to judicial review can be imposed only for a specified brief period during which the status quo must be maintained; (2) expeditious judicial review of that decision must be available; and (3) the censor must bear the burden of proof once in court"), citing *Freedman v. Maryland*, 380 U.S. 51, 58-60 (1965).

[2758] *John Doe, Inc. v. Mukasey*, 549 F.3d 861, 876-77 (2d Cir. 2008) noting the government contentions based on *Seattle Times Co. v. Rhinehard*, 467 U.S. 20 (1984)(pre-trial discover); Douglas Oil Co. v. Petrol Stops Northwest, 441 U.S. 211 (1979)(grand jury); *Kamasinski v. Judicial Review Council*, 44 F.3d 106 (2d Cir. 1994)(judicial misconduct); United States v. Snepp, 897 F.2d 138 (4th Cir. 1990)(CIA employees); United States v. *Marchetti*, 466 F.2d 1309 (4th Cir. 1972)(same).

[2759] *Seattle Times Co. v. Rhinehard*, 467 U.S. at 32.

[2760] *John Doe, Inc. v. Mukasey*, 549 F.3d at 878.

restriction on expression narrowly tailored as possible to protect the governmental interest.[2761]

The government's interest in national security is indisputably compelling.[2762] Unwilling to read section 2709(c) procedure as a licensing scheme, the Second Circuit panel nevertheless concluded that "in the absence of Government-initiated judicial review, subsection 3511(b) is not narrowly tailored to conform to First Amendment protected standards."[2763] Moreover, the judicial review must be real. It must "place on the Government the burden to show a good reason to believe that disclosure may result in an enumerated harm, i.e. a harm related to an authorized investigation to protect against international terrorism or clandestine intelligence activities."[2764] Such judicial review may occur ex parte and in camera, but it may not be bound by the executive's conclusive certification of harm feature of section 3511. In the eyes of the court, there is no meaningful judicial review "of the decision of the Executive Branch to prohibit speech if the position of the Executive Branch that speech would be harmful is 'conclusive' on the reviewing court, absent only a demonstration of bad faith."[2765] "To accept deference to that extraordinary degree would be to reduce strict scrutiny to no scrutiny, save only in the rarest of situations where bad faith could be shown," it concluded.[2766]

Yet the court envisioned a procedure under which NSL secrecy provision might survive:

> *We deem it beyond the authority of a court to "interpret" or "revise" the NSL statutes to create the constitutionally required obligation of the Governmentto initiate judicial review of a nondisclosure requirement. However, the Government might be able to assume such an obligation without additional legislation....*
>
> *If the Government uses the suggested reciprocal notice procedure as a means of initiating judicial review, there appears to be no impediment to the Government's including notice of a recipient's opportunity to contest the nondisclosure requirement in an NSL. If*

[2761] *Id.*

[2762] *John Doe, Inc. v. Mukasey*, 549 F.3d at 878, citing *Haig v. Agee*, 453 U.S. 280, 307 (1981).

[2763] *John Doe, Inc. v. Mukasey*, 549 F.3d at 880-81.

[2764] *Id.* at 881.

[2765] *Id.* at 882.

[2766] *Id.*

> *such notice is given, time limits on the nondisclosure requirement pending judicial review, as reflected in Freedman, would have to be applied to make the review procedure constitutional. We would deem it to be within our judicial authority to conform subsection 2709(c) to First Amendment requirements, by limiting the duration of the nondisclosure requirement, absent a ruling favorable to the Government upon judicial review, to the 10-day period in which the NSL recipient decides whether to contest the nondisclosure requirement, the 30-day period in which the Government considers whether to seek judicial review, and a further period of 60 days in which a court must adjudicate the merits, unless special circumstances warrant additional time. If the NSL recipient declines timely to precipitate Government-initiated judicial review, the nondisclosure requirement would continue, subject to the recipient's existing opportunities for annual challenges to the nondisclosure requirement provided by subsection 3511(b). If such an annual challenge is made, the standards and burden of proof that we have specified for an initial challenge would apply, although the Government would not be obliged to initiate judicial review.*[2767]

Given the possibility of constitutional application, the court saw no reason to invalidate sections 2709(c) and 3511(b) in toto. The exclusive presumptions of section 3511 cannot survive, the court declared, but the First Amendment finds no offense in the remainder of the two sections except "to the extent that they fail to provide for Government-initiated judicial review. The Government can respond to this partial invalidation ruling by using the suggested reciprocal notice procedure."[2768]

On remand under the procedure suggested by the Court of Appeals, the government submitted the declaration of the senior FBI official concerning the continued need for secrecy concerning the NSL. Following an ex parte, in camera hearing, the district court concluded the government had met its burden, but granted the plaintiff's motion for a unclassified, redacted summary of the FBI declaration.[2769]

[2767] *Id.* at 883-84.

[2768] *Id.* at 884.

[2769] *Doe v. Holder*, _____ F.Supp.2d _____, _____ (2009 WL 2432320) (S.D.N.Y. Aug. 5, 2009).

TITLE 18: APPENDIX

Classified Information Procedures Act (18 U.S.C. Appx. §§ 1-16)

Classified Information Procedures Act (CIPA): An Overview, 89-172 (March 2, 1989).

LARRY M. EIG, CONGRESSIONAL RESEARCH SERV., CLASSIFIED INFORMATION PROCEDURES ACT (CIPA): AN OVERVIEW (1989), *available at* http://www.intelligencelaw.com/library/secondary/crs/pdf/89-172_3-2-1989.pdf.

Larry M. Eig
Legislative Attorney
American Law Division

March 2, 1989

The Congressional Research Service works exclusively for the Congress, conducting research, analyzing legislation, and providing information at the request of committees, Members, and their staffs.

The Service makes such research available, without partisan bias, in many forms including studies, reports, compilations, digests, and background briefings. Upon request, CRS assists committees in analyzing legislative proposals and issues, and in assessing the possible effects of these proposals and their alternatives. The Service's senior specialists and subject analysts are also available for personal consultations in their respective fields of expertise.

Summary

When a violation of criminal law potentially implicates sensitive national security concerns, the Executive Branch may face a dilemma of either declining to prosecute a violation of law or risking disclosure of sensitive materials during a criminal trial. Prior to 1980 it was particularly difficult to assess whether a successful prosecution could proceed without jeopardizing disclosure of sensitive information because the government had no means of determining the extent, nature, or relevance of classified information at issue prior to its introduction at trial. In 1980, however, Congress enacted the Classified Information Procedures Act (CIPA) to provide a means for determining at an early stage whether a "disclose or dismiss" dilemma exists in a potential prosecution or whether a prosecution may proceed that both protects information the Executive regards as sensitive to security and assures the defendant a fair trial consistent with the mandates of the Constitution.

Among its core provisions, CIPA initiates an early focus on security issues by requiring a defendant in a criminal case to notify the prosecution and the court prior to trial of any classified information that he reasonably expects to disclose in his defense. Also, the notice provision is a continuing one, and a defendant must provide a separate notice of any additional classified information that he becomes aware of after his initial notice and intends to use. A defendant may not introduce any classified information that was not included in a CIPA notice.

Issues on the use, relevance, and admissibility of classified information that either was included in a notice by the defendant or is expected to be used by the prosecution are considered by the court in pretrial hearings. Under current case law, the court to some degree may take national security interests into account in determining admissibility, If a court finds that certain classified information is admissible into evidence, the court then may consider a request by the government to substitute summaries or redacted documents in lieu of original documents, The court may authorize a substitution in such a case only when a substitution affords a defendant substantially the same opportunity to defend himself as introduction of the original documents would, Once a court makes its findings on what information must, in fairnesa to the defendant, be introduced, the Attorney General may file an objection to disclosure on national security grounds, and the prosecution thereafter must be partially or completely dismissed.

The courts generally have upheld CIPA to constitutional challenge and have enforced the sanctions set forth in the statute in appropriate cases. However, the judge in the Iran-Contra prosecutions has ruled that CIPA procedures must give way when they risk excessive exposure of the defendant's case, Thie ruling furthers a frequently made observation that CIPA ie most effective in resolving potentially troublesome cases in which the classified information at risk proves to be only marginally sensitive or marginally relevant, It remains problematic whether the disclose or dismiss dilemma posed by a prosecution involving sensitive information at its core can be resolved in a manner that preserves the rights of the defendant,

Classified Information Procedures Act (CIPA): An Overview

The Executive Branch of our Government has the authority to prosecute violations of federal criminal law.[2770] The Executive Branch also takes measures to protect information in its possession relating to national security and to prevent its disclosure.[2771] When a violation of criminal law potentially implicates sensitive national security concerns, the Executive thus may face a dilemma of

---

[2770] U.S. CONST. art. 2, § 3, cl. 3 (President to take care that the laws be faithfully executed).

[2771] Exec. Order No. 12356, 47 Fed, Reg. 14874, 15657 (1982).

either declining to prosecute a violation of law or risking disclosure of sensitive materials during a criminal trial.[2772] Prior to 1980 it was particularly difficult to assem whether a successful prosecution could proceed without jeopardizing disclosure of sensitive information because the government had no means of determining the extent, nature, or relevance of classified information at issue prior to its introduction at trial, In 1980, however, Congress enacted the Classified Information Procedures Act (CIPA)[2773] in order to provide a discrete and orderly framework for determining at an early stage whether a "disclose or dismiss" dilemma exists in a potential prosecution or whether a prosecution may proceed that both protects information the Executive regards as sensitive to security and assures the defendant a fair trial consistent with the mandates of the Constitution.

I. Legislative History of CIPA

During the 1970's the number of prosecutions in which the actual or prospective disclosure of classified information became an issue substantially increased and wae expected to increase further. [2774] The term "graymail" came into use to refer "to actions of a criminal defendant in seeking access to, revealing, or threatening to reveal classified information in connection with his defense."[2775] The problems that arose during this period from the inability to resolve issues relating to classified information prior to trial was described by Assistant Attorney General Philip Heymann as follows:

> *To fully understand the problem, it is necessary to examine the decision making process in criminal cases involving classified information. Under present procedures, decisions regarding the relevance and admissibility of evidence are normally made as they arise during the course of the trial. In advance of trial, the government often must guess whether the defendant will seek to disclose certain classified information and speculate whether it will be found admissible if objected to at trial. In addition, there is some question whether material will be disclosed at trial and the damage inflicted before a ruling on the use of the information can be obtained. The situation is further complicated in cases where the government expects to disclose some classified item in*

[2772] Criminal defendants enjoy a constitutional right to a public trial, U.S. CONST. amend. VI.

[2773] Pub. L. No. 96-456, *codified* at 18 U.S.C. App. IV.

[2774] *E.g*., H.R. Rep, No. 96-831, 96th Cong., 2d Sess. 7 (1980); see also Graymail Legislation: Hearings Before the Subcommittee on Legislation of the House Permanent Select Committee on Intelligence, 96th Cong,, 1st Sees, 4-5 (1979)(statement of Assistant Attorney General Philip Heymann).

[2775] H.R. Rep. No. 96-831 at 7.

presenting its case. Without a procedure for pre-trial rulings on the disclosure of classified information, the deck is stacked against proceeding with these cases because all of the sensitive items that might be disclosed at trial must be weighed in assessing whether the prosecution is sufficiently important to incur the national security risks.

In the past, the government has foregone prosecution of conduct it believed to violate criminal laws in order to avoid compromising national security information. The costs of such decisions go beyond the failure to redress particular instances of illegal conduct. Such determinations foster the perception that government officials and private persons with access to military or technological secrets have a broad de facto immunity from prosecution for a variety of crimes. This perception not only undermines the public's confidence in the fair administration of criminal justice but it also promotes concern that there is no effective check against improper conduct by members of our intelligence agencies.[2776]

Mr. Heymann's remarks were made in hearings on unauthorized disclosure of classified information conducted by a panel of the House Intelligence Committee in January 1979. During the previous year, a subcommittee of the Senate Select Committee on Intelligence had completed an extensive study of national security information and the administration of justice.[2777] In its subsequent report of its study, the subcommittee prefaced its detailed discussion and recommendations with the following observations on the difficulty of prosecuting national security cases:

The subcommittee discovered that enforcement of laws intended to protect national security information often requires disclosure of the very information the laws seek to protect. Indeed, the more sensitive the information compromised, the more difficult it becomes to enforce the laws that guard our national security. At times then, regardless of whether the compromise is to a

---

[2776] *Graymail Legislation: Hearings Before the Subcommittee on Legislation ofthe House Permanent Select Committee on Intelligence*, 96th Cong., 1st Sess. 4-6 (1979) (statement of Assistant Attorney General Philip Heymann).

[2777] Staff of the Subcommittee on Secrecy and Disclosure of the Senate Select Committee on Intelligence, 95th Cong., 2d Sess., National Security Secrets and the Administration of Justice (Comm. Print 1978)) [hereinafter cited as Senate Print]. Among the proceedings held during the study was The Use of Classified Information in Litigation: Hearings Before the Subcommittee on Secrecy and Disclosure of the Senate Select Committee on Intelligence, 95th Cong., 2d Sess. (1978).

> *newspaper reporter or directly to a foreign agent, the Government often must choose between disclosing classified information in a prosecution or letting the conduct go unpunished, In the words of one Justice Department official who testified before the subcommittee, To what extent must we harm the national security in order to protect the national security?"*[2778]

Subsequent discussion in the report further highlighted the conflicts that often exist within the Executive branch:

> *At the heart of this failure of enforcement is a very deep- seated conflict between the concerns of the intelligence community on the one hand, and the Department of Justice on the other in enforcing the espionage statutes, The conflict arises over whether publicly to disclose classified information necessary to conduct the investigation and to proceed with the prosecution. Indeed this question of whether or which classified information is to be used in a particular judicial proceeding is a pervasive problem that goes well beyond enforcement of the espionage statute.*[2779]

In light of the intrabranch conflict that it perceived to inhere in national security cases, many of the subcommittee's recommendations focused on actions within the Executive Branch, Among these recommendations were (1) development of administrative procedures for disciplining employees responsible for violations of security or other laws, (2) issuance of guidelines by the Attorney General regarding the responsibility of the intelligence community to report crimes, and (3) issuance of binding regulations by the Attorney General setting forth procedures for the provision by intelligence agencies of information relevant to criminal proceedings.[2780] Other recommendations of the subcommittee focused on suggestions for congressional legislation. Perhaps foremost among these recommendations were consideration of a special omnibus pretrial proceeding to be used in cases where national secrets were likely to arise.[2781]

In July 1979, three bills were introduced proposing procedures similar to those discussed in the report of the Senate subcommittee. These bills were H.R. 4736, the House Intelligence Committee bill; H.R. 4745, the Administration bill; and S. 1482, the Senate Judiciary Committee bill. The House bills were referred to both the House Intelligence Committee and the House Judiciary Committee. The

---

[2778] *Senate Print* at 1.

[2779] *Id*. at 6.

[2780] Id. at 31, 32.

[2781] *Id*. at 32.

Subcommittee on Legislation of the House Intelligence Committee held hearings on the two House bills in August and September of 1979.[2782] Using H.R. 4736 as its vehicle, the House Intelligence Committee favorably reported a classified information procedures bill March 18, 1980.[2783] The Subcommittee on Civil and Constitutional Rights of the House Judiciary Committee held further hearings on H.R. 4736 in April and May of 1980.[2784] On September 17, 1980, the Judiciary Committee also reported H.R. 4736 favorably with an amendment requiring that reports on prosecutions implicating national security and on the operation of the legislation be submitted to both the Intelligence and the Judiciary Committee.[2785] The bill subsequently passed the House by voice vote September 22, 1980, without further amendment as its version of S. 1482.[2786] In the Senate, S. 1482 had been referred to the Senate Judiciary Committee and reported to the full Senate June 18, 1980.[2787] The bill passed the Senate by voice vote without further amendment June 25.[2788] While the versions of S. 1482 that were passed by the respective Houses were substantially similar, several differences between them remained to be resolved at conference, Among these differences were the reach of the Act (as reflected in the definition of the type of information that would trigger the pretrial procedure process), the sequence of various presentations during the pretrial hearing, and the standard for allowing presentation of evidence at trial in an alternative form, The conference resolved these issues by adopting the broader Senate version of protected information, a hybrid two-stage hearing procedure, and the more restrictive House standard for allowing disclosure of alternative evidence.[2789]

II. Procedures for Assessing Classified Information

A. Pretrial Conference

[2782] *Graymail Legislation: Hearings Before the Subcommittee on Legislation of the House Permanent Select Committee on Intelligence*, 96th Cong., 1st Sess. (1979).

[2783] H.R. Rep. No. 96-831, Part 1, 96th Cong., 2d Sess. (1980).

[2784] Use of Classified Information in Federal Criminal Cases: Hearings Before the Subcommittee on Civil and Constitutional Rights of House Committee on the Judiciary, 96th Cong. 2d Sess. (1980).

[2785] H.R. Rep. No. 96-831, Part 2, 96th Cong., 2d Sess. (1980).

[2786] 126 Cong. Rec. H9311 (daily ed. September 22, 1980).

[2787] S. Rep. No. 96-823, 96th Cong., 2d Sess. (1980).

[2788] 126 Cong. S8195 (daily ed. June 25, 1980).

[2789] H.R. Rep. No. 96-1436, 96th Cong., 2d Sess. (1980).

CIPA was enacted October 15, 1980, as Public Law 96-456,[2790] The procedures that it sets forth for early resolution of security issues begin with the right of either party or the court to call at any time after indictment for a prompt pretrial conference on matters relating to classified information that may arise during the course of the prosecution.[2791] Among the matters addressed at a pretrial conference under CIPA are the timing of discovery, the provision by the defendant of the notice of intent to disclose classified information required elsewhere in CIPA, and the initiation of hearings to determine what classified information may be presented at trial.[2792] The court also may consider other matters relating to the conduct of the trial during the pretrial conference.[2793] An admission made by the defense during a pretrial conference may not be used against the defendant unless it is in writing and signed.[2794]

B. Pretrial Discovery

With respect to discovery, CIPA allows the United States to make an *ex parte* showing to the court seeking to limit the disclosure of classified information to the defendant during the course of discovery under the Federal Rules of Criminal Procedure.[2795] Upon a sufficient showing, the court may authorize the government to delete specified items of classified information from documents to be made available to the defendant, to substitute a summary of information in classified documents for the documents themselves, or to substitute a statement admitting relevant facts that the classified information being sought would tend to prove.[2796]

The courts have upheld the examination of documents ex parte during discovery under CIPA to constitutional challenge.[2797] Furthermore, the courts also have

---

[2790] 94 Stat. 2025, 18 U.S.C. App. IV.

[2791] CIPA, § 2.

[2792] *Id.*

[2793] *Id.*

[2794] *Id.*

[2795] CIPA, § 4.

[2796] *Id.*

[2797] *United States v. Jolliff*, 548 F. Supp. 229, 231-232 (D. Md. 1981). The Federal Rules of Criminal Procedure also provide for *ex parte* examinations. Fed. R. Crim. P. 6(d)(l). Nonetheless, *ex parte* discovery proceedings still are criticized, particularly with respect to determining in what form otherwise discoverable evidence will be presented to a defendant. *E.g.*, Tamanaha, *A Critical Review of the Classified Information Procedures Act*, 13 Am. J. Cr. L. 277, 306-315 (1986) [hereinafter Tamanaha].

recognized a qualified governmental privilege to withhold certain material during discovery in CIPA cases that is similar in scope to the privilege to withhold an informant's identity recognized by the Supreme Court in Rovario v. United SWS.[2798] In CIPA cases, the government may withhold classified information during discovery without an adverse effect on its prosecution unless the defendant can show that disclosure of the information being sought not only is relevant, but also is central to the defense or is essential to a fair determination of the case.[2799] Moreover, it should be recalled that even when classified information is held to be discoverable after applying a *Rovario*-type balancing test, a court, upon a proper *ex parte* showing, still may order the release of the information sought in an alternative form.[2800] Nonetheless, courts will disallow substitution for the original information sought where it finds the proposed substitution to be inadequate to protect the defendant's interests.[2801]

C. Defendant's Notice of Classified Information

One major innovation of CIPA is to require the defendant to provide formal written notice to the government and the court of an intent to disclose classified information.[2802] Under this requirement, if a defendant reasonably expects to disclose or cause the disclosure of classified information in any manner in connection with trial or pretrial proceedings, the defendant must give notice to the court and the government within a period of time specified by the court or, where no time is specified, within thirty days prior to trial.[2803] A notice of an intent to disclose must include a brief description of the information at issue. The notice requirement is a continuing one, and whenever the defendant learns of additional classified material that he may reasonably expect to introduce, he must provide additional notice to the government and the court, Once notice is given, the defendant may not disclose information known or believed to be classified until a hearing on its use has been held and an appeal, if any, has been completed. The court may prohibit the defendant from disclosing during criminal proceedings any classified information not included in a notice and may prohibit the defendant from examining any witness with respect to that information. On the other hand, because giving prior notice may put the defendant at an unfair disadvantage, the government must provide the defendant the information it

---

[2798] 353 U.S. 53 (1957).

[2799] *See, e.g.*, *United States v. Pringle*, 751 F.2d 419 (1st Cir. 1984). *See also United States v. Sarkissian*, 841 F.2d 959, 965 (9th Cir. 1988).

[2800] CIPA, § 4.

[2801] *E.g.*, *United States v. Clegg*, 740 F.2d 16, 18 (9th Cir. 1984).

[2802] CIPA, § 5.

[2803] CIPA, § 5(a).

expects to use to rebut the classified information in the notice whenever a court determines that the classified information in the notice may be disclosed during criminal proceedings. Failure by the government to provide rebuttal information may result in sanctions on the government similar to those that may be imposed upon a defendant for failure to give notice.

Various aspects of the notice requirement have been litigated before the United States district courts and courts of appeals.[2804] During the course of this litigation, the courts at times have imposed sanctions on defendants who failed to provide adequate notice and denied them opportunity to pursue certain issues at trial, Courts imposing sanctions have characterized defendant's pretrial notice as "the central document in CIPA,"[2805] explaining that "without sufficient notice that sets forth with specificity the classified information that the defendant reasonably believes necessary to his defense, the government is unable to weigh the costa of, or consider alternatives to, disclosure."[2806] Furthermore, the courta have upheld the notice requirement to constitutional challenge.[2807] The Supreme Court itself does not appear to have addressed the CIPA notice provision.[2808] It recently has, however, upheld a State Supreme Court rule that precluded the introduction of certain testimony because defendant had failed to comply with a pretrial disclosure requirement.[2809]

D. Hearings to Consider Classified Information

A pretrial notification by the defendant of an intent to introduce classified material would appear to be the primary means of alerting the court and other

---

[2804] *E.g., U.S. v. Badia*, 827 F.2d 1458 (llth Cir. 1987) (defendant's failure, despite government warning, to provide particularized notice of intent to disclose classified information held to preclude raising certain matters at trial even though the government may have had reason to believe that defendant intended to assert a defense implicating security matters); United States v. Wilson, 760 F.2d 7 (2d Cir. 1984) (notification requirement upheld to constitutional challenge based on fifth amendment); United Shtee v. Collins, 720 F.2d 1195 (llth Cir. 1983) (defendant's notice held to be too general to comply with CIPAJs requirement of a particularized notice setting forth specifically the classified information that may be disclosed); Unifed States v. Jollifi 648 F,Supp. 229 (D.Md, 1981) (notification requirement upheld to constitutional challenge).

[2805] *United States v. Collins*, 720 F.2d at 1199.

[2806] *United States v. Badia*, 827 F.2d at 1465. See also *United States v. Collins*, 720 F.2d at 1199-1200 (requiring defendant to state with particularity which items he reasonably expects to disclose in his defense).

[2807] *See United States v. Wilson*, 750 F.2d at 9 and cases cited therein.

[2808] *E.g*., 479 U.S. 839 (1986) *denying cert. to United States v. Wilson*, 750 F.2d 7 (2d Cir. 1984).

[2809] *Taylor v. Illinois*, __U.S.__, 108 S.Ct. 646 (1988) (defendant's constitutional right to present testimony in his own behalf held not to prevent absolutely a rule that bars testimony for failure to comply with pretrial disclosure rule when weighty countervailing public interests are at stake).

parties to a prospective classified information issue at trial. Presumably, classified information isaues also could arise in other ways. For example, matters possibly could arise during trial that implicate sensitive information that could not have reasonably been foreseen prior to trial to be at issue. Also, issues relative to the government's use of classified information in its case may remain to be resolved in a judicial context. This may be so even though in many national security prosecutions any intrabranch conflict over what materials may be revealed during a public trial consistent with security interests presumably is resolved prior to a decision by the Department of Justice to seek an indictment. For example, a decision on whether to go forward with a prosecution may depend upon a ruling by the court on whether certain information may be introduced in alternative form. In other situations--prosecutions after appointment of an independent counsel under the Title VI of the Ethics in Government Act of 1978,[2810] for example-- circumstances may militate against full resolution of security issues within the Executive Branch prior to bringing formal charges.

Regardless of how classified information issues arise, however, CIPA sets forth a hearing procedure for resolving them.[2811] The hearing procedure provided, conducted at an early stage and outside of trial, determines separately (1) whether the classified information sought to be used is admissible and therefore should be disclosed[2812] and, (2) if disclosure of particular information is authorized, in what form it may be introduced.[2813] An initial hearing on classified information may be requested by the government within a period specified by the court.[2814] At issue at the hearing are "all determinations concerning the use, relevance, or admissibility of classified information that would otherwise be made during the trial or pretrial proceeding,"[2815] Both the government and the defendant may participate in a hearing, even though the hearing is conducted *in camera* upon certification by the Attorney General.[2816] The government must notify the defendant as to what material is to be considered at the hearing.[2817]

[2810] 28 U.S.C. § 591 et seq.

[2811] CIPA, § 6.

[2812] CIPA, § 6(a).

[2813] CIPA, § 6(c).

[2814] CIPA, § 6(a).

[2815] Id.

[2816] Id.

[2817] CIPA, § 6(b).

This notification may describe the material by generic category only if the material has not previously been made available to the defendant?[2818]

When the government's request for a hearing is filed prior to a particular pretrial proceeding or trial, the court must rule prior to the commencement of further proceedings.[2819] The court must state in writing the basis of its determination concerning the use, relevance, or admissibility of each item of classified information.[2820] A finding that classified information may be disclosed may trigger the alternative disclosure procedures. If the court determines that specific classified information may be disclosed, the government may move that the court, in lieu of disclosure, order the substitution of a statement admitting relevant facts or of a summary of the information.[2821]

The court is required to authorize substitution upon finding, after a further hearing, that a statement or summary will provide the defendant "with

substantially the same ability to make his defense as would disclosure of the specific classified information."[2822] In connection with the motion for substitution, the government may submit an affidavit by the Attorney General explaining the basis for the classification of the information at issue and that disclosure of the information would cause identifiable damage to the national security.[2823] An affidavit filed by the Attorney General may be examined *ex parte*.[2824]

The court must order a defendant not to disclose otherwise admissible classified information whenever a substitution motion by the government is denied and the Attorney General files an additional affidavit with the court still objecting to the

---

[2818] Id.

[2819] CIPA,§ 6(a).

[2820] Id.

[2821] CIPA, § 6(c).

[2822] Id.

[2823] CIPA, § 6(c)(2).

[2824] Id.

disclosure of the classified information at issue.[2825] In such an event, the court must dismiss the prosecution unless the court finds that dismissal would not serve the interests of justice and orders other appropriate action in lieu of dismissal.[2826] Further appropriate action may include, but need not be limited to, dismissing specified counts only, finding against the government on issues to which the undisclosed information pertains, or striking or precluding specified testimony.[2827] An order dismissing a prosecution in whole or part or mandating other appropriate action may not take effect until after the government has had an opportunity to appeal the order and, if the appeal is unsuccessful, to withdraw its objection to disclosure.[2828] The government may appeal a decision authorizing disclosure or imposing sanctions for nondisclosure immediately.[2829] Such an interlocutory appeal must be considered by the court of appeals on an expedited basis.[2830]

Much of the litigation on the "use, relevance, and admissibility" stage of CIPA hearings has addressed the appropriate scope of inquiry at that point. More particularly, litigants have questioned whether the government's interest in protecting classified information may be taken into account in determining what evidence may be admitted into evidence at all or whether that interest may be taken into account only when determining what alternative form, if any, otherwise admissible information may be introduced. The lead case in the area is *United States v. Smith*.[2831] Smith, a former Army employee charged with eelling certain material to the Soviet Union, sought to introduce classified information to support his defense that he had believed he was participating in a CIA double agent operation when transferred the material at iseue. The district court and a panel of the court of appeals ruled that some of the information Smith sought to introduce was admissible because it wa relevant evidence under the Federal Rules of Criminal Procedures.[2832] According to these decisions, the government's interest in protecting classified information in the hands of the defendant is

---

[2825] CIPA, § 6(e)(l).

[2826] CIPA, § 6(e)(2).

[2827] Id.

[2828] Id.

[2829] CIPA, § 7.

[2830] Id.

[2831] *United States v. Smith*, 780 F.2d 1102 (4th Cir, 1984) (ruling 7-5 en bane); *United States v. Smith*, 750 F.2d 1215 (4th Cir. 1984); *United States v. Smith*, 592 F. Supp. 424 (E.D. Va. 1984).

[2832] *United States v. Smith*, 750 F.2d 1215 (4th Cir, 1984); *United States v. Smith*, 592 F. Supp. 424 (E.D. Va. 1984).

pertinent in CIPA hearing only at the stage of determining whether otherwise relevant information may be introduced in an alternative form. The court of appeals ruling en barn disagreed.[2833] It rather held that a *Rovario*-type balancing test was appropriate not only during discovery in classified information cases, but also during relevance, use, and admissibility hearings.[2834] This ruling thus allows the government to use national security interests to preclude the introduction of some classified information altogether, rather than be restricted to using those concerns only for the purpose of substituting alternative evidence. Nonetheless, even under this ruling, the defendant may be authorized to introduce classified material upon a showing that the material is "essential" or "necessary to the defense" and not "merely cumu1ative"nor "speculative.[2835] The en barn ruling in Smith has been followed in later cases."[2836]

There does not appear to be much reported litigation on the substitution procedures that follow a finding that classified information is relevant and admissible. However, even though the government may make a more complete and *ex parte* representation to the court at that stage on the sensitivity of the material at issue, it .may be difficult to convince a court that evidence already found during the first stage of hearings to be central to the defendant's case nevertheless must be admitted only in a substituted form, Again, CPA only permits a substitution to be made if it will leave the defendant with "substantially the same ability to make his defense."[2837]

At least one court has held that introduction of edited documents would be unfair to the defendant because of their diminished effect.[2838]

E. Other CIPA Provisions

In addition to the notification and hearing procedures for determining admissibility, CIPA sets forth separate standards governing the introduction of classified information into evidence. For example, CIPA states that a court may order that only part of a classified document or a redacted version of a classified document be introduced if admission of a complete document is unnecessary and

---

[2833] *United States v. Smith*, 780 F.2d 1102 (4th Cir. 1984) (ruling 7-5 en banc).

[2834] 780 F.2d at 1106-1110.

[2835] *See* 780 F.2d at 1110.

[2836] *E.g,, United States v. Zettl*, 835 F.2d 1059 (4th Cir, 1987).

[2837] CIPA, § 6(c).

[2838] *United States v. Clegg*, 846 F.2d 1221, 1224 (9th Cir. 1988).

consideration of an incomplete document is not unfair.[2839] Furthermore, the government may object to any question or line of inquiry that may require the witness to disclose classified information not previously found to be admissible. Following an objection by the government, the court is to determine whether a prospective response may be admitted without compromising classified information.[2840] Also, in an espionage or similar case requiring the government to prove that material relates to the national defense or constitutes classified information, CIPA requires the government to notify the defendant of the specific material it expects to rely upon to establish the national security element of the offense so that the defendant may have adequate time to prepare a defense.[2841]

Two provisions of CIPA require other branches of government to adopt procedures relating to classified and the courts. First, CIPA directs the Chief Justice of the United States, in consultation with the Attorney General, the Director of Central Intelligence, and the Secretary of Defense, to prescribe rules establishing procedures for the protection of classified information in the custody of the federal courts.[2842] Chief Justice Burger complied with this directive and issued security procedures February 12, 1981.[2843] Second, CIPA directs the Attorney General to issue guidelines specifying the factors to be used by the Department of Justice in deciding whether to undertake a prosecution in which classified information may be revealed.[2844] Third, CIPA further requires the Justice Department to prepare detailed written findings whenever it declines to prosecute a case pursuant to the guidelines.[2845] Decisions not to prosecute under the guidelines also must, "c]onsistent with applicable authorities and duties, including those conferred by the Constitution upon the executive and legislative branches," be reported by the Justice Department to the respective Intelligence Committees and Judiciary Committees.[2846]

[2839] CIPA, § 8(b).

[2840] Presumably these provisions primarily are intended to supplement the notice and hearing requirements that apply when a defendant has a reasonable expectation that classified information may be disclosed. In other words, the provisions appear primarily intended to cover those situations where the defendant does not have a reasonable expectation that classified information is implicated and does not realize that an answer to his inquiries may be classified.

[2841] CIPA, § 10.

[2842] CIPA, § 9.

[2843] CIPA, § 9 note.

[2844] CIPA, § 12(a).

[2845] CIPA, § 12(b).

[2846] CIPA, § 13.

III. Criticism and Recent Developments: Rulings in the Trial of Lt. Col. Oliver North

In their discussions of CIPA, courts and commentators have remarked that the Act is not intended to make substantive changes regarding defendants' rights and the use of classified information.[2847] Rather, according to these authorities, CIPA is intended only to put in place procedural rules that facilitate early rulings on the admissibility of classified information alleged to be at issue and on the acceptability of substitutions for evidence found to be both sensitive and admissible.[2848] At times, however, the procedural scheme set forth in CIPA itself may be seen as adversely affecting a defendant's rights, particularly where the defense expects to introduce a large amount of relevant classified information.

Orders of District Judge Gesell issued in the course of proceedings arising from the Iran-Contra affair illustrate how close adherence to CIPA may be seen ae compromising a defendant.[2849] The focus of the Iran-Contra affair are allegations that certain individuals secretly applied funds, including funds generated by a classified government effort to free Americans held in the Middle East, to various unauthorized purposes through deceiving Congress, obstructing investigations, and other unlawful means.[2850] Of the four individuals indicted so far through the Independent Counsel appointed to investigate these events, most of the CIPA litigation has concerned the prosecution of Lieutenant Colonel Oliver North. After observing that "the most sensitive information and most critical national security intelligence methods and sources available to the government" appeared to be "inextricably enmeshed in the events challenged by the indictment [of Lt. Col. North]," Judge Gesell stated the following regarding the application of CIPA:

> *It will be impossible to conduct this case under the precise strictures of CPA, not only because of this broad intrusion into classified areas of information but also because it is impossible in advance to determine and correctly rule on all issues of relevance, materiality and admissibility. It probably was never contemplated that classified information problems of this magnitude would be presented to a trial judge in a case ...*
>
> ...

[2847] *Eg., United States v, Smith*, 780 F.2d at 1106 (majority opinion), 1112 (dissent); *Tamamha, supra* n.28, at 294.

[2848] Id.

[2849] *United Stubs v. Poindexter*, 698 F. Supp. 316 (D.D.C. 1988); *Unites States v. North*, 698 F. Supp. 323 (D.D.C. 1988).

[2850] 698 F. Supp, at 302.

> *[In enacting CIPA Congress] emphasized that the Court should not undertake to balance the national security interests of the government against the rights of the defendant but rather that in the end remedies and sanctions against the government must be designed to make the defendant whole again. Thus while a limited opportunity for creative judicial adjustment of CIPA procedures exists, in the end, defendant's constitutional rights must control.*
>
> *. . . Counsel for North has urged that strict application of CIPA will force North to reveal to the government well in advance his strategy, his evidence, and, indeed, even aspects of his defense. . . . This, it is argued with considerable force, will place North at a practical and tactical disadvantage, infringing upon his constitutional rights under the Fifth and Sixth Amendments. . . . The Court has determined that many of these concerns can hopefully be avoided by applying pretrial procedures consistent with the congressional intent underlying CIPA. A way must be found to preserve defendant's constitutional rights that still affords adequate protection for national security concerns.*[2851]

Judge Gesell thus saw his task not as applying CIPA, which he believed would infringe upon the rights of Lt. Col. North, but rather as trying to at least preserve the spirit of CIPA by fashioning procedures that were tailored to the needs of the case before him. The procedure subsequently outlined by Judge Gesell largely followed the notice provisions in CIPA but differed from CIPA in the diminished role given to the prosecution and, to a lesser degree, the court during pretrial review of material intended to be used by the defense. Rather than determining use and relevance issues at hearings where the prosecution was to be present, as is the case under CIPA, Judge Gesell set out a procedure under which the court and the defense alone were to meet concerning the use and relevance of item contained in the notice given by the defense. At these ex prte meetings, the judge was to actively explore with defense counsel possible substitutions for the classified information sought to be introduced, After the court, without divulging defeme strategy, then ruled on the relevance and materiality of the remaining classified documente contained in the defense's notice, the court was to notify the interagency hkforce that was determining which documents could be released for the purpose of having these remaining documents reviewed, Only then could the prosecuting Independent Counsel become actively involved in examining materials in the defense's case, and this participation was limited to seeking substitutions for documents found by the taskforce to be too sensitive for full disclosure, Beyond reviewing classified documents contained in the defense's notice, Judge Gesell refused to consider in advance the subjects to be covered in the defense's opening statement or in the testimony of the defense witnesses,

---

[2851] 698 F. Supp. at 319, 320, 321.

including the defendant's. Judge Gesell also gave the defense broad rights to discover information redacted in documents intended to be used by the prosecution.[2852]

IV. Conclusion

In ruling that CIPA procedures must give way when they risk excessive exposure of the defendant's case, Judge Gesell highlights the limited efficacy of CIPA in highly sensitive cases. Judge Gesell's opinion suggests that the more a defendant relies on sensitive information, the more difficult it is to fashion procedures for resolving security issues. Furthermore, CIPA never has been seen as assuring that all security issues could be resolved. Rather CIPA is most effective as a means for resolving potentially troublesome cases in which the classified information at risk proves to be only marginally relevant or marginally sensitive. It remains problematic whether the disclose or dismiss dilemma posed by a prosecution involving sensitive information at its core can be resolved in a manner that preserves the rights of the defendant.

[2852] 698 F. Supp. at 321-322.

TITLE 47: TELEGRAPHS, TELEPHONES, AND RADIOTELEGRAPHS

47 U.S.C. Chapter 9: Interception of Digital and Other Communications (47 U.S.C. §§ 1001-1021)

Digital Surveillance: The Communications Assistance for Law Enforcement Act, RL30677 (June 8, 2007).

PATRICIA MOLONEY FIGLIOLA, CONGRESSIONAL RESEARCH SERV., DIGITAL SURVEILLANCE: THE COMMUNICATIONS ASSISTANCE FOR LAW ENFORCEMENT ACT (2007), *available at* http://www.intelligencelaw.com/library/secondary/crs/pdf/RL30677_6-8-2007.pdf.

Order Code RL30677
Updated June 8, 2007

Patricia Moloney Figliola
Specialist in Telecommunications and Internet Policy
Resources, Science, and Industry Division

Summary

The Communications Assistance for Law Enforcement Act (CALEA, P.L. 103414, 47 U.S.C. 1001-1010), enacted October 25, 1994, is intended to preserve the ability of law enforcement officials to conduct electronic surveillance effectively and efficiently despite the deployment of new digital technologies and wireless services that have altered the character of electronic surveillance. CALEA requires telecommunications carriers to modify their equipment, facilities, and services, wherever reasonably achievable, to ensure that they are able to comply with authorized electronic surveillance actions.

Since 2004, the Federal Communications Commission (FCC) has been considering a number of questions as to how to apply CALEA to new technologies, such as Voice over Internet Protocol (VoIP). In August 2005, in response to a March 2004 petition by a group of law enforcement agencies, the FCC released a Notice of Proposed Rulemaking and Declaratory Ruling which required providers of certain broadband and interconnected VoIP services to accommodate law enforcement wiretaps. The FCC found that these services could be considered replacements for conventional telecommunications services already subject to wiretap rules, including circuit-switched voice service and dial-up Internet access. The Order is limited to facilities-based broadband Internet access service providers and VoIP providers that offer services that use the public switched telephone network ("interconnected VoIP providers).

In May 2006, the FCC addressed several outstanding issues regarding CALEA implementation. Among other clarifications, the FCC (1) affirmed its May 14, 2007 compliance deadline for facilities-based broadband Internet access and interconnected VoIP services, and clarified that the date applied to all such providers; (2) explained that the FCC does not plan to intervene in the standards-setting process in this matter; (3) permitted telecommunications carriers the option of using Trusted Third Parties to assist in meeting their CALEA obligations; (4) restricted the availability of compliance extensions to equipment, facilities, and services deployed prior to October 25, 1998; (5) found that the FCC may enforce action under section 229(a) of the Communications Act against carriers that fail to comply with CALEA; and (6) concluded that carriers are responsible for CALEA development and implementation costs for post-January 1, 1995, equipment and facilities, and declined to adopt a national surcharge to recover CALEA costs.

In June 2006, the United States Court of Appeals for the District of Columbia Circuit affirmed the FCC's decision concluding that VoIP and facilities-based broadband Internet access providers have CALEA obligations similar to those of telephone companies.

Background

In the early 1990s the Federal Bureau of Investigation (FBI) asked Congress for legislation to assist law enforcement agencies to continue conducting electronic surveillance. The FBI argued that the deployment of digital technologies in public telephone systems was making it increasingly difficult for law enforcement agencies to conduct electronic surveillance of communications over public telephone networks. As a result of these arguments and concerns from the telecommunications industry,[2853] as well as issues raised by groups advocating protection of privacy rights,[2854] the Communications Assistance for Law Enforcement Act (CALEA) was enacted on October 25, 1994 (47 U.S.C. 1001-1021), in the final days of the 103rd Congress.

CALEA is intended to preserve the ability of law enforcement officials to conduct electronic surveillance effectively and efficiently, despite the deployment of new digital technologies and wireless services by the telecommunications industry.

[2853] In this report, the telecommunications industry includes common carrier telephone companies, mobile wireless telecommunications providers, telecommunications equipment manufacturers, and other entities that provide telecommunications services to the public.

[2854] Privacy rights groups involved in the CALEA debate include the Electronic Privacy Information Center, the Electronic Frontier Foundation, advocacy groups which both support on-line privacy rights of individuals, the Center for Democracy and Technology, which also advocates electronic privacy (and is funded primarily by the telecommunications, computer, and media industries), and the American Civil Liberties Union (ACLU), which represents a broad array of civil rights based on the First and Fourth Amendments.

CALEA requires telecommunications carriers to modify their equipment, facilities, and services to ensure that they are able to comply with authorized electronic surveillance. These modifications were originally planned to be completed by October 25, 1998. Since that time, the Federal Communications Commission (FCC) issued two additional orders establishing June 30, 2002, as the date by which telecommunications carries must have upgraded all their systems.[2855] Equipment manufacturers have fulfilled their obligation to provide CALEA solutions and carriers are implementing them. The FBI and FCC continue to monitor and review the implementation of this program.

Some Technical Terms

As a result of the revolution in digital technology in telecommunications, the process of wiretapping and other electronic surveillance has become more complex, and legal ambiguities have been introduced. As a background to understanding the problems associated with CALEA implementation, the definitions of several terms are necessary. Electronic surveillance refers to either the interception of communications content (as in a conversation) also known as wiretapping, or the acquisition of call-identifying information (the number dialed). The latter activity is accomplished through the use of pen register devices, which capture call-identifying information for numbers of outgoing calls from the location of lawful interception, and traps and traces, which capture information for numbers received at the location of lawful interception, much like consumer caller ID systems. Under current federal law, law enforcement (i.e., police or the FBI) must obtain a court order before conducting any of these activities. However, a wiretap requires a higher "evidentiary burden" than a pen register or trap and trace, including showing that there is probable cause for believing that a person is committing one of a list of specific crimes.[2856]

Under traditional analog technology, it was easy to separate the above categories of electronic surveillance. However, the advent of digital signal transmission technologies has made that distinction less clear. Information signals (voice or data) can be transmitted over telephone networks in one of two ways: circuit-switched and packet-switched modes.[2857] In circuit-switched systems, a communications path is established between the parties and dedicated

---

[2855] United States Department of Justice, Federal Bureau of Investigation, Communications Assistance for Law Enforcement Act, Eighth Annual Report to Congress, November 30, 2002 (Eighth Annual Report), pp. 7-9.

[2856] See CRS Report 98-326, Privacy: An Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping, by Gina Stevens and Charles Doyle.

[2857] Switches are network devices that select a path or circuit for sending data to its next destination over the telephone network. Switches may also include functions of the router, a device also used in computer networks, that determines the route and adjacent network point for data to be sent.

exclusively to one conversation for the duration of the call. In packet-switched systems, the information is broken down into smaller pieces called "packets"using a digital process. Each packet contains a small part of the message content along with call-identifying information called a "header" that indicates the origination and destination points of the information. Each packet is transmitted separately and is reassembled into the complete message at the destination point.

The packet-switched mode is the signal transmission technology used in all Internet communications. Packet switching is considered a more efficient use of a network than circuit switching because the same line can be used for multiple communications simultaneously. Although the circuit-switched mode was historically used in all voice telephone calls, the packet-switched mode is increasingly being used for voice and data transmissions over telephone networks.

CALEA's Main Provisions

CALEA requires telecommunications carriers to assist law enforcement in performing electronic surveillance on their digital networks pursuant to court order or other lawful authorization. The telecommunications industry, privacy rights groups, and law enforcement agencies agree that CALEA was not intended to expand law enforcement's authority to conduct electronic surveillance. On the contrary, CALEA was intended only to ensure that after law enforcement obtains the appropriate legal authority, carriers will have the necessary capabilities and sufficient capacity to assist law enforcement in conducting digital electronic surveillance regardless of the specific telecommunications systems or services deployed.

CALEA (47 U.S.C. 1002) directs the telecommunications industry to design, develop, and deploy solutions that meet certain assistance capability requirements for telecommunications carriers to support law enforcement in the conduct of lawfully-authorized electronic surveillance. Pursuant to a court order or other lawful authorization, carriers must be able, within certain limitations, to: (1) expeditiously isolate all wire and electronic communications of a target transmitted by the carrier within its service area; (2) expeditiously isolate call-identifying information that is reasonably available on a target; (3) provide intercepted communications and call-identifying information to law enforcement; and (4) carry out intercepts unobtrusively, so targets are not made aware of the electronic surveillance, and in a manner that does not compromise the privacy and security of other communications.

To allow carriers to give law enforcement the means to conduct its wiretaps, CALEA (47 U.S.C. 1003) requires the Attorney General to determine the number of simultaneous interceptions (law enforcement agencies' estimate of their maximum capacity requirements) that telecommunications carriers must be able to support.

To maintain privacy rights of individuals, CALEA (47 U.S.C. 1004) requires telecommunications carriers to ensure that any interception of communications or access to call-identifying information that is conducted within their premises can only be done with a court order. It also requires the specific intervention of an officer or employee of the carrier acting in accordance with regulations prescribed by the Federal Communications Commission (FCC).

CALEA (47 U.S.C. 1005) directs telecommunications carriers to consult with telecommunications equipment manufacturers to develop equipment necessary to comply with the capability and capacity requirements identified by the FBI. For efficient industry-wide implementation of the above requirements, CALEA (47 U.S.C. 1006) directs the law enforcement community to coordinate with the telecommunications industry and state utility commissions to develop suitable technical standards and establish compliance dates for equipment. In its *Eighth Annual Report*, the FBI stated that, "to date, most manufacturers have either complete, or nearly complete, CALEA solutions available for their carrier customers."[2858]

CALEA (47 U.S.C. 1008) gives the Attorney General, subject to the availability of appropriations, authority to pay telecommunications carriers for all reasonable costs directly associated with the modifications performed by carriers in connection with equipment, facilities, and services installed or deployed on or before January 1, 1995 (known as the "grandfather" date).

Major Events Following Enactment of CALEA

Initial Delays

CALEA gave implementation responsibility to the Attorney General, who, in turn, delegated the responsibility to the FBI. The FBI leads that nationwide effort on behalf of federal, state, and local law enforcement agencies. FBI officials initially anticipated that it would take a year for a standard to be developed and agreed upon by law enforcement, the telecommunications carriers, and the equipment manufacturers. Telecommunications consultants estimated that it would take the industry another three years to design, build and deploy new systems to comply with CALEA. Instead, industry and law enforcement became involved in a protracted dispute over what should be required for law enforcement's wiretapping capabilities.

By March 1997, the completion of the capability standard was overdue by 16 months. The FBI attempted to expedite the industry's implementation of CALEA by releasing regulations that included a cost recovery plan for the federal government's payment of costs associated with CALEA, as well as capability and

[2858] Eighth Annual Report, p. 5.

capacity requirements for the industry to meet. The plan required more extensive upgrades to networks than the telecommunications industry believed were necessary for law enforcement to preserve its wiretapping capabilities. Industry groups and privacy advocates disputed the FBI's plan. They argued that the FBI was attempting to expand its surveillance capabilities beyond the congressional intention of CALEA, and was attempting to unfairly shift costs and accountability away from the federal government onto private industry. Furthermore, the industry argued that, without an adopted capability standard, it could not begin designing, manufacturing, and purchasing the equipment to achieve CALEA compliance.

In December 1997, the Telecommunications Industry Association (TIA, representing telecommunications equipment manufacturers) adopted, over the objections of the law enforcement community, a technical standard, J-STD-025, also known as the "J-standard." This standard prescribes upgrades to network devices to meet CALEA's assistance capability requirements for local exchange, cellular, and broadband personal communications services (PCS). Although the FBI claimed that the J-standard did not provide all of the capabilities needed, the industry asserted that CALEA's language stated that telecommunications carriers would be compliant if they met publicly available standards adopted by the industry.

Privacy rights groups, on the other hand, protested two aspects of the J-standard that they asserted would make information beyond what is legally required available to law enforcement. One was a feature enabling the telecommunications network to provide location information for users of mobile wireless telecommunications services. The location information protocols in J-STD-025 allow law enforcement agencies to obtain information on the physical location of the nearest cell site (i.e., the receiver/transmitter antenna and base station) of mobile phone handsets at the beginning and end of each call. Wireless carriers are now deploying another technology (called triangulation) that will enable the carriers, and law enforcement, to track wireless telephone users more precisely, potentially within a few meters. The other was a feature enabling the network to access packet-mode data from telephone calls using more advanced systems. Privacy rights groups argued that these capabilities would violate the Fourth Amendment rights of individuals against unreasonable searches and seizures. Despite these objections, telecommunications manufacturers began designing new switches and upgrades to existing switches according to the J-standard.

Currently, equipment manufacturers have successfully incorporated the J-standard into their new equipment and carriers are now well underway with their efforts to upgrade their systems.

The FBI's "Punch List"

In the negotiations to develop the J-standard, TIA had refused to include some of the capabilities that law enforcement officials claimed they needed to facilitate

digital wiretapping. As a result, in March 1998, the FBI petitioned the FCC to require the telecommunications industry to adopt eleven additional capabilities. Industry and privacy rights groups protested that the FBI's plan would unlawfully expand enforcement capabilities. Eventually, the "punch-list"[2859] included the following six[2860] items:

- Content of subject-initiated conference calls — Would enable law enforcement to access the content of conference calls supported by the subject's service (including the call content of parties on hold).
- Party hold, join, drop — Messages would be sent to law enforcement that identify the active parties of a call. Specifically, on a conference call, these messages would indicate whether a party is on hold, has joined or has been dropped from the conference call.
- Subject-initiated dialing and signaling information — Access to all dialing and signaling information available from the subject would inform law enforcement of a subject's use of features (such as the use of flash-hook and other feature keys).
- In-band and out-of-band signaling (notification message) — A message would be sent to law enforcement whenever a subject's service sends a tone or other network message to the subject or associate (e.g., notification that a line is ringing or busy).
- Timing information — Information necessary to correlate call-identifying information with the call content of a communications interception.
- Dialed digit extraction — Information would include those digits dialed by a subject after the initial call setup is completed.[2861]

Capacity Requirements

The FBI's subsequent implementation actions were also opposed by the telecommunications industry. In March 1998, the FBI announced its estimated capacity requirements for local exchange, cellular, and broadband PCS.[2862] The industry protested the FBI's estimates, arguing that it would require telephone carriers to accommodate thousands of wiretaps simultaneously, an impractical and unnecessary burden. In July 1998, the FBI developed guidelines and procedures to facilitate small carrier compliance with its capacity requirements,

---

[2859] The "punch list" was named as such by the telecommunications industry, which believed the FBI was improperly forcing industry to comply with the FBI's requirements.

[2860] The additional capabilities originally requested by the FBI that were not included were: standardized delivery interface; separated delivery, surveillance status; continuity check tone (c-tone); and feature status.

[2861] Federal Register 63 page 63639, FCC, Further Notice of Proposed Rulemaking, November 16, 1998.

[2862] Federal Register 63, page 12217, FBI, Final Notice of Capacity, March 12, 1998.

and asked carriers to identify any systems or services that did not have the capacity to accommodate those requirements. In December 1998, the FBI began a proceeding to develop capacity requirements for services other than local exchange, cellular, and broadband PCS, asked additional questions of interested parties in June 2000.[2863] These technologies and services included paging, mobile satellite services, specialized mobile radio, and enhanced specialized mobile radio. To date, the proceeding is still pending.

Previous FCC Actions

As a result of petitions from the industry and the FBI, the FCC became involved in the implementation of CALEA. In October 1997, the FCC released its first Notice of Proposed Rule Making (NPRM) on CALEA implementation.[2864] The NPRM sought comments from interested parties regarding a set of policies and procedures proposed by the FCC for telecommunications carriers to follow. The proposed procedures would (1) preclude the unlawful interception of communications, (2) ensure that authorized interceptions are performed, (3) maintain secure and adequate records of any interceptions, and (4) determine what entities should be subject to these requirements, whether the requirements are reasonable, and whether to grant extensions of time for compliance with the requirements.

In response to the NPRM, telecommunications carriers, privacy rights groups, and the FBI submitted comments to the FCC to attempt to influence the final decision. Then, in April 1998, the FCC released a Public Notice requesting comments on issues raised in those petitions concerning the dates that carriers were required to comply with CALEA and the dispute over the J-standard. Based on comments it received, the FCC extended the implementation deadline until June 30, 2000, stating that without a standard, the necessary equipment would not be available in time.[2865]

In October 1998, the FCC initiated a proceeding to review the technical capabilities prescribed by the J-standard.[2866] The goal of that proceeding was to determine whether telecommunications carriers should be required under CALEA to meet the FBI's "punch list" items. The FCC addressed these issues in

---

[2863] Federal Register 63, page 70160, FBI Notice of Inquiry, December 18, 1998, and Federal Register 65, page 40694, FBI Further Notice of Inquiry, June 30, 2000.

[2864] FCC NPRM CC Docket No. 97-213, FCC Record 97-356, released October 10, 1997.

[2865] FCC Memorandum Opinion and Order in the Matter of Petition for the Extension of the Compliance Date under Section 107 of CALEA, released September 11, 1998.

[2866] FCC Proposes Rules to Meet Technical Requirements of CALEA. Report No. ET 98-8. FCC News, October 22, 1998.

several documents released over the following year. In March 1999, the FCC's First Report and Order established the minimum capability requirements for telecommunications carriers to comply with CALEA.[2867] Telecommunications carriers were required to ensure that only lawful wiretaps occur on their premises and that the occurrence of wiretaps is not divulged to anyone other than authorized law enforcement personnel. On August 2, 1999, the FCC decided to allow carriers to decide how long they would maintain their records of law enforcement's wiretap, pen register, and trap and trace interceptions.[2868] On August 31, 1999, the Second Report and Order established a definition for "telecommunications carrier" to include all common carriers, cable operators, electric and other utilities that offer telecommunications services to the public, commercial mobile radio services, and service resellers.[2869] The definition did not include Internet service providers (ISPs), which were explicitly excluded under the CALEA statute.

The FCC's Third Report and Order, released August 31, 1999, adopted technical requirements for wireline, cellular, and broadband PCS carriers to comply with CALEA requirements.[2870] The ruling adopted the J-standard, including the two capabilities that were opposed by the privacy rights groups (i.e., the ability to provide location information and packet-mode data to law enforcement). As described above, the FCC also adopted six of the punch list capabilities requested by the FBI to be implemented by telecommunications carriers. The Order required all aspects of the J-standard except for the packet-mode data collection capability to be implemented by June 30, 2000. The Order required carriers to comply with the packet-mode data capability and the six punch list capabilities by September 30, 2001.[2871] (The FCC ultimately extended the date by which all telecommunications carriers must have upgraded their systems to June 30, 2002.[2872])

On April 9, 2001, the FCC adopted its Second Order on Reconsideration,[2873] which clarified the arrangements telecommunications carriers must make to

---

[2867] FCC 99-11, Report and Order CC Docket No. 97-213, released March 15, 1999.

[2868] FCC 99-184, Order on Reconsideration, CC Docket No. 97-213, released August 2, 1999.

[2869] FCC 99-229, Second Report and Order, CC Docket No. 97-213, released August 31, 1999.

[2870] FCC 99-230, Third Report and Order, CC Docket No. 97-213, released August 31, 1999.

[2871] FCC Sides with FBI on Tapping, Wired News, August 27, 1999, [http://www.wired.com/news].

[2872] FCC Pubic Notice DA 02-270, released March 26, 2002.

[2873] Federal Register 66, page 22446, FCC, Second Order on Reconsideration, CC Docket No. 97-213, May 4, 2001.

ensure that law enforcement agencies can contact them when necessary, and the interception activity that triggers a record-keeping requirement.

In September 2001, FCC released a tandem Order[2874] and Public Notice[2875] on CALEA implementation. In the Order, the Commission extended until November 19, 2001, the deadline by which wireline, cellular, and broadband personal communications services (PCS) carriers must implement a packet-mode communications electronic surveillance capability, or to seek individual relief under section 107(c) of CALEA. The notice explained the petitioning process for telecommunications carriers seeking relief under section 107(c) for an extension of the new compliance deadline with respect to packet-mode communications, as well as other safe harbor standards.

Finally, on April 11, 2002, the FCC released an Order on Remand,[2876] which responded to a decision issued by the United States Court of Appeals for the District of Columbia Circuit[2877] vacating four of the punch list electronic surveillance capabilities mandated by the Third Report and Order in this proceeding. The FCC found that all of the capabilities were necessary and authorized by CALEA and had to be provided by wireline, cellular, and broadband PCS telecommunications carriers by June 30, 2002. The FCC also required that two additional punch list capabilities that were mandated by the Third Report and Order, but not reviewed by the Court of Appeals be provided by that same date.

The FCC granted preliminary extensions to requesting carriers with respect to punch list implementation that will expire on June 30, 2004. It granted preliminary extensions in connection with "packet" services that had been scheduled to expire on November 19, 2003, but that date was further extended to January 30, 2004. No further action with respect to that extension has been taken.

Government Activity: 2004 - Present

The FBI and other law enforcement agencies, the FCC, and Congress are all concerned with CALEA-related issues, particularly with respect to packet-based services (i.e., voice over Internet Protocol [VoIP]) and "push-to-talk" services offered by wireless providers.

[2874] Federal Register 66, page 50841, FCC, Order, CC Docket No. 97-213, October 5, 2001.

[2875] FCC Pubic Notice DA 01-2243, released September 28, 2001.

[2876] Federal Register 67, page 21999, Order on Remand, CC Docket No. 97-213, May 2, 2002.

[2877] See United States Telecom. Association v. FCC, 227 F.3d 450 (D.C. Cir. 2000), available at [http://www.fcc.gov/ogc/documents/opinions/2000/99-1442.html].

FBI Activity

The FBI has remained active in promoting its positions related to its CALEA powers.

Comments to the FCC's Wireless Broadband Task Force Report

On April 22, 2005, the DOJ filed comments on the FCC's Wireless Broadband Task Force Report,[2878] requesting that the FCC "continue to preserve the vital national security and criminal law enforcement capabilities of CALEA as it develops a deregulatory framework for wireless broadband Internet access services." Reply comments in the proceeding were due May 23, 2005.

Notice of Information Collection Under Review

On April 13, 2005, the FBI published a 60-day Notice of Information Collection Under Review.[2879] The notice announced a CALEA Readiness Survey program, which seeks to evaluate the effectiveness of CIU programs for implementing CALEA solutions in the Public Switched Telephone Network. Comments in this proceeding were accepted until June 13, 2005.

Petition for Declaratory Ruling

On March 10, 2004, the FBI, the Department of Justice (DOJ), and the Drug Enforcement Administration petitioned the FCC to identify additional telecommunications services not identified specifically within CALEA that should be subject to it.[2880] The services named in the FBI petition include some now considered beyond the scope of CALEA by many observers, including services that fall under the FCC's definition of "information services" under the Communications Act of 1934. However, CALEA provides the FCC a broader framework to determine that a service is a "telecommunications service." Comments and replies to the petition were due April 12 and April 27, 2004, respectively. The FCC ruled on this Petition on August 5, 2005, discussed below (See "FCC Action," page 10).

Inspector General Report

[2878] GN Docket No. 04-163. Additional information on this topic can be found online at the FCC's website at [http://www.fcc.gov/wbatf].

[2879] 70 Fed. Reg. 19,503 (2005). This document is available online at [http://www.askcalea.net/docs/20050413_70fr19503.pdf].

[2880] Joint Petition for Expedited Rulemaking of United States Department of Justice, Federal Bureau of Investigation, and Drug Enforcement Administration, RM-10865, March 10, 2004.

The FBI's Inspector General issued a report in April 2004 on CALEA implementation.[2881] In its report, the IG expressed concern over the cost estimates for obtaining CALEA compliance, which have varied widely. Industry has stated it believes estimates full compliance will cost approximately $1.3 billion; the FBI has estimated costs in the range of $500 million to $1 billion. Further, in December 2003, the FBI estimated that an additional $204 million would be necessary to complete deployment of CALEA. The IG stated in its report that it did not believe implementation costs could be determined with any degree of specificity, but that it was unlikely CALEA could be implemented with the $49.5 million that remains unobligated from current funding.

FCC Activity

In response to law enforcement's petition and after considering the comments and replies from interested parties, the FCC released an NPRM and Declaratory Ruling on August 4, 2004.[2882] Additionally, the FCC has issued two Orders in this matter.

Declaratory Ruling

In the Declaratory Ruling accompanying the NPRM, the FCC clarified that commercial wireless "push-to-talk" services are subject to CALEA, regardless of the technologies that wireless providers choose to apply in offering them.

First Report and Order

On August 5, 2005, the FCC ruled that providers of certain broadband and interconnected VoIP services must accommodate law enforcement wiretaps.[2883] The FCC found that these services can be considered replacements for conventional telecommunications services currently subject to wiretap rules, including circuit-switched voice service and dial-up Internet access. As such, the new services are covered by CALEA, which requires the FCC to preserve the ability of law enforcement to conduct wiretaps as technology evolves. The rules

---

[2881] U.S. Department of Justice, Office of the Inspector General of the, entitled "Implementation of the Communications Assistance for Law Enforcement Act by the Federal Bureau of Investigation," available at [http://www.usdoj.gov/oig/reports/FBI/ a0419/index.htm], April 7, 2004.

[2882] In the Matter of Communications Assistance for Law Enforcement Act and Broadband Access and Services, Notice of Proposed Rulemaking and Declaratory Ruling, FCC 04-187, ET Docket 04-295, RM-10865, adopted August 4, 2004, released August 9, 2004. Available online at [http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-04-187A1.pdf]. See also Federal Register 69, page 56976.

[2883] In the Matter of Communications Assistance for Law Enforcement Act and Broadband Access and Services, First Report and Order and Further Notice of Proposed Rulemaking, FCC 05-153, ET Docket 04-295, RM-10865, adopted August 5, 2005, released September 23, 2005. Available online at [http://hraunfoss.fcc.gov/edocs_public/attachmatch/ FCC-05-153A1.pdf].

are limited to facilities-based broadband Internet access service providers and VoIP providers that offer services permitting users to receive calls from, and place calls to, the public switched telephone network — these providers are called interconnected VoIP providers.

In making its ruling, the FCC found that the definition of "telecommunications carrier" in CALEA is broader than the definition of that term in the Communications Act and can, therefore, include providers of services that are not classified as telecommunications services under the Communications Act. CALEA contains a broader definition of telecommunications provider that authorizes the FCC to classify an entity a telecommunications carrier if it finds that such service is a replacement for a substantial portion of the local telephone exchange.

The FCC established a deadline of 18 months from the effective date of the Order for providers to achieve full compliance and adopted a Further Notice of Proposed Rulemaking to seek more information about whether specific classes of facilities-based broadband Internet access providers should be exempt from CALEA (i.e., small and rural providers and providers of broadband networks for educational and research institutions).

A coalition of organizations filed a Petition for Review with the United States Court of Appeals for the District of Columbia Circuit on October 25, 2005.[2884] Specifically, the "petitioners seek relief from the Order on the grounds that it exceeds the Commission's statutory authority and is arbitrary, capricious, unsupported by substantial evidence, and contrary to law. Petitioners request that this Court vacate the Order and the Final Rules adopted therein and grant such other relief as may be appropriate."[2885]

Second Report and Order

On May 3, 2006,[2886] the FCC addressed several issues regarding CALEA implementation, specifically, the Order:

- Affirms the May 14, 2007, CALEA compliance deadline for facilities-based broadband Internet access and interconnected VoIP services (as

---

[2884] The coalition is composed of CompTel, American Library Association, Association of Research Libraries, Center for Democracy & Technology, Electronic Frontier Foundation, Electronic Privacy Information Center, Pulver.com, and Sun Microsystems.

[2885] A copy of the Petition, No. 05-1408, is available online at [http://www.cdt.org/ digi_tele/20051025caleapetition.pdf].

[2886] In the Matter of Communications Assistance for Law Enforcement Act and Broadband Access and Services, Second Report and Order and Memorandum Opinion and Order, FCC 06-56, ET Docket 04-295, adopted May 3, 2006. This Order has not yet been released, but the news release is available online at [http://hraunfoss.fcc.gov/edocs_public/ attachmatch/DOC-265221A1.pdf].

established by the First Report and Order) and clarifies that the date will apply to all such providers.
- Explains that the FCC does not plan, at this time, to intervene in the standards-setting process in this matter.
- Permits telecommunications carriers the option of using Trusted Third Parties (TTPs) to assist in meeting their CALEA obligations.
- Restricts the availability of compliance extensions to equipment, facilities, and services deployed prior to October 25, 1998.
- Finds that the commission may, in addition to law enforcement remedies available through the courts, take separate enforcement action under section 229(a) of the Communications Act against carriers that fail to comply with CALEA.
- Concludes that carriers are responsible for CALEA development and implementation costs for post-January 1, 1995, equipment and facilities, and declines to adopt a national surcharge to recover CALEA costs.
- Requires all carriers providing facilities-based broadband Internet access and interconnected VoIP service to submit interim reports to the FCC to ensure that they will be CALEA-compliant by May 14, 2007, and also requires all such providers to which CALEA obligations were applied in the First Report and Order to come into compliance with the system security requirements in the commission's rules within 90 days of the effective date of this Second Report and Order.

Court Challenge

In June 2006, the United States Court of Appeals for the District of Columbia Circuit affirmed the FCC's decision concluding that VoIP and facilities-based broadband Internet access providers have CALEA obligations similar to those of telephone companies.[2887]

Congressional Activity: 108th-110th Congress

No bills have been introduced in the 110th Congress and none were introduced during the 109th Congress that would have amended the CALEA statute. Two bills were introduced in the 108th Congress that would have had an impact on CALEA-related powers for law enforcement, although neither would have actually amended the CALEA statute.

House of Representatives, 108th Congress

In the House of Representatives, H.R. 4129, the VOIP Regulatory Freedom Act of 2004, was introduced by Representative Pickering on April 2, 2004, and referred to the Committee on Energy and Commerce, Subcommittee on

[2887] American Council on Education v. FCC, No. 05-1404 (Consolidated with 05-1408, 05-1438, 05-1451, 05-1453). Argued May 5, 2006; decided June 9, 2006. Available online at [http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-266204A1.pdf].

Telecommunications and the Internet on April 8, 2004.[2888] The subcommittee also held a hearing on September 8, 2004, "Law Enforcement Access to Communications in a Digital Age." Although that hearing was not held specifically to address H.R. 4129, it did touch on many of the implementation issues that are facing service providers and law enforcement.[2889]

Senate, 108th Congress

In the Senate, S. 2281, the VOIP Regulatory Freedom Act of 2004, was introduced and referred to the Committee on Commerce, Science, and Transportation by Senator Sununu on April 5, 2004. This bill was intended as a companion bill to H.R. 4757, the Advanced Internet Communications Services Act of 2004, although H.R. 4757 did not contain any CALEA-related provisions.

A hearing on S. 2281 was held by the Committee on Commerce, Science, and Transportation on June 16, 2004,[2890] and the bill was ordered to be reported with an amendment in the nature of a substitute favorably on July 22, 2004; the substitute language was significantly different than that in the original bill. On November 19, 2004, the bill was again reported by Senator McCain and placed on the Senate Legislative Calendar, first without written a report on November 19, 2004, and then with a written report on December 7, 2004 (see S.Rept. 108-425).

Comparison of the House and Senate CALEA-Related Provisions in the 108th Congress

Neither bill would have amended CALEA — each provided its own statutory requirements separate from CALEA. However, the House bill contained much more specific language than the Senate bill, which only stated that the FCC "shall require a provider of a connected VoIP application to provide access to necessary information to law enforcement agencies not less than that require of information service providers."[2891] A "connected VoIP application" is defined in both bills as "a VoIP application that is capable of receiving voice communications from or sending voice communications to the public switched network, or both."

[2888] The VOIP Regulatory Freedom Act of 2004, H.R. 4129, Section 4 (c)(1)-(3).

[2889] The House held other hearings during the 108th Congress that addressed telecommunications and Internet-related issues. A full list of the hearings held by the Committee on Energy and Commerce is available online at [http://energycommerce.house.gov/108/action.htm].

[2890] The Senate held other hearings during the 108th Congress that addressed telecommunications and Internet-related issues. A full list of the hearings held by the Committee on Commerce, Science, and Transportation is available online at [http://commerce.senate.gov/hearings/index.cfm].

[2891] The VOIP Regulatory Freedom Act of 2004, S. 2281, Section 4 (c).

The House bill, which was seen as much more favorable to law enforcement interests than the Senate bill, would have required the FCC to conduct a proceeding within 180 days of the date of enactment to "determine whether it is technologically feasible and reasonable" to apply the assistance capability requirements now applied to the "equipments, facilities, or services of a telecommunications carrier" to a connected VoIP application.[2892] If the FCC were to have made an affirmative determination in this case, it would have be required to establish "rules, technical requirements, and standards" to apply such requirements while also protecting privacy and security, minimizing the costs of implementation, continuing to encourage the development of new technologies, and providing a reasonable time for compliance. In developing these rules, the FCC would have been required to consult with affected service providers, equipment manufacturers, the U.S. Attorney General, state and local law enforcement, and other interested parties.[2893]

[2892] The bill would also require the FCC to undertake such a proceeding every six months until such time as a determination is made.

[2893] See also Tech Law Journal, "Summary of VOIP Related Bills," July 21-25, 2004. Available online at [http://www.techlawjournal.com/home/newsbriefs/2004/07e.asp]. This article also contains a comparison of the non-CALEA-related provisions of these bills.

TITLE 50: WAR AND NATIONAL DEFENSE

50 U.S.C. Chapter 15: National Security (50 U.S.C. §§ 401-442a)

Subchapter III: Accountability for Intelligence Activities (50 U.S.C. §§ 413-415c)

Sensitive Covert Action Notifications: Oversight Options for Congress, R40691 (January 29, 2010).

ALFRED CUMMING, CONGRESSIONAL RESEARCH SERV., SENSITIVE COVERT ACTION NOTIFICATIONS: OVERSIGHT OPTIONS FOR CONGRESS (2010), *available at* http://www.intelligencelaw.com/library/secondary/crs/pdf/R40691_1-29-2010.pdf.

Alfred Cumming
Specialist in Intelligence and National Security
acumming@crs.loc.gov, 7-7739
January 29, 2010

7-5700
www.crs.gov
R40691

Summary

Legislation enacted in 1980 gave the executive branch authority to limit advance notification of especially sensitive covert actions to eight Members of Congress—the "Gang of Eight"—when the President determines that it is essential to limit prior notice in order to meet extraordinary circumstances affecting U.S. vital interests. In such cases, the executive branch is permitted by statute to limit notification to the chairmen and ranking minority members of the two congressional intelligence committees, the Speaker and minority leader of the House, and Senate majority and minority leaders, rather than to notify the full intelligence committees, as is required in cases involving covert actions determined to be less sensitive.

Congress, in approving this new procedure in 1980, during the Iran hostage crisis, said it intended to preserve operational secrecy in those "rare" cases involving especially sensitive covert actions while providing the President with advance consultation with the leaders in Congress and the leadership of the

intelligence committees who have special expertise and responsibility in intelligence matters. The intent appeared to some to be to provide the President, on a short-term basis, a greater degree of operational security as long as sensitive operations were underway. In 1991, in a further elaboration of its intent following the Iran-Contra Affair, congressional report language stated that limiting notification to the Gang of Eight should occur only in situations involving covert actions of such extraordinary sensitivity or risk to life that knowledge of such activity should be restricted to as few individuals as possible.

In its mark-up of H.R. 2701, the FY2010 Intelligence Authorization Act, the House Permanent Select Committee on Intelligence (HPSCI) replaced the Gang of Eight statutory provision, adopting in its place a statutory requirement that each of the intelligence committees establish written procedures as may be necessary to govern such notifications. According to committee report language, the adopted provision vests the authority to limit such briefings with the committees, rather than the President.

On July 8, 2009, the executive branch issued a Statement of Administration Policy (SAP) in which it stated that it strongly objected to the House Committee's action to replace the Gang of Eight statutory provision, and that the President's senior advisors would recommend that the President veto the FY2010 Intelligence Authorization Act if the committee's language was retained in the final bill.

The Senate Intelligence Committee, in its version of the FY2010 Intelligence Authorization Act, left unchanged the Gang of Eight statutory structure, but approved several changes that would tighten certain aspects of current covert action reporting requirements. Although the executive branch has not issued a Statement of Administration Policy with regard to the Senate's bill, Director of National Intelligence Admiral Dennis Blair has indicated that he would recommend that the President veto the bill if the covert action notification changes contained in the bill remained in final legislation. Congress has not acted on the FY2010 Intelligence Authorization bill.

With Congress considering possible changes in covert action congressional notifications, this report describes the statutory provision authorizing Gang of Eight notifications, reviews the legislative history of the provision, and examines both the impact of such notifications on congressional oversight as well as options that Congress might consider to possibly improve oversight.

Requirements for Notifications of Sensitive Covert Actions to Congress

Under current statute, the President generally is required keep the congressional intelligence committees fully and currently informed of all covert actions[2894] and that any covert action[2895] "finding"[2896] shall be reported to the committees as soon as possible after such approval and before the initiation of the covert action authorized by the finding.

If, however, the President determines that it is essential to limit access to a covert action finding in order to "meet extraordinary circumstances affecting vital interests of the United States,"[2897] then rather than providing advanced notification to the full congressional intelligence committees, as is generally required, the President may limit such notification to the "Gang of Eight," and any other congressional leaders he may choose to inform. The statute defines the "Gang of Eight" as being comprised of the chairmen and ranking members of the two congressional intelligence committees and the House and Senate majority and minority leadership.[2898]

In report language accompanying the 1980 enactment, Congress established its intent to preserve the secrecy necessary for very sensitive covert actions, while providing the President with a process for consulting in advance with congressional leaders, including the intelligence committee chairmen and ranking minority members, "who have special expertise and responsibility in intelligence matters."[2899] Such consultation, according to Congress, would ensure

---

[2894] National Security Act as amended, Sec. 503 [50 U.S.C. 413b] (b) and (c).

[2895] A covert action is defined in statute as an activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly. See the National Security Act of 1947, Sec. 503(e), 50 U.S.C. 413b(e).

[2896] A Finding is a presidential determination that an activity is necessary to "support identifiable foreign policy objectives" and "is important to he national security of the Untied States." See Intelligence Authorization Act for FY1991, P.L. 102-88, Title VI, Sec. 602 (a) (2), 50 U.S.C. 413b (a).

[2897] National Security Act of 1947 as amended, Sec. 503 [50 U.S.C. 413b] (c) (2). See Addendum A, Title V of the National Security Act as amended. The authorization for Gang of Eight notification also permits the President to notify "such other Member or Members of the congressional leadership as may be included by the President."

[2898] Ibid.

[2899] Addendum A, S.Rept. 96-730, 96th Cong., 2nd sess. (1980), p. 10. This report accompanied S. 2284, from which Title V of P.L. 96-450 is derived. Gang of Eight notification was included in a new Title V, Sec. 501, Sec. 501 (a) (1) added to the National Security Act of 1947 as amended by Sec. 407 (a) (3) of P.L. 96-450.

strong oversight, while at the same time, "share the President's burden on difficult decisions concerning significant activities."[2900]

In 1991, following the Iran-Contra Affair,[2901] Intelligence Conference Committee Conferees more specifically stated that Gang of Eight notifications should be used only when "the President is faced with a covert action of such extraordinary sensitivity or risk to life that knowledge of the covert action should be restricted to as few individuals as possible."[2902] Congressional Conferees also indicated that they expected the executive branch to hold itself to the same standard by similarly limiting knowledge of such sensitive covert actions within the executive.[2903]

Additional Gang of Eight Requirements

In addition to having to determine that vital interests are implicated, the President must comply with four additional statutory conditions in notifying the Gang of Eight. First, the President is required to provide a statement setting out the reasons for limiting notification to the Gang of Eight, rather than the full intelligence committees.[2904] The two intelligence committee chairmen, both Gang of Eight Members, also must be provided signed copies of the covert action finding in question.[2905] Third, the President is required to provide the Gang of Eight advance notice of the covert action in question.[2906] And, lastly, Gang of

---

[2900] Ibid.

[2901] The Iran-Contra affair was a secret initiative by the administration of President Ronald Reagan in the 1980s to provide funds to the Nicaraguan Democratic Resistance from profits gained by selling arms to Iran. The purpose was at least two-fold: to financially support the Nicaraguan Democratic Resistance and to secure the release of American hostages held by pro-Iranian groups in Lebanon.

[2902] Joint Explanatory Statement of the Committee of Conference, accompanying Conf.Rept. 102-166, 102nd Congress, 1st sess. (1991), p. 28. The Joint Explanatory Statement accompanied H.R. 1455, the FY1991 Intelligence Authorization Act, which was subsequently signed into law (P.L. 102-88). The "risk to life" language is not repeated in statute.

[2903] Ibid.

[2904] National Security Act of 1947 as amended, Sec. 503 [50 U.S.C. 413b] (c) (4). The statute does not explicitly specify whether such a statement should be in writing, nor specifically to whom such a statement should be provided.

[2905] Ibid.

[2906] National Security Act of 1947 as amended, Sec. 503 [50 U.S.C. 413b] (c) (2). The President must comply with these last two requirements—providing signed copies of the covert action and providing advance notification—when notifying the full committees of covert action operations that are determined to be less sensitive than "Gang of Eight" covert actions. Sec. 503 [50 U.S.C. 413b] (a) (1) requires a written finding unless immediate action by the U.S. is required and time does not permit preparation of a written finding. In the latter situation, a contemporaneous

Eight Members must be notified of any significant changes in a previously approved covert action, or any significant undertaking pursuant to a previously approved finding.[2907]

When Prior Notice to the Gang of Eight is Withheld

Although the statute requires that the President provide the Gang of Eight advance notice of certain covert actions, it also recognizes the President's constitutional authority to withhold such prior notice altogether by imposing certain additional conditions on the President should the decision be made to withhold. If prior notice is withheld, the President must "fully inform" the congressional intelligence committees[2908] in a "timely fashion"[2909] after the commencement of the covert action. The President also is required to provide a statement of the reasons for withholding prior notice to the Gang of Eight.[2910] In other words, a decision by the executive branch to withhold prior notice from the Gang of Eight would appear to effectively prevent the executive branch from limiting an-after-the-fact notification to the Gang of Eight, even if the President had determined initially that the covert action in question warranted Gang of Eight treatment. Rather, barring prior notice to the Gang of Eight, the executive

---

written record must be immediately reduced to a written finding as soon as possible within 48 hours.

[2907] Ibid, (d).

[2908] National Security Act of 1947 as amended, Sec. 503 [50 U.S.C. 413b] (c) (3).

[2909] Ibid. What constitutes "timely fashion" was the subject of intense debate between the congressional intelligence committees and the executive branch during the consideration of the fiscal year 1991 Intelligence Authorization Act. At that time, House and Senate intelligence committee conferees noted that the executive branch had asserted that the President's constitutional authorities "permit the President to withhold notice of covert actions from the committees for as long as he deems necessary." The conferees disputed the President's assertion, claiming that the appropriate meaning of "timely fashion" is "within a few days." Specifically, conferees stated, "While the conferees recognize that they cannot foreclose by statute the possibility that the President may assert a constitutional basis for withholding notice of covert actions for periods longer than 'a few days,' they believe that the President's stated intention to act under the 'timely notice' requirement of existing law to make a notification 'within a few days' is the appropriate manner to proceed under this provision, and is consistent with what the conferees believe is its meaning and intent." The conference report included the text of a letter sent to the chairman of the House Intelligence Committee, in which President George H.W. Bush stated: "In those rare instances where prior notice is not provided, I anticipate that notice will be provided within a few days. Any withholding beyond this period will be based upon my assertion of authorities granted this office by the Constitution..." See H.Conf.Rept. 102-166, 102nd Cong., 1st sess., pp. 27-28 (1991). Despite President George H.W. Bush's refusal to commit to either "timely" notification as defined by Congress, or any notification at all, Robert M. Gates, President George H.W. Bush's nominee as Director of Central Intelligence, said he believed that non-notification should be withheld for no more than a few days at the most, and that he would contemplate resignation if it extended beyond that time period. See Congressional Quarterly Almanac, 102nd Cong., 1st sess., 1991, Vol. XLVII, p. 482.

[2910] Ibid.

branch would then be required to inform the full intelligence committees of the covert action in "timely fashion." In doing so, Congress appeared to envision a covert action, the initiation of which would require a short-term period of heightened operational security.

Congress Signaled Its Intent That the Gang of Eight Would Decide When To Inform the Intelligence Committees

During the Senate's 1980 debate of the Gang of Eight provision, congressional sponsors said their intent was that the Gang of Eight would reserve the right to determine the appropriate time to inform the full intelligence committees of the covert action of which they had been notified.[2911]

The position of sponsors that the Gang of Eight would determine when to notify the full intelligence committees underscores the point that while the statute provides the President this limited notification option, it appears to be largely silent on what happens after the President exercises this particular option. Sponsors thus made it clear that they expected the intelligence committees to establish certain procedures to govern how the Gang of Eight was to notify the full intelligence committees. Senator Walter Huddleston, Senate floor manager for the legislation, said "the intent is that the full oversight committees will be fully informed at such time the eight leaders determine is appropriate. The committees will establish the procedures for the discharge of this responsibility."[2912]

Senator Huddleston's comments referred to Sec. 501(c) of Title V of the National Security Act which stipulates that "The President and the congressional intelligence committees shall each establish such procedures as may be necessary to carry out the provisions of this title."

With regard to Sec. 501(c), Senate report language stated:

> *The authority for procedures established by the Select Committees is based on the current practices of the committees in establishing their own rules. One or both committees may, for example, adopt procedures under which designated members are assigned responsibility on behalf of the committee to receive information in particular types of circumstances, such as when all members*

[2911] See Addendum B, copy of the Senate debate as recorded in the Congressional Record, 96th Congress, 2nd Session, Volume 126—Part 20, September 17, 1980 to September 24, 1980. See p. 17693.

[2912] Ibid, p. 17693.

cannot attend a meeting or when certain highly sensitive information is involved.[2913]

Congressional intent thus appeared to be that the collective membership of each intelligence committee, rather than the committee leadership, would develop such procedures.[2914] Moreover, the rules that each committee have subsequently adopted, while they deal in detail as to how the committees are to conduct their business, do not appear to address any procedures that might guide Gang of Eight notifications generally. Rather, to the extent that any such procedures have been adopted, those procedures appear to have been put into place at the executive branch's insistence, according to congressional participants.[2915]

Congress Approved Gang of Eight Notifications in 1980, Following the Iran Hostage Rescue Attempt

Congress approved the Gang of Eight notification provision in 1980 as part of a broader package of statutory intelligence oversight measures generally aimed at tightening intelligence oversight while also providing the Central Intelligence Agency (CIA) greater leeway to carry out covert operations,[2916] following a failed covert operation to rescue American embassy hostages in Iran.[2917]

Congressional approval came after President Jimmy Carter decided not to notify the intelligence committees of the operation in advance because of concerns over operational security and the risk of disclosure. Director of Central Intelligence

---

[2913] See addendum B, S.Rept. 96-730, 96th Cong, 2nd sess. See p. 13 of the report.

[2914] Ibid, p. 12.

[2915] Letter from Representative Jane Harman to President George W. Bush, January 4, 2006. Another example of the informality which sometimes informs the intelligence notification process involves so-called Gang of Four notifications. The Gang of Four consists of the chairmen of the congressional intelligence committees, the Vice Chairman of the Senate Intelligence Committee and the Ranking Member of the House Intelligence Committee. The executive branch frequently limits certain intelligence notifications to these four Members, sometimes including committee staff directors, even though neither statute, or committee rules, appear to make provision for such notifications.

[2916] Congressional Quarterly Almanac, Vol. XXXVI, 1980, p. 66.

[2917] There actually were two separate operations — both of which constituted covert actions, since neither was undertaken to collect intelligence — to rescue U.S. embassy personnel after Iranian "students" overran the U.S. Embassy in Tehran on Nov. 4, 1979. The failed operation involved an attempted airborne rescue of U.S. hostages which was aborted when three of the rescue helicopters experienced mechanical difficulties. A subsequent collision of one of the helicopters and a refueling plane left seven American rescuers dead. An earlier effort resulted in the successful extrication of six Americans who had been working at the U.S. embassy but had avoided capture by taking refuge in the residences of the Canadian ambassador and deputy chief of mission.

Stansfield Turner briefed the congressional intelligence committees only after the operations had been conducted. Although most members reportedly expressed their understanding of the demands for secrecy and thus the Administration's decision to withhold prior notification,[2918] Senate Intelligence Committee Chairman Birch Bayh expressed concern that the executive branch's action reflected a distrust of the committees. He suggested that future administrations could address disclosure concerns by notifying a more limited number of Members "so that at least somebody in the oversight mechanism would know.... If oversight is to function better, you first need it to function [at all]."[2919] Such sentiments appear to have contributed to the subsequent decision by Congress to permit the executive branch to notify the Gang of Eight in such cases.[2920]

Authority of Gang of Eight to Affect Covert Action

Even with statutory arrangements governing covert action, including Gang of Eight covert actions, Congress does not have the authority under statute to veto outright a covert action. Indeed, former Senator Howard Baker successfully pushed the inclusion in the 1980 legislative package of a provision making clear that Congress did not have approval authority over the initiation of any particular covert action.[2921]

Nonetheless, the Gang of Eight Members, as do the intelligence committees, arguably have the authority to influence whether and how such covert actions are conducted over time. For example, Members could express opposition to the initiation of a particular covert action. Some observers assert that in the absence of Members' agreement to the initiation of the covert action involved, barring such agreement, an administration would have to think carefully before proceeding with such a covert action as planned.[2922]

[2918] At the time, the Hughes-Ryan Amendment of 1974 requiring that the executive branch report on Central Intelligence Agency covert operations to as many as eight congressional committees, including the intelligence committees, was still the law.

[2919] See L. Britt Snider, The Agency and the Hill, CIA's Relationship With Congress, 1946-2004, (Washington, D.C.: Center For the Study of Intelligence, Central Intelligence Agency, 2008), p. 283.

[2920] Ibid.

[2921] National Security Act of 1947 as amended, Sec. 501[50 U.S.C. 413] (a) (2).

[2922] L. Britt Snider, The Agency and the Hill, CIA's Relationship With Congress, 1946-2004, (Washington, D.C.: Center For the Study of Intelligence, Central Intelligence Agency, 2008), p. 311. See also Mike Soraghan, "Reyes Backs Pelosi On Intel Briefings," The Hill, May 1, 2009. House Intelligence Committee Ranking Member Peter Hoekstra reportedly stated that Members of Congress are able to challenge policies they disagree with. "This is nuts, this saying, 'I couldn't do anything,'" Hoekstra told the Hill, adding that he at least once complained to then President Bush and got a policy changed, according to the newspaper.

The Gang of Eight over time could also influence funding for such operations. Initial funding for a covert action generally comes from the CIA's Reserve for Contingency Fund, for which Congress provides an annual appropriation. Once appropriated, the CIA can fund a covert action using money from this fund, without having to seek congressional approval. But the executive branch generally must seek additional funds to replenish the reserve on an annual basis. If the Gang of Eight, including the two committee chairmen and ranking members, were to agree not to continue funding for a certain covert action, they arguably could impress on the membership of the two committees not to replenish the reserve fund, providing they informed the committees of the covert action, a decision which the congressional sponsors said they intended to be left to the discretion of the Gang of Eight in any case.

Thus, the Gang of Eight could influence the intelligence committees to increase, decrease or eliminate authorized funding of a particular covert action. Some observers point out, however, that the leaders' overall effectiveness in influencing a particular covert action turns at least as much on their capability to conduct effective oversight of covert action as it does on their legal authority.

Impact on Congressional Intelligence Oversight

The impact of Gang of Eight notifications on the effectiveness of congressional intelligence oversight continues to be debated.

Supporters of the Gang of Eight process contend that such notifications continue to serve their original purpose, which, they assert, is to protect operational security of particularly sensitive covert actions that involve vital U.S. interests while still involving Congress in oversight. Further, they point out that although Members receiving these notifications may be constrained in sharing detailed information about the notifications with other intelligence committee members and staff, these same Members can raise concerns directly with the President and the congressional leadership and thereby seek to have any concerns addressed.[2923] Supporters also argue that Members receiving these restricted briefings have at their disposal a number of legislative remedies if they decide to oppose a particular covert action program, including the capability to use the appropriations process to withhold funding until the executive branch behaves according to Congress's will.[2924]

Critics counter with the following points. First, they say, Gang of Eight notifications do not provide for effective congressional oversight because

---

[2923] See Congressional Quarterly transcript of press conference given by Representative Peter Hoekstra, December 21, 2005.

[2924] See Tim Starks, "Pelosi Controversy Suggests Changes to Congressional Briefings Are Due," Congressional Quarterly, May 14, 2009.

participating Members "cannot take notes, seek the advice of their counsel, or even discuss the issues raised with their committee colleagues."[2925] Second, they contend that Gang of Eight notifications have been "overused."[2926] Third, they assert that, in certain instances, the executive branch did not provide an opportunity to Gang of Eight Members to approve or disapprove of the program being briefed to them.[2927] And fourth, they contend that the "limited information provided Congress was so overly restricted that it prevented members of Congress from conducting meaningful oversight."[2928]

Directors of National Intelligence and Central Intelligence Agency Critical of Gang of Eight Notifications For Non-Covert Actions

During their respective Senate confirmation hearings, Director of National Intelligence (DNI) Dennis Blair and CIA Director Leon Panetta criticized the use of the Gang of Eight notification procedure to notify Congress of the National Security Agency's (NSA) electronic communications surveillance program—often referred to as the Terrorist Surveillance Program, or TSP—and the CIA's detention, interrogation and rendition program. DNI Blair said both programs "involved sensitive collection activities rather than covert actions. The 'Gang of 8' notice is available … only where notice of covert action is concerned, and its use in these programs was not expressly allowed."[2929] Director Panetta said "the NSA surveillance program was not a covert action program, and, therefore, limiting notification to the 'gang of eight' was inappropriate."[2930] DNI Blair said that,

---

[2925] See letter from Representative Jane Harman to President George W. Bush, January 4, 2006, regarding the National Security Agency (NSA) electronic communications surveillance program, often referred to as the Terrorist Surveillance Program, or TSP.

[2926] See Tim Starks, "Pelosi Controversy Suggests Changes to Congressional Briefings Are Due," Congressional Quarterly, May 14, 2009.

[2927] Press release from Senator John D. (Jay) Rockefeller, December 19, 2005, commenting on the Terrorist Surveillance Program initiated by the George W. Bush Administration. As discussed earlier in this memorandum, under Sec. 501(a)(2), nothing in Title V "shall be construed as requiring the approval of the congressional intelligence committees as a condition precedent to the initiation of any significant anticipated intelligence activity.

[2928] Ibid.

[2929] See "Additional Pre-hearing Questions for Dennis C. Blair upon nomination to be Director of National Intelligence," Question/Answer 4(C), at http://intelligence.senate.gov/090122/blairresponses.pdf.

[2930] See "Additional Pre-hearing Questions for the Record For the Honorable Leon E. Panetta upon his selection to be the Director of The Central Intelligence Agency," Question/Answer 23 at http://intelligence.senate.gov/090205/answers.pdf. In his response, Director Panetta did not address whether the CIA's detention, interrogation and rendition program was an intelligence collection program, or a covert action program. Former CIA Director Michael Hayden, has said

because of the restrictive nature of Gang of Eight notifications in these two instances, "the intelligence committees were prevented from carrying out their oversight responsibilities."[2931] Director Panetta, expressing similar sentiments, said that such limited notifications "restrict the ability of the intelligence committees to conduct oversight."[2932]

House Intelligence Committee Replaces Gang of Eight Procedure in FY2010 Intelligence Authorization Act

In marking up its version of the FY2010 Intelligence Authorization Act, the House Intelligence Committee replaced the Gang of Eight statutory provision, adopting in its place a statutory requirement that each of the intelligence committees establish written procedures as may be necessary to govern such notifications.

The current Gang of Eight statutory provision stipulates:

> *If the President determines that it is essential to limit access to the finding to meet extraordinary circumstances affecting vital interest of the United States, the finding may be reported to the chairmen and ranking minority members of the congressional intelligence committees, the Speaker and the minority leader of the House of Representatives, the majority and minority leaders of the Senate, and such other member or members of the congressional leadership as may be included by the President*[2933]

---

that the program "... began life as a covert action ... " See Australian Broadcasting Corporation, AM, April 17, 2009.

Before the notification briefings were subsequently expanded to include more Members, the executive treated both programs as particularly sensitive collection programs insofar as notification was concerned, in that it limited its initial notification to the Gang of Four. See letter from Representative Jane Harman to President George W. Bush, December 21, 2005, in which she makes reference to the Administration's use of the Gang of Four notification process, used initially to notify Congress. The Bush Administration also employed the Gang of Four notification procedure to notify Congress of the CIA's detention, interrogation and rendition program. See "Members Briefings on Enhanced Interrogation Techniques (EITs)," released by the CIA on May 6, 2009. A listing of the briefings can be found at http://www.humanevents.com/downloads-pdfs/EIT%20Briefings.pdf.

[2931] See "Additional Pre-hearing Questions for Dennis C. Blair upon nomination to be Director of National Intelligence," Question/Answer 4(C), at http://intelligence.senate.gov/090122/blairresponses.pdf.

[2932] See "Additional Pre-hearing Questions for the Record For the Honorable Leon E. Panetta upon his selection to be the Director of The Central Intelligence Agency," Question/Answer 23 at http://intelligence.senate.gov/090205/answers.pdf.

[2933] Sec. 503 of the National Security Act [50 U.S.C. 413b] (c)(2).

The substitute language approved by the House Intelligence Committee stipulates:

> *If, pursuant to the procedures established by each of the congressional intelligence committees under Section 501(c), one of the congressional intelligence committees determines that not all members of that committee are required to have access to a finding under this subsection, the President may limit access to such findings or such notice as provided in such procedures.*[2934]

According to committee report language, the provision:

> *requires the President to brief all members of the congressional intelligence committees, but implicitly provides for the possibility of more restricted briefings pursuant to the written procedures established by the congressional intelligence committees, pursuant to the revised Section 501 (c). This language vests the authority to limit the briefings with the committees, rather than the President.*[2935]

The Report's reference to a revision of Sec. 501 of the National Security Act pertained to the committee's approval of statutory language requiring that the President and the congressional intelligence committees each establish such "written" procedures as may be necessary to carry out the statutes provisions.[2936] Current statute does require that any such procedures be in writing.

In approving the new provision, the committee rejected an amendment that would have authorized the committee's chairman and ranking member to decide whether to comply with a presidential request to limit access to certain intelligence information, including covert actions.

The rejected amendment stipulated that if the chairman and ranking member were unable to agree on whether or how to limit such access, access to the information would be limited if so requested by the President.[2937]

[2934] See Intelligence Authorization Act for Fiscal Year 2010, H.R. 2701, Sec. 321 [111th Congress, 1st sess.].

[2935] See H.Rept. 111-186, accompanying the Intelligence Authorization Act for Fiscal Year 2010, pp. 21-22 [111th Congress, 1st sess.].

[2936] See Intelligence Authorization Act for 2010, H.R. 2701, Sec. 321 (b).

[2937] See Intelligence Authorization Act For 2009, H.R. 5959, Sec. 502 (b). This language applied to reports of intelligence activities other than covert action. The amendment offered to the FY2010 Intelligence Authorization Act during the Committee's markup was extended to include reporting of covert actions.

According to the views of the minority contained in the report, the provision adopted by the committee:

> *nowhere creates a statutory presumption that all Members of the Committee should be briefed. Instead, it would require the Committee to unilaterally develop procedures for the handling of reporting on sensitive matters, even though the President has significant constitutional authorities in the area of national security that Courts have repeatedly said must be considered with and balanced against the authorities of Congress. The provision nowhere provides a mechanism for ensuring that decisions within the Committee are made on a bipartisan basis or for reconciling any dispute between the branches with respect to such reporting, which is a receipt for Constitutional gridlock that could be disastrous with respect to such sensitive matters.*[2938]

The House Intelligence Committee Adopted Several Other Covert Action-Related Measures as Part of FY2010 Intelligence Bill

The House Intelligence Committee adopted several additional statutory changes with regard to covert action notifications. One such change would require that the information or material concerning covert actions include any information or material relating to the legal authority under which a covert action is being or was conducted, and any information or material relating to legal issues upon which guidance was sought in carrying out or planning the covert action, including dissenting legal views.[2939]

Another change would require that the President provide Members who are not notified of a particular covert action, pursuant to the procedures established by the each of the committees, with general information on the content of the covert action.[2940]

The committee also adopted a provision that would permit a member who objects to a particular covert action that has been notified to submit an objection to the

---

[2938] See H.Rept. 111-186, accompanying the Intelligence Authorization Act for Fiscal Year 2010, Minority Views, p. 3 [111th Congress, 1st sess.].

[2939] See H.R. 2701, Intelligence Authorization Act for Fiscal Year 2010, Sec. 321 (d).

[2940] Ibid, (g) (2).

Director of National Intelligence. The DNI is required to notify the President of the objection no later than 48 hours after the objection has been submitted.[2941]

Finally, the committee approved covert action-related provisions that would

- require that the CIA inspector general audit each covert action every three years;[2942]
- require that the President maintain a record of the Members of Congress notified of a covert action and to provide such record within 30 days after the notification is provided;[2943] and
- define the current statutory phrase "significant undertaking" to mean an activity involving the potential for loss of life; requiring an expansion of existing authorities, including authorities relating to research, development, or operations; resulting in the expenditure of significant funds or other resources; requiring notification under section 504; giving rise to a significant risk of disclosing intelligence sources or methods; or possibly causing serious damage to the diplomatic relations if the activity were to be disclosed without authorization.[2944]

Senate Intelligence Committee Tightened Certain Covert Action Reporting Requirements

In its version of the FY2010 Intelligence Authorization Act, the Senate Intelligence Committee left unchanged the Gang of Eight statutory structure, but approved several changes that would tighten certain aspects of current covert action reporting requirements.

The committee adopted language stating that there shall be no exception to the requirements of Title V off the National Security Act to inform the intelligence committees of all covert actions.[2945] The committee voted to require that all members of the intelligence committees be notified when the executive branch does not provide information "in full" to all members.[2946] In such cases, the Director of National Intelligence would be required to provide in writing to the committees in a "timely manner" a statement explaining the reasons for withholding certain information from the full membership and a description of

---

[2941] Ibid, (g) (1).

[2942] Ibid, Sec. 411.

[2943] Ibid, Sec. 321 (g) (3).

[2944] Ibid, Sec. 321 (d) (2).

[2945] S. 1494, Intelligence Authorization Act For Fiscal Year 2010, Sec. 331.

[2946] Ibid, Sec. 332.

the main features of the covert action in question. The executive branch also would be required to include in reports to Congress on covert actions an explanation of the significance of the covert action and report any change to a covert action,[2947] rather than any "significant" change,[2948] as is currently required under statute.

Finally, the committee approved language that would require that the executive branch provide to the intelligence committees any information or material regarding the legal authority under which a covert action is or was conducted,[2949] and that funding for an intelligence activity would be provided only if the intelligence committees had been fully and currently informed of that activity, or had been notified when the executive branch did not provide information in full to all members.[2950]

In additional views accompanying the committee's report[2951] on the legislation, Senators John Rockefeller and Olympia Snowe said they supported the committee-adopted language because, they wrote, it would improve the notification processes, while not eliminating the Gang of Eight procedure, "which many of us believe can serve an important purpose for quick and timely notifications on extraordinarily sensitive covert actions."[2952]

A small number of the committee members opposed the notification provision contained in the bill that would require the executive branch to notify the full membership of the intelligence committees when a covert action notification does not disclose all information regarding such an activity to all members of the committees. In additional views, they stated that the adopted provision would modify the current balance in the National Security Act with respect to the congressional notification procedures and that such a provision "will unnecessarily increase the tension between the Legislative and Executive branches over information access."[2953]

[2947] Ibid.

[2948] National Security Act of 1947 as amended, Sec. 503 (d).

[2949] Ibid, Sec. 333.

[2950] Ibid, Sec. 334.

[2951] S.Rept. 111-55, accompanying S. 1494, the Intelligence Authorization Act For Fiscal Year 2010 (111th Congress, 1st Sess.), pp. 76-77.

[2952] Ibid, p. 76.

[2953] Ibid, p. 75.

Executive Branch Threatens Veto Of House and Senate Versions of 2010 Intelligence Authorization Act

On July 8, 2009, the executive branch issued a Statement of Administration Policy (SAP)[2954] in which it stated that it strongly objected to the House committee's action to replace the Gang of Eight statutory provision, and that the President's senior advisors would recommend that the President veto the FY2010 Intelligence Authorization Act if the committee's language was retained in the final bill. According to the executive branch's statement, the committee's new statutory language "would run afoul of tradition by restricting an important established means by which the President protects the most sensitive intelligence activities that are carried out in the Nation's vital national security interests."[2955]

Although the executive branch has not issued a Statement of Administration Policy with regard to the Senate's bill, Director of National Intelligence Admiral Dennis Blair has indicated that he would recommend that the President veto the bill if the covert action notification changes it contained remained in final legislation.[2956]

Gang of Eight Notifications: The Historic Record

Notwithstanding the continuing debate over the merits of such notifications, what remains less clear is the historic record of compliance with Gang of Eight provisions set out in statute. Questions include: have such notifications generally been limited to covert actions, ones that conform to congressional intent that such covert actions be highly sensitive and involve the risk to life? When prior notification is limited to the Gang of Eight, has the executive branch provided an explanatory statement as to why it limited notification to the Gang of Eight? If the Gang of Eight is not provided prior notice, has the executive branch then informed the intelligence committees at a later date and provided a reason why prior notification was not provided? Has the Gang of Eight, once notified, ever then made a determination to notify the intelligence committees, a prerogative envisioned by its congressional sponsors? Have the congressional intelligence committees, at any time since they were established, attempted to develop procedures to guide Gang of Eight notifications, as envisioned by the sponsors of the Gang of Eight provision?

[2954] See Statement of Administration Policy on H.R. 2701, the Intelligence Authorization Act for Fiscal Year 2010, July 8, 2009.

[2955] Ibid.

[2956] See Ellen Nakashima, "Intelligence Oversight Bill Faces Obstacles," Washington Post, September 18, 2009, p. A-3.

Possible Gang of Eight Options

The 111th Congress, in its assessment, could deem that the Gang of Eight notification procedure, as currently provided for in statute and by practice, continues to strike a reasonable balance between the twin objectives of operational security and congressional oversight. If, however, changes are sought, Congress could consider the following options.

Alternative One

Congress could adopt the approach approved by the House Intelligence Committee during its markup of the FY2010 Intelligence Authorization Act. This approach would eliminate the Gang of Eight statutory provision, according to its sponsors, substituting instead a provision that its sponsors said would require that the President brief all members of the congressional intelligence committees, while implicitly providing for the possibility of more restricted briefings pursuant to the written procedures that would be established by the congressional intelligence committees as may be necessary to carry out the statute's provisions.

Alternative Two

Congress could adopt the approach approved by the Senate Intelligence Committee during its markup of the FY2010 Intelligence Authorization Act. Rather than eliminating the current Gang of Eight statutory provision, the Senate language would make no exception to the requirement that the intelligence committees be notified of all covert actions. The language also would require that all members of the intelligence committees be notified when the executive branch did not provide information "in full" to all members about a particular covert action. In such cases, the Director of National Intelligence would be required to provide in writing to the committees in a "timely manner" a statement explaining the reasons for withholding certain information from the full membership and a description of the main features of the covert action in question. The executive branch also would be required to include in reports to Congress on covert actions an explanation of the significance of the covert action being considered and report any change to a covert action, rather than any "significant" change, as is currently required under statute. Finally, under the Senate Committee's provisions, the executive branch would be required to provide any information or material regarding the legal authority under which a covert action is or was conducted, and funding for a particular covert action would be provided only if the intelligence committees had been fully and currently informed of that activity, or had been notified if the executive branch had not provided information in full to all members of the two intelligence committees.

Alternative Three

Congress could adopt the provision supported by some members of the House Intelligence Committee but ultimately rejected by a majority of the committee membership that would have authorized the chairmen and ranking members of

the intelligence committees to decide whether to comply with a presidential request to limit access to certain intelligence information, including covert actions. The amendment stipulated that if the chairman and ranking member were unable to agree on whether or how to limit such access, access to the information would be limited, if so requested by the President.

Alternative Four

If Congress were to decide to preserve the Gang of Eight notification procedure, but were to consider modifying the process, such modifications could include specifying explicitly in statute that

- Gang of Eight notifications are permitted only in situations involving covert action, rather than in those situations involving non-covert action programs, including sensitive intelligence collection programs;
- a Gang of Eight notification remain in place as long as sensitive operations are underway. Once such operational sensitivities no longer prevail, however, the full membership of the intelligence committees would be informed;
- Gang of Eight Members, rather than the executive branch, will decide when to notify the full membership of the intelligence committees.
- the executive branch be required to provide a statement of the reasons, in writing, for limiting notification to the Gang of Eight, and that the executive branch provide a written statement to the congressional intelligence committees in a timely fashion when it does not provide prior notice of a covert action to the Gang of Eight.
- Pursuant to Sec. 501(c) of the National Security Act, which requires the establishment of procedures as may be necessary to carry out the provisions of the statute, Congress could require that the congressional intelligence committees establish certain procedures that would govern Gang of Eight notifications, as the sponsors of the Gang of Eight provision apparently originally intended. Such procedures could include permitting Gang of Eight Members to take notes as such briefings and establishing a process of more formal consultation between Gang of Eight Members.[2957]

Alternative Five

Congress statutorily could eliminate the Gang of Eight procedure and bring sensitive covert actions notifications back within the intelligence committee structure by permitting the President to limit initial briefings of such operations

[2957] Given the demands of timing and scheduling, according to former executive branch officials, in the interest of time, Gang of Eight Members are sometimes notified by secure phone. If scheduling permits, briefings are provided to Gang of Eight Members, often on an individual basis. It is unclear whether Gang of Eight Members ever have requested to be briefed as a group, or whether certain time and scheduling constraints would make such a request practical.

to the chairmen and ranking members of the two intelligence committees, the so-called "Gang of Four" formulation. Under this change, committee leadership could be permitted to consult with House and Senate leaders, and staff, and inform the full intelligence committees when they determine it to be appropriate.

Alternative Six

Congress statutorily could require that the executive branch inform the full membership of the intelligence committees of all covert actions, irrespective of their perceived sensitivity.

Conclusion: Striking a Balance

Striking the proper balance between effective oversight and security remains a challenge to Congress and the executive. Doing so in cases involving particularly sensitive covert actions presents a special challenge. Success turns on a number of factors, not the least of which is the degree of comity and trust that defines the relationship between the legislative and executive branches. More trust can lead to greater flexibility in notification procedures. When trust in the relationship is lacking, however, the legislative branch may see a need to tighten and make more precise the notification architecture, so as to assure what it views as being an appropriate flow of information, thus enabling effective oversight.

Statutory Procedures under Which Congress Is To Be Informed of U.S. Intelligence Activities, Including Covert Actions (i.e. Gang of Eight), Memorandum (January 18, 2006).

ALFRED CUMMING, CONGRESSIONAL RESEARCH SERV., STATUTORY PROCEDURES UNDER WHICH CONGRESS IS TO BE INFORMED OF U.S. INTELLIGENCE ACTIVITIES, INCLUDING COVERT ACTIONS, MEMORANDUM (2006), , *available at* http://www.intelligencelaw.com/library/secondary/crs/pdf/memo_1-18-2006.pdf.

FROM:
Alfred Cumming
Specialist in Intelligence and National Security
Foreign Affairs, Defense and Trade Division

Introduction

This memorandum examines certain existing statutory procedures that govern how the executive branch is to keep Congress informed of U.S. intelligence activities, reviews pertinent legislative history underpinning the development of those procedures, and looks at the notification process that reportedly was followed in informing certain Members of Congress of the President's decision to authorize the National Security Agency (NSA) to collect signals intelligence within the United States. According to U.S. Attorney General Alberto Gonzales, the program involved "intercepts of contents of communications where...one party to the communication is outside the United States" and the government has "a reasonable basis to conclude that one party to the communication is a member of al Qaeda, affiliated with al Qaeda, or a member of an organization affiliated with al Qaeda, or working in support of al Qaeda."[2958]

Statutory Obligations of the President to Ensure that Intelligence Committees Are Kept "Fully and Currently Informed"

Under current statute,[2959] the President is to ensure that the congressional intelligence committees are kept "fully and currently informed"[2960] of U.S.

[2958] Press Release, White House, Press Briefing by Attorney General Alberto Gonzales and General Michael Hayden, Principal Deputy Director for National Intelligence (Dec. 19, 2005), available at [http://www.whitehouse.gov/news/releases/2005/12/20051219-1.html].

[2959] National Security Act of 1947, Secs. 501-503 [50 U.S.C. 413 -413(b)]. In a change enacted as part of the fiscal year (FY) 1991 Intelligence Authorization Act (P.L. 102-88), Congress, for the first time, placed a statutory obligation upon the President to ensure that the congressional

intelligence activities, including any"significant anticipated intelligence activity."[2961] According to legislative history, the term "fully and currently informed," is intended to mean that complete and timely notice of actions and policies is provided, and that the committees will be informed of intelligence activities in such detail as the committees may require.[2962] Further, the Senate in report language said it expected the executive branch not to limit itself to providing full and complete information upon request from the committees, but to affirmatively keep the committees fully and currently informed.[2963]

---

intelligence committees are kept fully and currently informed of United States intelligence activities, including any significant anticipated intelligence activity. Until 1991, the Director of Central Intelligence and the intelligence agency heads had been statutorily responsible for keeping the congressional intelligence committees fully and currently informed of such activities under changes enacted in 1980. See FY1981 Intelligence Authorization Act, Sec. 501(a) (P.L. 96-450). In enacting the FY 1981 Act, the Senate Select Committee on Intelligence (SSCI) asserted that one of its principal goals was to modify the Hughes-Ryan Amendment of 1974, which required reports on CIA covert operations to as many as eight congressional committees, and substituting in its place a general provision requiring prior notice of covert operations and full access by the two intelligence committees to information concerning all intelligence activities. See S.Rept. No. 96-730, 96th Congress, 2nd sess., pp. 2-3 (1980).

In reporting its version of the FY 1991 Intelligence Authorization Act, the SSCI asserted that overall responsibility for keeping the intelligence committees fully and currently informed should be vested in the President because of the importance and sensitivity of secret intelligence activities that may affect vital national interests, and because the President, who exercises authority over all departments, agencies and entities in the executive branch, may have unique knowledge of such activities. See S.Rept. No.102-85, 102 Congress, 1 sess., p. 30 (1991).

[2960] The phrase "fully and currently informed" originated in the requirement contained in Sec. 202 of the Atomic Energy Act of 1946. Identical wording also is contained in S.Res. 400, 94th Congress, which created the SSCI. See Sec. 11(a) of the resolution. Historic practice has been that in fully and currently informing the intelligence committees about intelligence activities, other than covert actions, the executive branch generally has communicated such information – almost always in classified form – to the Chairmen and Ranking Members of the intelligence committees, often in writing. Such communications then are made available to the rest of the committee membership.

[2961] In Senate report language accompanying the FY1991 Intelligence Authorization Act (P.L. 102-88),the SSCI wrote, "The requirement to report significant anticipated activities means, in practice, that the committees should be advised of important new program initiatives and specific activities that have major foreign policy implications." See S.Rept. No. 102-85, 102 Congress, 1 sess., p. 32 (1991).

[2962] In explaining its use of the phrase fully and currently informed in report language accompanying the FY1981 Intelligence Authorization Act (P.L. 96-450), the SSCI noted: "... For over thirty years this authority served the information needs of the Joint Committee on Atomic Energy well by assuring it complete and timely notice of actions and policies of the Federal government in the field of atomic energy. The language is also contained in Senate Resolution 400, 94th Congress, and has served the Select Committee well by ensuring that the Committee is informed of intelligence activities in such detail as the committee may require... " See S.Rept. No. 96-730, 96th Congress, 2nd sess., p. 7 (1980).

[2963] Ibid.

Although the President has a legal obligation to ensure that the congressional intelligence committees are fully and currently informed of all intelligence activities, the statute distinguishes between "intelligence activities"[2964] and "covert action"[2965] as a separate category of intelligence activities, and establishes different reporting mechanisms for each.

Reporting Requirements For Intelligence Activities, Including Significant Anticipated Intelligence Activities

For all intelligence activities, including any significant anticipated intelligence activity other than covert action, the statute requires that "the congressional intelligence committees" are to be kept "fully and currently informed" of such activities;[2966] with an exception possibly being because limiting such notification would be necessary to protect intelligence sources and methods.[2967]

[2964] Although the term intelligence activities is defined in statute to include covert actions and financial intelligence activities, "intelligence activities" are not further defined in law. See National Security Act of 1947, Sec. 501 [50 U.S.C. 413] (f). In report language accompanying the FY1991 Intelligence Authorization Act (P.L. 102-88), however, the SSCI described intelligence activities as consisting of "... the gathering of information ...," while characterizing covert action as "…. an instrument of foreign policy ... that goes beyond information gathering." S.Rept. No. 102-85, 102nd Cong., 1st sess., pp. 33-34 (1991). More detailed definitions of intelligence activities and "intelligence-related activities" are contained in the Senate resolution and the House Rule which established the SSCI and the House Permanent Select Committee on Intelligence (HPSCI), respectively. See Sec. 14(a) of S.Res. 400, and Sec. 10(a) of House Rule XLVIII.

[2965] The term covert action is defined in statute to mean "... an activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly..." See the National Security Act of 1947, Sec. 503 [50 U.S.C. 413b] (e). In enacting the FY1991 Intelligence Authorization Act (P.L. 102-88), Congress, for the first time, statutorily defined the term covert action. The definition was intended to supersede the references to Central Intelligence Agency (CIA) "operations" abroad contained in the Hughes-Ryan Amendment, and to "special activities" as defined by Executive Order 12333, signed by President Ronald Reagan on Dec. 4, 1981. According to Senate report language accompanying the Senate's version of the FY1991 Act, the statutory definition of covert action was intended to reflect current practice as it had developed under the Hughes–Ryan Amendment and the executive order definition of "special activities." According to the SSCI, the statutory definition was meant to clarify the understanding of covert action activities that require presidential findings and reporting to Congress, not to relax or go beyond previous understandings. See S.Rept. No. 102-85, 102 Congress, 1 sess., p. 42 (1991).

[2966] National Security Act of 1947, Sec. 501 [50 U.S.C. 413 (a)(1) and Sec. 502 [50 U.S.C. 413a] (a)(1). Common practice by the executive branch in informing the intelligence committees about intelligence activities, other than Gang of Eight notifications, has been to communicate such information to the chairmen and ranking members of the two committees, often in writing. Such communications then generally are made available to the rest of the committee membership, and follow-up briefings by the executive branch are scheduled when determined to be necessary.

[2967] National Security Act of 1947, Sec. 502 [50 U.S.C. 413a] (a).

Another statutory provision specifically requires that the Director of National Intelligence (DNI) and the intelligence agency heads "keep the intelligence committees fully and currently informed of all intelligence activities…"[2968] and "…furnish the congressional intelligence committees any information or material concerning intelligence activities, other than covert actions…"[2969] which is within their control. The statute further requires that any report to the intelligence committees regarding a significant anticipated intelligence activity be submitted to the intelligence committees in writing, and that any such report contain a concise statement of any pertinent facts as well as an explanation of the significance of the intelligence activity in question.[2970]

Other than there being a possible exception that would authorize a more limited notification in order to protect intelligence sources and methods, the law would appear to contain no other language authorizing the President, the DNI or the intelligence agency heads to determine the number of intelligence committee members that are informed of "all intelligence activities….", other than covert action. Rather, the law requires that the "congressional intelligence committees" be kept fully and currently informed of all intelligence activities.[2971]

In keeping the congressional intelligence committees fully and currently informed, the DNI is required to show "due regard for the protection from unauthorized disclosure of classified information relating to sensitive intelligence sources and methods or other exceptionally sensitive matters."[2972] According to Senate report language accompanying the FY1991 Intelligence Authorization Act, the "protection from unauthorized disclosure" language was "… intended to have the same meaning as the legislative history of the similar preambular clause in existing law."[2973] That underlying preambular clause states:

However, it is recognized that in extremely rare circumstances a need to preserve essential secrecy may result in a decision not to impart certain sensitive aspects of operations or collection programs to the oversight committees in order to

---

[2968] Ibid, (1).

[2969] Ibid, (2).

[2970] Ibid, (b).

[2971] National Security Act of 1947, Sec. 501 [50 U.S.C. 413 (a) (1) and Sec. 502 [50 U.S.C. 413a] (a)(1).

[2972] Ibid, Sec. 502 [50 U.S.C. 413a] (a).

[2973] S.Rept. No. 102-85, 102 Congress, 2 sess., p. 33 (1991).

protect extremely sensitive intelligence sources and methods.[2974] [emphasis added]

Covert Action Reporting Requirements

By contrast, the President is legally authorized to limit congressional access to a covert action finding if he determines that it is essential to do so in order "to meet extraordinary circumstances affecting vital interests of the United States…"[2975] If he makes such a determination, the President is authorized to limit reporting of such a covert action finding to the chairmen and ranking members of the congressional intelligence committees, the House and Senate majority and minority leaders, and any other member or members of the congressional leadership that the President may designate. This covert action finding notification procedure is sometimes referred to as a "Gang of Eight" notification, because such a notification usually involves the notification of eight Members of Congress.[2976]

The statute does not define, nor does accompanying congressional report language indicate, what would constitute "extraordinary circumstances affecting vital interests."[2977] The President appears to have the sole discretion in making such a determination. In enacting the statutory language as part of the FY1991 Intelligence Authorization Act, conferees stated: "… that this provision be utilized when the President is faced with a covert action of such extraordinary sensitivity or risk to life that knowledge of the covert action should be restricted to as few individuals as possible."[2978]

If the President does not report to the intelligence committees as soon as possible after approving a covert action finding and before its initiation, or if he does not provide a more limited Gang of Eight notification, he must, in "a timely

---

[2974] S.Rept. No. 96-730, 96 Congress, 2 sess., p. 6 (1980).

[2975] National Security Act of 1947, Sec. 503 [50 U.S.C. 413b] (c) (2). Although the President is required to provide the congressional intelligence committees prior notice before initiating a covert action, the statute does permit the President, in certain extraordinary circumstances to either withhold prior notice altogether, or to limit it to the "Gang of Eight." In either case, the President is required to fully inform the committees of the particular covert action "in a timely fashion" and provide a statement of the reasons for not giving the committees prior notice.

[2976] Even though the President is authorized to notify another member, or members, of the congressional leadership beyond those serving in the eight leadership positions designated in the statute, the reporting process remains known colloquially as a "Gang of Eight" notification.

[2977] National Security Act of 1947, Sec. 503 [50 U.S.C. 413b] (c) (2).

[2978] H.Conf.Rept. No. 102-166, 102 Congress, 1 sess., p. 28 (1991).

fashion,"[2979] fully inform the committees of the covert action and provide a statement of the reasons for not providing the intelligence committees prior notice.

Congress Limits Use of "Gang of Eight" Notice to Covert Actions

In enacting the FY1991 Intelligence Authorization Act, Congress restricted the President's authority to limit prior notice to only members of the Gang of Eight to findings involving covert actions, provided the President determined that doing so was "...essential...to meet extraordinary circumstances..." affecting U.S. vital interests.[2980] The 1991 Act restricted the President's authority to provide Congress the more limited Gang of Eight prior notices only in situations involving covert action, and not in those situations involving other non-covert action intelligence activities. With regard to intelligence activities, other than those involving covert action, the executive branch was legally obligated to inform "the congressional intelligence committees."[2981] Congress in 1991 signaled its view that the earlier 1980 congressional reporting requirements had been intended to apply primarily to covert actions, rather than to all intelligence activities.[2982]

[2979] What constitutes "timely fashion" was the subject of intense debate between the congressional intelligence committees and the executive branch during the consideration of the FY1991 Intelligence Authorization Act. At that time, House and Senate intelligence committee conferees noted that the executive branch had asserted that the President's constitutional authorities "...permit the President to withhold notice of covert actions from the committees for as long as he deems necessary." The conferees disputed the assertion, claiming that the appropriate meaning of "timely fashion" is "within a few days." Specifically, conferees stated, "... While the conferees recognize that they cannot foreclose by statute the possibility that the President may assert a constitutional basis for withholding notice of covert actions for periods longer than "a few days," they believe that the President's stated intention to act under the "timely notice" requirement of existing law to make a notification "within a few days" is the appropriate manner to proceed under this provision, and is consistent with what the conferees believe is its meaning and intent." The conference report includes the text of a letter sent to the House Intelligence Committee chairman, in which President George H.W. Bush stated: "... In those rare instances where prior notice is not provided, I anticipate that notice will be provided within a few days. Any withholding beyond this period will be based upon my assertion of authorities granted this office by the Constitution..." See H.Conf.Rept. No. 102-166, 102 Congress, 1 sess, pp. 27-28 (1991).

[2980] P.L. 96-450, Sec. 501(a) (1) (B). In addition to limiting Gang of Eight limited prior notice authority, P.L. 96-450 included several other covert action program reforms enacted by Congress, the stated intention of which was put in place a more coherent and comprehensive statutory oversight framework for covert action and other intelligence activities. The reforms included the requirements that covert action findings be in writing; a finding may not be retroactive; a finding may not authorize any action that would violate the Constitution or any statute of the United States; and, a finding must identify any third parties (third countries or private parties outside normal U.S. Government controls) who implement a covert action in any significant way.

[2981] National Security Act, Sec. 501 [50 U.S.C. 413] (a) (1) and Sec. 502 [50 U.S.C. 413a] (a) (1).

[2982] S.Rept. No. 102-85, 102 Congress, 1 sess., p. 32 (1991).

NSA Domestic Surveillance

In a Dec. 17, 2005 radio address, President George W. Bush said that he had authorized NSA to intercept the international communications of people with known links to al Qaeda and related terrorist organizations in the weeks following the September 11 terrorist attacks.[2983] He said that executive branch representatives had since briefed congressional leaders more than a dozen times regarding the NSA program and its activities,[2984] and that the Members who were briefed were given an opportunity to express their approval or disapproval of the program.[2985] Two of the Members who were briefed, and who said they voiced concerns about the program, disputed that they were provided an opportunity to either approve or disapprove the NSA program.[2986] Other Members who said they were informed about the program said they could not recall certain members objecting to or disagreeing with the program moving forward.[2987]

NSA Program Notification Limited to Gang Of Eight

Some of the Members of Congress who were briefed about the program said that the executive branch had limited its briefings of the legislative branch to the Gang of Eight.[2988] They further asserted that the executive branch had prohibited them from sharing any information about the program with congressional colleagues, including members of the two congressional intelligence committees.[2989]

Based upon publicly reported descriptions of the program, the NSA surveillance program would appear to fall more closely under the definition of an intelligence collection program, rather than qualify as a covert action program as defined by

---

[2983] For a legal analysis of the NSA program, see Congressional Research Service Memorandum, Presidential Authority to Conduct Warrantless Electronic Surveillance to Gather Foreign Intelligence Information, by Elizabeth B. Bazan and Jennifer K. Elsea, Jan. 5, 2006.

[2984] Radio Address, President George W. Bush, Dec. 17, 2005.

[2985] Town Hall Meeting, President George W. Bush, Jan. 11, 2006.

[2986] News release of Senator John D. (Jay) Rockefeller, Vice Chairman Rockefeller Reacts to Reports of NSA Intercept Program in United States, Dec. 19, 2005. See also, Nancy Pelosi, "The Gap in Intelligence Oversight," Washington Post, Jan. 15, 2006, p. B7. See also, news release of Representative Nancy Pelosi, Pelosi Requests Declassification of Her Letter on NSA Activities, Dec. 20, 2005.

[2987] Press statement by Senator Pat Roberts, Senator Roberts' Response to Media Reports About Senator Rockefeller's 2003 Letter, Dec. 20, 2005. See also, transcript of a news conference with Representative Peter Hoekstra, Federal News Service, Dec. 21, 2005.

[2988] Letter from Representative Jane Harman to President George W. Bush, Jan. 4, 2006.

[2989] News release of Senator John D. (Jay) Rockefeller, Vice Chairman Rockefeller Reacts to Reports of NSA Intercept Program in United States, Dec. 19, 2005.

statute.[2990] The term covert action is defined in statute to mean "... an activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly..."[2991]

If the NSA surveillance program were to considered an intelligence collection program, limiting congressional notification of the NSA program to the Gang of Eight, which some Members who were briefed about the program contend, would appear to be inconsistent with the law, which requires that the "congressional intelligence committees be kept fully and currently informed of all intelligence activities,"[2992] other than those involving covert actions.

It may be argued that there apparently is no provision in law restricting whether and how the leaders of the committees share with the membership information pertaining to intelligence activities that the executive branch has provided to the chairmen and ranking members. Nor apparently is there any legal provision which sets forth any procedures that would govern the access of appropriately cleared committee staff to such classified information.

Both committees have adopted rules that govern access by committee members to such matters, contained in hardcopy, e.g. "papers" and "material." The House Permanent Select Committee on Intelligence (HPSCI) committee rules stipulate: "All Members of the Committee shall at all times have access to all classified papers and other material received by the Committee from any source."[2993] According to the Senate Select Committee (SSCI) on Intelligence committee rules, "Each member of the Committee shall at all times have access to all papers and other material received from any source."[2994] Both committees also reserve the right to determine committee staff access to information in the committees' possession.[2995]

[2990] National Security Act of 1947, Sec. 503(e)(1). According to this section of the law, the term covert action does not include, among other activities, those activities, the primary purpose of which is to acquire intelligence. Representative Jane Harman, Ranking Member of the HPSCI, made this point in a Jan. 4, 2006 letter to President Bush.

[2991] National Security Act of 1947, Sec. 503 [50 U.S.C. 413b] (e).

[2992] Sec. 501 [50 U.S.C. 413] (a) (1) and Sec. 502 [50 U.S.C. 413a] (a) (1).

[2993] Rules of Procedure For the Permanent Select Committee on Intelligence, United States House of Representatives, 108th Congress, Rule 14 (b).

[2994] Rules of Procedure For the Select Committee on Intelligence, United States Senate (Amended Jan. 26, 2005), Rule 9.3.

[2995] Rules of Procedure For the Permanent Select Committee on Intelligence, United States House of Representatives, 108th Congress, Rule 14 (b); and Rules of Procedure For the Select Committee on Intelligence, United States Senate (Amended Jan. 26, 2005), Rule 9.5.

Moreover, in an indication that both chambers have taken steps to affirmatively set out procedures to govern the handling of classified information in the possession of Congress, both chambers have made available to the committees a process under which each could disclose publicly any information in its possession – including classified material – if either committee determined that the public interest would be served by doing so.[2996]

Protection of Intelligence Sources and Methods

The executive branch may argue that it limited its briefing of the NSA program to the Gang of Eight, and further instructed those Members not to share information about the program with other members of the intelligence committees, in order to protect intelligence sources and methods. Limiting the sharing of intelligence information so as to protect intelligence sources and methods is an accepted Intelligence Community practice. Such practice is based upon the theory that as more individuals are informed about certain intelligence information, the greater is the risk that sources and methods will be disclosed, inadvertently or otherwise. Although limiting its briefing of the NSA program to the Gang of Eight may or may not be inconsistent with the legal requirement that the intelligence committees be kept fully and currently informed of intelligence activities, other than those involving covert action, the executive branch could assert that it also is legally required to pay "... due regard for the protection from unauthorized disclosure of classified information relating to sensitive intelligence sources and methods or other exceptionally sensitive matters..."[2997]

Congress has recognized such a necessity and stated its intent that the executive branch, in extremely rare circumstances, may need "...to preserve essential secrecy.." and thus may decide "...not to impart certain sensitive aspects of operations or collection programs to the oversight committees in order to protect extremely sensitive intelligence sources and methods..."[2998] In acknowledging this narrow need, however, Congress did not explicitly recognize, in statute or report language, the executive branch's right to withhold from the intelligence committees information about the existence of the intelligence operations and collection programs, but rather only its authority to hold back information pertaining to certain sensitive aspects of such operations and programs. [emphasis added]

The executive branch may assert that the mere discussion of the NSA program generally could expose certain intelligence sources and methods to disclosure,

---

[2996] Rules of the 109 Congress, U.S. House of Representatives, Rule X; and S.Res. 400, 94 Congress, Sec. 8.

[2997] National Security Act of 1947, Sec. 502 [50 U.S.C. 413a] (a).

[2998] S.Rept. No. 96-730, 96 Congress, 2 sess., p. 6 (1980).

thus making it necessary to limit the number of those knowledgeable of the program in order to reduce the risk of such disclosure occurring.

Notification Precedent

The executive branch could point out that despite the current statutory obligation of keeping the intelligence committees fully and currently informed of intelligence activities, other than those involving covert action, the leadership of these two committees over time have accepted executive branch practice of limiting notification of intelligence activities in some cases to either the Gang of Eight, or to the chairmen and ranking members of the intelligence committees.[2999]

[2999] House of Representatives Democratic Leader Nancy Pelosi has argued that the executive branch employs "a-need-to -know" principle in deciding which Members of the congressional intelligence committees should be kept fully and currently informed of certain intelligence information, and thus, sometimes, limit the sharing of intelligence information to the chairmen and ranking members of the committees. She asserts that Congress should adopt a similar principle, and contends that the entire membership of the intelligence committees must be kept informed if Congress is to conduct effective oversight of the intelligence community. See Nancy Pelosi, "The Gap in Intelligence Oversight," Washington Post, Jan. 15, 2006, p. B7.

"Gang of Four" Congressional Intelligence Notifications, R40698 (January 29, 2010).

ALFRED CUMMING, CONGRESSIONAL RESEARCH SERV., "GANG OF FOUR" CONGRESSIONAL INTELLIGENCE NOTIFICATIONS (2010), , *available at* http://www.intelligencelaw.com/library/secondary/crs/pdf/R40698_1-29-2010.pdf.

Alfred Cumming
Specialist in Intelligence and National Security
acumming@crs.loc.gov, 7-7739

January 29, 2010

7-5700
www.crs.gov
R40698

Summary

"Gang of Four" intelligence notifications generally are oral briefings of certain particularly sensitive *non-covert action intelligence activities*, including principally, but not exclusively, intelligence collection programs, that the Intelligence Community typically limits to the chairmen and ranking members of the two congressional intelligence committees, and at times, but not always, to their respective staff directors.

Gang of Four notifications are not based in statute but have constituted a practice generally accepted by the leadership of the intelligence committees and that is employed when the Intelligence Community believes a particular intelligence activity to be of such sensitivity that a restricted notification is warranted in order to reduce the risk of disclosure, inadvertent or otherwise. Intelligence activities viewed as being less sensitive typically are briefed to the full membership of each committee.

In either case—whether a given briefing about non-covert action intelligence activities is limited to the Gang of Four, or provided to the full membership of the intelligence committees—the current statute conditions the provision of any such information on the need to protect from unauthorized disclosure classified information relating to sensitive intelligence sources and methods or other exceptionally sensitive matters.

Congress has said that its intent in this regard is that in extremely rare circumstances a need to preserve essential secrecy may result in a decision not to impart certain sensitive aspects of operations or collection programs to the

intelligence oversight committees in order to protect extremely sensitive intelligence sources and methods. With regard to the phrase "other exceptionally sensitive matters," Congress has said its intent in using this phrase is to refer to other extremely sensitive categories of classified information such as information concerning the operational details of military deployment and extraordinarily sensitive diplomatic contacts, which the intelligence committees do not routinely require to satisfy their responsibilities.

This report reviews the history of Gang of Four notification process and compares this procedure with that of the "Gang of Eight" notification procedure. The "Gang of Eight" procedure is statutorily based and provides that that the Chairmen and Ranking Members of the intelligence committee, along with the Speaker and minority leader of the House, and Senate majority and minority leaders—rather than the full membership of the intelligence committees—are to receive prior notice of particularly sensitive covert action programs, if the President determines that limited access to such programs is essential to meet extraordinary circumstances affecting vital U.S. interests.

Although the FY2010 Intelligence Authorization bills approved by the two congressional intelligence committees address Gang of Eight covert action notifications, neither of the two bills reference Gang of Four notifications. Congress has not acted on the FY2010 Intelligence Authorization bill.

Not Statute-Based "Gang of Four" Briefings

The "Gang of Four" intelligence notification procedure has no basis in statute. Nor is such a procedure referenced in the rules of either of the two congressional intelligence committees. Rather, this particular notification procedure could be reasonably characterized as a more informal notification procedure that, over time, has come to be used by the executive branch, and generally accepted by the leadership of the intelligence committees, to provide limited notification of particularly sensitive intelligence activities to the committees' chairmen and ranking members. At times, the committees' majority and minority staff directors have been included in such briefings.

The use of Gang of Four notifications pre-dates the establishment of the congressional intelligence committees in the mid-1970s.[3000] Initially, such limited notifications were used to inform relevant congressional committee leadership of especially sensitive intelligence matters, including both covert action and intelligence collection programs.[3001] Observers commenting on such

---

[3000] The Senate Select Committee on Intelligence was established in 1976; the House Permanent Select on Intelligence was established in 1977.

[3001] See The CIA and Congress; the Untold Story From Truman to Kennedy, by David M. Barrett, University Press of Kansas, 2005, pp. 100-103.

notifications used during this time period characterized them as being oral and often cursory, and being limited to committee chairmen and ranking members and one or two senior staff members.[3002]

In 1980, when Congress approved the new "Gang of Eight"[3003] notification procedure for particularly sensitive covert action programs, use of the Gang of Four process came to be generally limited to notifying the committee leadership of sensitive non-covert action intelligence programs.

Protection of Sources and Methods or Other Exceptionally Sensitive Matters

In 1980, Congress also adopted statutory language requiring that, except for covert action notifications, which are governed by a separate set of statutory requirements, the Intelligence Community is obligated to keep the congressional intelligence committees fully and currently informed of all intelligence activities and furnished with any information or material concerning such intelligence activities.[3004] Congress conditioned these two reporting requirements on the need to protect from unauthorized disclosure classified information relating to sensitive intelligence sources and methods or other exceptionally sensitive matters.[3005] Report language stated:

> *The Administration recognizes that the intelligence oversight committees of the House and Senate are authorized to receive such information. However, it is recognized that in extremely rare circumstances a need to preserve essential secrecy may result in a decision not to impart certain sensitive aspects of operations or collection programs to the oversight committees in order to protect extremely sensitive intelligence sources and methods.[3006] [emphasis added]*

In 1991, Congress adopted new but similar language with regard to the protection of sources and methods, adding in statute the phrase "other exceptionally

---

[3002] See L. Britt Snider, The Agency and the Hill, CIA's Relationship With Congress, 1946-2004, (Washington, D.C.: Center For the Study of Intelligence, Central Intelligence Agency, 2008), p. 281. See also Frank J. Smist, Jr., Congress Oversees the United States Intelligence Community, Second Edition, 1947-1994, The University of Tennessee Press, 1994, p. 119.

[3003] See the National Security Act of 1947 as amended, Sec. 503 [50 U.S.C. 413b] (c) (2).

[3004] See P.L. 96-450, Sec. 501 (a).

[3005] Ibid.

[3006] See S.Rept. 96-730, p. 6 [96th Congress, 1st sess.] This Report accompanied S. 2284, a proposed Intelligence Oversight Act of 1980.

sensitive matters." Doing so, according to accompanying report language, would more accurately reflect and was intended to have the same meaning as the legislative history of the 1980 statutory change. The Report language stated that the added phrase:

> *... is intended to refer to other extremely sensitive categories of classified information such as information concerning the operational details of military deployments, and extraordinarily sensitive diplomatic contacts, which the intelligence committees do not routinely require to satisfy their responsibilities.*[3007] *[emphasis added]*

The issue of Intelligence Community reporting obligations has been raised anew in recently published reports, reportedly prompting the House Intelligence Committee to launch an investigation to determine whether there was any past decision or direction to withhold information from the Committee. Committee Republicans have asserted that the investigation represents an effort to protect Democratic leader, House Speaker Nancy Pelosi, who has asserted that the CIA mislead her about its terrorist interrogation program. See Tabassum Zakaria, "U.S. House Launches Investigation into CIA Program, Reuters, July 17, 2009, and "House Intel Committee to Investigate CIA Program," Associated Press, July 17, 2009. Senate Intelligence Chairman Dianne Feinstein reportedly has said that current Director of Central Intelligence Leon Panetta recently told lawmakers that former Vice President Richard Cheney had ordered that information regarding a secret Central Intelligence Agency initiative had been withheld from the congressional intelligence committees. Sen. Feinstein was quoted as saying, "We were kept in the dark. That's something that should never, ever happen again." Withholding such information from Congress, she reportedly said, "is a big problem, because the law is very clear." See Siobhan Gorman, "CIA Had Secret Al Qaeda Plan," Wall Street Journal, July 13, 2009. Other Members of the Intelligence Committees reportedly have disagreed with Sen. Feinstein's assessment, in whole or in part. Sen. Christopher Bond, Vice Chairman of the Senate Intelligence Committee, was quoted as saying, "There is absolutely no evidence that anyone lied to or misled Congress." Bond also reportedly stated, "The CIA doesn't have the time, we don't have the time, to be briefed on everything the agency's doing around the world. Every time they sneeze, we don't hear about it, unless it's a significant impact, or there's a major impact on our activity. And this was another activity to collect better information on potential threats. It did not work ... it's not an interrogation program. It didn't even rise to the level of covert action." See Ronald Kessler, "Sen. Bond: Democrats Conducting 'Jihad' to Protect Pelosi" Newsmax.com, July 13, 2009. Senator Bond also reportedly has stated that the Committee's records indicate that the CIA

[3007] See S. Rept. 102-85, accompanying S. 1325, which authorized FY1991 Intelligence appropriations.

appropriately notified Members of the CIA's program, a claim which Chairman Feinstein rejected. See Chris Strohm, "Bond Fires Back at Democrats Over CIA's Secret Program," Congress Daily/A.M., July 16, 2009. Congressman Peter Hoekstra, Ranking Member of the House Intelligence Committee, reportedly stated that that he would not judge the CIA harshly in the case of the unidentified program, because it was not fully operational. But he said that in general, the CIA had not been as forthcoming as the law required. See Scott Shane, "Cheney is Linked to Concealment of the C.I.A. Project," New York Times, July 12, 2009. According to other reports, former President George W. Bush authorized killing al-Qaida leaders shortly after Sept. 11 terrorist attacks, and that Congress was made aware of that. However, according to this report, Director Panetta also told Members that according to notes that he had been given on the early months of the program, then-Vice President Cheney directed the CIA not to inform Congress of the specifics of the secret program. See Pamela Hess, "Officials: CIA Program Targeted al-Qaida Leaders," Associated Press, July 13, 2009.

Use of Limited Notifications Continued After Establishment of Congressional Intelligence Committees

In the wake of congressional investigations undertaken in the mid-1970s that documented a pattern of misconduct on the part of U.S. intelligence agencies, Congress tightened its oversight of the Intelligence Community by establishing intelligence committees in the House and Senate that were to be exclusively devoted to intelligence oversight. Until these two committees were established, Congress's oversight of the intelligence agencies, although more assertive than is generally understood, particularly insofar as the Central Intelligence Agency (CIA) was concerned, was generally viewed as limited and informal.[3008] That approach began to change in the face of the revelations of wrong-doing by the Intelligence Community.

In the resolutions establishing the intelligence committees, Congress set out several new obligations that, at least in the case of the Senate, emphasized certain executive branch obligations to keep the two new intelligence committees fully and currently informed of all intelligence activities, including both collection and covert action programs.[3009] Although legally non-binding, the "sense of the

---

[3008] See The CIA and Congress; the Untold Story From Truman to Kennedy, by David M. Barrett, University Press of Kansas, 2005, for an overview of congressional intelligence oversight during this period.

[3009] The origin of the phrase "fully and currently informed" is the requirement contained in Sec. 202 of the Atomic Energy Act of 1946. The language also is contained in S.Res. 400, 94th Congress and, according to congressional sponsors who inserted the language in statute, the requirement has well served both the Joint Committee on Atomic Energy and the Senate

Senate" resolution establishing the committee also stated that the intelligence agencies should keep the committee informed of "any significant anticipated activities," and provide such information as may be requested by the committee relating to matters within its jurisdiction. Although the House did not include similar language in its resolution, both committees took the position that they were "appropriate committees" for the purposes of receiving notice of covert actions, a position to which the administration of President Jimmy Carter acquiesced.[3010]

Despite the Senate's directive that the Senate's new intelligence committee be kept fully and currently informed of all intelligence activities, the executive branch continued its practice of limiting notification of certain sensitive intelligence activities, including covert and collection operations, to the committees' chairmen and ranking members—the Gang of Four —with the apparent acquiescence of the committees' leadership. According to one account, the Committee's chairman, Senator Birch Bayh[3011] said:

> *There were a couple of other areas where the president wouldn't tell the entire committee. He let me know but not the entire committee. I suggested to Goldwater[3012] we keep it to ourselves. Barry concurred. There were a couple of others we decided to tell to the entire committee.[3013]*

Intelligence Committee by ensuring that the Committee would remain informed in such detail as the Committee required. Sponsors pointed out in report language accompanying the statutory change that the responsibility of the executive branch is not limited to providing full and complete information upon request from the intelligence committees but, rather, includes "an affirmative duty on the part of the head of each entity to keep the committees fully and currently informed all major policies, directive, and intelligence activities." See S.Rept. 96-730, p. 7, accompanying S. 2284, the Intelligence Oversight Act of 1980, May 15, 1980.

[3010] See "Legislative Oversight of Intelligence Activities: The U.S. Experience," Report prepared by the Select Committee on Intelligence, United States Senate, 103rd Congress, 2nd sess., October 1994, p. 6.

[3011] Senator Birch Bayh was named chairman after Senator Daniel Inouye, the Committee's first chairman, resigned as chairman.

[3012] Senator Barry Goldwater was the Committee's vice chairman during this period of time. The Senate Intelligence Committee's establishing resolution called for the establishment of a committee vice chairman, rather than a "ranking member." The vice chairman acts in the "place and stead" of the committee chairman in the absence of the chairman. See S.Res. 400, Sec. 2 (c), 94th Congress.

[3013] See Frank J. Smist, Jr., Congress Oversees the United States Intelligence Community, Second Edition, 1947-1994, The University of Tennessee Press, 1994, p. 121.

According to this same account, there were other sensitive operations about which the committee and its chairman received no notification.[3014]

Gang of Four members reportedly continue to keep the contents of sensitive briefings to themselves, although on certain occasions, the chairman and ranking member of the House Intelligence Committee reportedly have agreed to share the information with their respective party leaders.[3015] According to at least one Gang of Four member, the choice to do so is not always the lawmakers' to make. Representative Silvestre Reyes, the current chairman of the House Intelligence Committee, reportedly said that, during the administration of President George W. Bush, he was unable to have legal counsel or subject matter experts in attendance during such restricted briefings, leaving the committee unable to conduct oversight. "We were at a huge disadvantage, because [the administration and the intelligence community] called the shots," Reyes reportedly stated.[3016]

1979 Iran Hostage Crisis

Although Senate Intelligence Committee Chairman Bayh appeared to accept the practice of restricted Gang of Four notifications, he reportedly was furious[3017] when he learned President Carter had not informed him in advance of the 1980 covert efforts to rescue U.S. hostages held in Iran because of concerns over operational security and the risk of disclosure.[3018] Director of Central Intelligence Stansfield Turner briefed the full intelligence committees, but only after the operations had been conducted.[3019]

[3014] Ibid.

[3015] See Shane Harris, "The Survivor," National Journal, June 6, 2009, pp. 36-43.

[3016] Ibid, p. 42.

[3017] See Frank J. Smist, Jr., Congress Oversees the United States Intelligence Community, Second Edition, 1947-1994, The University of Tennessee Press, 1994, p. 121.

[3018] At the time of the 1980 Iran covert hostage rescue operation, existing law—the 1974 Hughes-Ryan Amendment— required notification of any proposed covert action program to up to eight congressional committees "in a timely fashion"—a phrase generally interpreted to mean that the president could inform Congress of covert operations after the fact. See the Congressional Quarterly Almanac, Vol. XXXVI, 1980, p. 66.

[3019] There actually were two separate operations—both of which constituted covert actions, since neither was undertaken to collect intelligence—to rescue U.S. embassy personnel after Iranian "students" overran the U.S. Embassy in Tehran on November 4, 1979. The failed operation involved an attempted airborne rescue of U.S. hostages which was aborted when three of the rescue helicopters experienced mechanical difficulties. A subsequent collision of one of the helicopters and a refueling plane left several American rescuers dead. An earlier effort resulted in the successful extrication of Americans who had been working at the U.S. embassy but had avoided capture by taking refuge in the residences of the Canadian ambassador and deputy chief of mission. See L. Britt Snider, The Agency and the Hill, CIA's Relationship With Congress, 1946-

Bayh expressed his concern that the executive branch's action reflected a distrust of the intelligence committees. "It would have been so easy to tell us," he was quoted as saying. "Any leaker of that information would be hung up by his thumbs. I expressed my anger to Carter about not informing us. Carter had a thing about not being able to trust the committee."[3020]

Other members of the Committee, however, apparently were quite sympathetic to the administration's concerns and expressed their understanding of the demands of secrecy and the subsequent decision to withhold prior notification. One, a senior Republican on the Committee, was quoted as saying, "The more people you tell, the more danger there is of losing life. I say: 'To hell with the Congress.'"[3021]

Despite the overall sympathy shown for President Carter's position by other members of the intelligence committees, Senator Bayh suggested that future administrations could address disclosure concerns by notifying a more limited number of members, a special subcommittee of five or seven, "so that at least somebody in the oversight mechanism would know .... If oversight is to function better, you first need it to function."[3022] This general sentiment appeared to prevail.

Later in 1980, Congress approved in statute the new Gang of Eight notification procedure. Henceforth, the intelligence committees' leadership, the Speaker and minority leader of the House, and Senate majority and minority leaders, were to be provided prior notice of particularly sensitive covert action programs if the President determined that limited access to such programs was essential to meet extraordinary circumstances affecting vital U.S. interests.[3023] At that time, neither the statute nor accompanying report language further defined what would constitute "extraordinary circumstances affecting vital U.S. interests," although in 1991, Intelligence Conference Committee Conferees stated that the Gang of Eight notification procedure should be invoked when "the President is faced with a covert action of such extraordinary sensitivity or risk to life that knowledge of the covert action should be restricted to as few individuals as

---

2004, (Washington, D.C.: Center For the Study of Intelligence, Central Intelligence Agency, 2008), p. 283.

[3020] See Frank J. Smist, Jr., Congress Oversees the United States Intelligence Community, Second Edition, 1947-1994, The University of Tennessee Press, 1994, p. 121.

[3021] Ibid.

[3022] Ibid.

[3023] See the National Security Act of 1947 as amended, Sec. 503 [50 U.S.C. 413b] (c).

possible."[3024] Conferees also indicated that they expected the executive branch to hold itself to the same standard by similarly limiting knowledge of such sensitive covert actions within the executive.[3025]

Distinctions Between Gang of Four and Gang of Eight Notifications

Gang of Four and Gang of Eight[3026] notifications differ in several ways. A principal difference is that the Gang of Four notification procedure is not based in statute, as previously mentioned, but rather is a more informal notification process that generally has been accepted by the leadership of the intelligence committees over time.

By contrast, the Gang of Eight procedure is provided for in statute, and imposes certain legal obligations on the executive branch. When employing this particular notification procedure, the President must make a determination that vital U.S. interests are at stake if a notification is to be restricted to the Gang of Eight[3027] and provide a statement setting forth the reasons for limiting notification to the Gang of Eight, rather than notifying the full membership of the intelligence committees.[3028] The President also is required to provide the Gang of Eight advance notice of the covert action in question,[3029] although the statute also recognizes the President's constitutional authority to withhold such prior notice altogether.[3030] Finally, the chairmen of the intelligence committees, both Gang of

---

[3024] Joint Explanatory Statement of the Committee of Conference, accompany Conf.Rept. 102-166, 102nd Congress, 1st sess. (1991), p. 28. The Joint Explanatory Statement accompanied H.R. 1455, the FY1991 Intelligence Authorization, Act, which was subsequently signed into law (P.L. 102-88). The "risk to life" language is not in statute.

[3025] Ibid.

[3026] For an in-depth review of Gang of Eight procedures, see CRS Report R40691, Sensitive Covert Action Notifications: Oversight Options for Congress, by Alfred Cumming.

[3027] See the National Security Act of 1947 as amended, Sec. 503 [50 U.S.C. 413b](c)(2).

[3028] Ibid, Sec. 503 [50 U.S.C. 413b](c)(4). That statute does not explicitly specify whether such a statement must be in writing, nor does it explicitly specify to whom such a statement should be provided.

[3029] Ibid, Sec. 503 [50 U.S.C. 413b](c)(2). The President must comply with these last two requirements—providing signed copies of the covert action and providing advance notification—when notifying the full committees of covert action operations that are determined to be less sensitive than Gang of Eight covert actions.

[3030] If, however, the President withholds prior notice for the Gang of Eight, he must "fully inform" the congressional intelligence committees in a "timely fashion" after commencement of the covert action in question. See the National Security Act of 1947 as amended, Sec. 503 [50 U.S.C. 413b](c)(3).

Eight Members, must be provided signed copies of the covert action finding in question,[3031] and Gang of Eight Members must be notified of any significant changes in a previously approved covert action, or any significant undertaking pursuant to a previously approved finding.[3032]

A second distinction between the two notification procedures, at least since 1980 when the Gang of Eight procedure was first adopted in statute, is that Gang of Four notifications generally are limited to non-covert action intelligence activities, including principally but not exclusively intelligence collection programs viewed by the Intelligence Community as being particularly sensitive. Gang of Eight notifications, by contrast, are statutorily limited to especially sensitive covert action programs.

Third, the two procedures also appear to differ with regard to certain restrictions that have been placed on Members who are briefed. With regard to Gang of Eight briefings, Members have been unable to take notes, seek the advice of their counsel, or discuss the issues raised with their committee colleagues.[3033] Historically, such conditions appear to have been imposed by the executive branch and to have been generally complied with by those Members who have been notified.[3034] With regard to Gang of Four procedures, however, such procedures appear to have been generally more informal and flexible. For example, staff directors have been included in certain Gang of Four briefings, and note-taking, at least in certain instances, has not been explicitly prohibited.

Notwithstanding these distinctions, there arguably is no provision in statute that restricts whether and how the Chairmen and Ranking Members of the intelligence committees share with committee members information pertaining to intelligence activities that the executive branch has provided only to the committee leadership, either through Gang of Four or Gang of Eight notifications. Nor apparently is there any statutory provision which sets forth any procedures that would govern the access of appropriately cleared committee staff to such classified information. As discussed earlier, there have been instances when intelligence committee leadership has decided to inform the full

---

[3031] Ibid.

[3032] Ibid, (d).

[3033] See letter from Representative Jane Harman to President George W. Bush, January 4, 2006, regarding the National Security Agency (NSA) electronic communications surveillance program, often referred to as the Terrorist Surveillance Program, or TSP.

[3034] See Frank J. Smist, Jr., Congress Oversees the United States Intelligence Community, Second Edition, 1947-1994, The University of Tennessee Press, 1994, p. 119.

membership of the intelligence committees of certain Gang of Four notifications.[3035]

Despite a statutory provision directing the intelligence committees to establish certain procedures that may be necessary to carry out the statutory provisions requiring that the committees be kept fully and currently informed of intelligence activities, the committees apparently have not established such procedures with regard to Gang of Four and Gang of Eight notifications.[3036] If the intelligence committees were to do so, congressional intent would appear to indicate that the establishment of such procedures would be a committee responsibility, rather than one left to the discretion of the committees' chairmen and ranking members.[3037]

Impact of Limited Notifications on Congressional Oversight

The impact of such limited congressional intelligence notification procedures as Gang of Four and Gang of Eight continues to be debated.

Supporters of Gang of Eight notifications, for example, assert that such restricted notifications continue to serve their original purpose, which is to protect operational security of particularly sensitive intelligence activities while they are on-going. Further, they point out that although Members receiving these notifications may be constrained in sharing detailed information about the notifications with other intelligence committee members and staff, these same Members can raise concerns directly with the President and the congressional leadership and thereby seek to have any concerns addressed.[3038] Supporters also argue that Members receiving these restricted briefings have at their disposal a number of legislative remedies if they decide to oppose particular programs,

---

[3035] See footnote 14.

[3036] In marking up its version of the FY2010 Intelligence Authorization Act, the House Permanent Select Committee on Intelligence replaced the Gang of Eight statutory provision, adopting instead a statutory requirement that each of the intelligence committees establish written procedures as may be necessary to govern such notifications. The executive branch on July 8, 2009, issued a Statement of Administration which stated that the President's senior advisors would recommend that the President veto the FY2010 Intelligence Authorization Act if the Committee's language was retained in the final bill.

[3037] See S.Rept. 96-730, 96th Cong., 2nd sess. (1980), p. 12. This report accompanied S. 2284, from which Title V of P.L. 96-450 is derived.

[3038] See Congressional Quarterly transcript of press conference given by Representative Peter Hoekstra, December 21, 2005.

including the capability to use the appropriations process to withhold funding until the executive branch behaves according to Congress's will.[3039]

Some critics counter that restricted notifications such as Gang of Eight do not provide for effective congressional oversight because participating Members "cannot take notes, seek the advice of their counsel, or even discuss the issues raised with their committee colleagues."[3040] Other critics contend that restricted notifications such as Gang of Eight and Gang of Four briefings have been "overused."[3041] Some critics also assert, with regard to the Gang of Four notification procedure, that its use is unlawful because such a procedure is not statutorily based.[3042]

Directors of National Intelligence and Central Intelligence Agency Critical of Gang of Eight Notifications For Non-Covert Actions

During his Senate confirmation hearings, Director of National Intelligence (DNI) Admiral Dennis Blair criticized the use of the Gang of Eight notification procedure to notify Congress of the National Security Agency's (NSA) electronic communications surveillance program—often referred to as the Terrorist Surveillance Program, or TSP—and the CIA's detention, interrogation and rendition program. Both programs, DNI Blair said, " ... involved sensitive collection activities rather than covert actions. The "Gang of 8" notice is available ... only where notice of covert action is concerned, and its used in these programs was not expressly allowed."[3043] DNI Blair said that because of the restrictive

---

[3039] See Tim Starks, "Pelosi Controversy Suggests Changes to Congressional Briefings Are Due," Congressional Quarterly, May 14, 2009.

[3040] See letter from Representative Jane Harman to President George W. Bush, January 4, 2006, regarding the National Security Agency (NSA) electronic communications surveillance program, often referred to as the Terrorist Surveillance Program, or TSP.

[3041] See Tim Starks, "Pelosi Controversy Suggests Changes to Congressional Briefings Are Due," Congressional Quarterly, May 14, 2009.

[3042] See Vicki Divoll, "Congress's Torture Bubble," Washington Post, May 13, 2009.

[3043] See "Additional Pre-hearing Questions for Dennis C. Blair upon nomination to be Director of National Intelligence," Question/Answer 4(C), at [http://intelligence.senate.gov/090122/blairresponses.pdf].

Before the notification briefings were expanded to include more members, the executive appeared to treat both programs as particularly sensitive collection programs insofar as congressional notification was concerned, in that it limited its initial notification to the Gang of Four. See letter from Representative Jane Harman to President George W. Bush, December 21, 2005, in which she makes reference to the Administration's use of the Gang of Four notification process, used initially to notify Congress of the NSA's terrorist surveillance program. The Bush Administration apparently also employed the Gang of Four notification procedure to notify Congress of the CIA's

nature of Gang of Eight notifications, its use in these two instances prevented the intelligence committees "from carrying out their oversight responsibilities."[3044]

CIA Director (DCIA) Panetta, during his confirmation process, said the NSA's Surveillance Program was not a covert action program, and thus restricting notification of that program to the Gang of Eight was "inappropriate."[3045] Although in his response DCIA Panetta did not address whether the CIA's detention, interrogation and rendition program was an intelligence collection program, or a covert action program, he did assert that where covert action is concerned, the Gang of Eight notification procedure "ought to be limited to extraordinary cases, where operational details will be revealed whose disclosure might jeopardize those involved …This result might be justified so long as lives remain at risk, but not after the danger has passed."[3046] He went on to say that restricted Gang of Eight notifications deny the eight Members the ability to conduct oversight because they "cannot tell anyone else what they have heard, and are thereby denied the ability to seek professional advice from their staffs or consult with knowledgeable members."[3047]

Both Directors Support Gang of Four Notifications Under Certain Circumstances

During their respective confirmations, DNI Blair and DCIA Panetta said they would limit the use of notification of certain sensitive intelligence activities, other than covert actions, to the chairmen and ranking members of the intelligence committees for special cases involving the potential for the loss of life if an intelligence operation were to be exposed. Both officials prefaced their respective statements by referencing the statutory requirement that informing the committees of such intelligence activities be done "To the extent consistent with due regard for the protection from unauthorized disclosure of classified information relating to sensitive intelligence sources and methods or other

---

detention, interrogation and rendition program. See "Members Briefings on Enhanced Interrogation Techniques (EITs)," released by the CIA on May 6, 2009. A listing of the briefings can be found at http://www.humanevents.com/downloadspdfs/EIT%20Briefings.pdf.

[3044] See "Additional Pre-hearing Questions for Dennis C. Blair upon nomination to be Director of National Intelligence," Question/Answer 4(C), at http://intelligence.senate.gov/090122/blairresponses.pdf.

[3045] See "Additional Pre-hearing Questions for the Record For the Honorable Leon E. Panetta upon his selection to be the Director of The Central Intelligence Agency," Question/Answer 23 at http://intelligence.senate.gov/090205/answers.pdf.

[3046] Ibid. Although DCIA Panetta did not address whether the CIA's detention, interrogation and rendition program was an intelligence collection program, or a covert action program, former DCIA Michael Hayden has said that the program " … began life as a covert action … " See Australian Broadcasting Corporation, AM, April 17, 2009.

[3047] Ibid.

exceptionally sensitive matters ... "[3048] Both officials said they interpreted the phrase to provide a degree of latitude in deciding how—not whether – extremely sensitive matters would be brought to the committees' attention.

DNI Blair stated, "In such cases, it may be prudent to begin by notifying the leaders and staff directors of the intelligence committees and attempt to reach an accommodation with them in terms of how and when the committee as a whole should be brought into the matter in question."[3049]

In responding specifically to a question for the record as to when he would believe notification of an intelligence activity may be limited to the chairman and vice chairman or ranking member, DNI Blair referred specifically to "extremely sensitive" collection activities "... which could involve the loss of life if disclosed – I would go to the leaders of the intelligence committees first, to discuss my concerns and how and when notice could prudently be provided to the entire committee."[3050]

Conclusion

The Gang of Four notification procedure has no basis in statute. Rather, this procedure could be reasonably characterized as a more informal notification process that, at various times, has been used by the executive branch, to provide limited notification of particularly sensitive intelligence activities to the chairmen and ranking members of the intelligence committees. The Gang of Four procedure appears to have been a practice that has been generally accepted by the chairmen and ranking members of the intelligence committees over time, although there is some indication that, on occasion, committee leadership has resisted the executive branch and its use of this particular notification procedure.[3051]

Further, in approving Sec. 501[50 U.S.C. 413](c) of the National Security Act of 1947, which calls on the President and the congressional intelligence committees to establish such procedures as may be necessary to carry out the provisions of this title—referring to the Act's Title V—it appears that congressional intent was that the full membership of the committees, rather than the chairmen and

---

[3048] See the National Security Act of 1947 as amended, Sec. 502 [50 U.S.C. 413b](a).

[3049] See "Additional Pre-hearing Questions for Dennis C. Blair upon nomination to be Director of National Intelligence," Question/Answer 4(A), at http://intelligence.senate.gov/090122/blairresponses.pdf.

[3050] Ibid, Question/Answer 4(D).

[3051] See hearing transcript of testimony presented by former House Intelligence Committee Chairman Lee Hamilton before the Senate Select Committee on Intelligence: "Open Hearing: Congressional Oversight," November 13, 2007.

ranking members, would determine such procedures. No such procedures appear to have been developed with regard to the Gang of Four and Gang of Eight notifications.

The Gang of Eight notification procedure, by contrast, is based in statute. Its use is limited to especially sensitive covert actions in which the President determines that such limited notification is essential to meet extraordinary circumstances affecting vital U.S. interests.

Striking the proper balance between effective oversight and security remains a challenge for Congress and the executive. Doing so in cases involving particularly sensitive collection and covert action programs presents a special challenge. Success turns on a number of factors, not the least of which is the degree of comity and trust that exists in the relationship between the legislative and executive branches. More trust can lead to greater flexibility in notification procedures. When trust in the relationship is lacking, however, the legislative branch may see a need to tighten and make more precise the notification architecture, so as to assure, in its view, that an appropriate flow of information occurs, thus enabling effective oversight.

[DoD] Covert Action: Legislative Background and Possible Policy Questions, RL33715 (July 6, 2009).

ALFRED CUMMING, CONGRESSIONAL RESEARCH SERV., COVERT ACTION: LEGISLATIVE BACKGROUND AND POSSIBLE POLICY QUESTIONS (2009), , *available at* http://www.intelligencelaw.com/library/secondary/crs/pdf/RL33715_7-6-2009.pdf.

Alfred Cumming
Specialist in Intelligence and National Security
acumming@crs.loc.gov, 7-7739

July 6, 2009

Congressional Research Service
7-5700
www.crs.gov
RL33715

Summary

Published reports have suggested that in the wake of the 9/11 terrorist attacks, the Pentagon has expanded its counter-terrorism intelligence activities as part of what the Bush Administration termed the global war on terror. Some observers have asserted that the Department of Defense (DOD) may have been conducting certain kinds of counterterrorism intelligence activities that would statutorily qualify as "covert actions," and thus require a presidential finding and the notification of the congressional intelligence committees.

Defense officials have asserted that none of DOD's current counter-terrorist intelligence activities constitute covert action as defined under the law, and therefore, do not require a presidential finding and the notification of the intelligence committees. Rather, they contend that DOD conducts only "clandestine activities." Although the term is not defined by statute, these officials characterize such activities as constituting actions that are conducted in secret, but which constitute "passive" intelligence information gathering. By comparison, covert action, they contend, is "active," in that its aim is to elicit change in the political, economic, military, or diplomatic behavior of a target.

Some of DOD's activities have been variously described publicly as efforts to collect intelligence on terrorists that will aid in planning counter-terrorism missions; to prepare for potential missions to disrupt, capture or kill them; and to help local militaries conduct counter-terrorism missions of their own.

Senior U.S. intelligence community officials have conceded that the line separating Central Intelligence Agency (CIA) and DOD intelligence activities has

blurred, making it more difficult to distinguish between the traditional secret intelligence missions carried out by each. They also have acknowledged that the U.S. Intelligence Community confronts a major challenge in clarifying the roles and responsibilities of various intelligence agencies with regard to clandestine activities. Some Pentagon officials have appeared to indicate that DOD's activities should be limited to clandestine or passive activities, pointing out that if such operations are discovered or are inadvertently revealed, the U.S. government would be able to preserve the option of acknowledging such activity, thus assuring the military personnel who are involved some safeguards that are afforded under the Geneva Conventions. Covert actions, by contrast, constitute activities in which the role of the U.S. government is not intended to be apparent or to be acknowledged publicly. Those who participate in such activities could jeopardize any rights they may have under the Geneva Conventions, according to these officials.

In committee report language accompanying H.R. 2701, the FY2010 Intelligence Authorization Act, the House Permanent Select Committee on Intelligence (HPSCI) expressed its concern that the distinction between the CIA's intelligence-gathering activities and DOD's clandestine operations is becoming blurred and called on the Defense Department to meet its obligations to inform the Committee of such activities.

This report examines the statutory procedures governing covert action and associated questions to consider.

Introduction

Some observers assert that since 9/11 the Pentagon has begun to conduct certain types of counterterrorism intelligence activities that may meet the statutory definition of a covert action. The Pentagon, while stating that it has attempted to improve the quality of its intelligence program in the wake of 9/11, has contended that it does not conduct covert actions.

Congress in 1990 toughened procedures governing intelligence covert actions in the wake of the Iran-Contra affair, after it was discovered that the Reagan Administration had secretly sold arms to Iran, an avowed enemy that had it branded as terrorist, and used the proceeds to fund the Nicaraguan Democratic Resistance, also referred to by some as "Contras." In response, Congress adopted several statutory changes, including enacting several restrictions on the conduct of covert actions and establishing new procedures by which Congress is notified of covert action programs. In an important change, Congress for the first time statutorily defined covert action to mean "an activity or activities of the United States Government to influence political, economic, or military conditions

abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly."[3052]

The 1991 statutory changes remain in effect today. This report examines the legislative background surrounding covert action and poses several related policy questions.

Background

In 1974, Congress asserted statutory control over covert actions in response to revelations about covert military operations in Southeast Asia and other intelligence activities. It approved the Hughes-Ryan Amendment to the Foreign Assistance Act of 1961 requiring that no appropriated funds could be expended by the CIA for covert actions unless and until the President found that each such operation was important to national security, and provided the appropriate committees of Congress with a description and scope of each operation in a timely fashion.[3053] The phrase "timely fashion" was not defined in statute.

In 1980, Congress endeavored to provide the two new congressional intelligence committees with a more comprehensive statutory framework under which to conduct oversight.[3054] As part of this effort, Congress repealed the Hughes-Ryan Amendment and replaced it with a statutory requirement that the executive branch limit its reporting on covert actions to the two intelligence committees, and established certain procedures for notifying Congress prior to the implementation of such operations. Specifically, the statute stipulates that if the President determines it is essential to limit prior notice to meet extraordinary circumstances affecting the vital interests of the United States, the President may limit prior notice to the chairmen and ranking minority members of the intelligence committees, the speaker and minority leader of the House, and the majority and minority leaders of the Senate—a formulation that has become known as the "Gang of Eight." If prior notice is withheld, the President is required to inform the Committees in a "timely fashion" and provide a statement of the reasons for not giving prior notice.[3055]

In 1984, in the wake of the mining of Nicaraguan harbors in support of the Nicaraguan Democratic Resistance, the chairman and vice chairman of the

---

[3052] Sec. 503(e) of the National Security Act of 1947 [50 U.S.C. 413b].

[3053] P.L. 93-559 (1974). The "appropriate committees of Congress" was interpreted to include the Committees on Armed Services, Foreign Relations (Senate) and Foreign Affairs (House), and Appropriations of each House of Congress, a total of six committees.

[3054] The Senate Select Committee on Intelligence was established in 1976. The House Permanent Select Committee on Intelligence was established in 1977.

[3055] P.L. 96-450 (1980).

Senate Select Committee on Intelligence signed an informal agreement—which became known as the "Casey Accords"—with then-Director of Central Intelligence (DCI) William Casey establishing certain procedures that would govern the reporting of covert actions to Congress. In 1986, the committee's principals and the DCI signed an addendum to the earlier agreement, stipulating that the Committee would receive prior notice if "significant military equipment actually is to be supplied for the first time in an ongoing operation … even if there is no requirement for separate higher authority or Presidential approval." This agreement reportedly was reached several months after President Reagan signed the January 17, 1986, Iran Finding which authorized the secret transfer of certain missiles to Iran.[3056]

Following the Iran-Contra revelations, President Ronald Reagan in 1987 issued National Security Decision Directive 286 prohibiting retroactive findings and requiring that findings be written. The executive branch, without congressional consent, can revise or revoke such National Security Directives.

In 1988, acting on a recommendation made by the Congressional Iran-Contra Committee, the Senate approved bipartisan legislation that would have required that the President notify the congressional intelligence committees within 48 hours of the implementation of a covert action if prior notice had not been provided. The House did not vote on the measure.

Still concerned by the fall-out from the Iran-Contra affair, Congress in 1990 attempted to tighten its oversight of covert action. The Senate Intelligence Committee approved a new set of statutory reporting requirements, citing the ambiguous, confusing and incomplete congressional mandate governing covert actions under the then-current law. After the bill was modified in conference, Congress approved the changes.[3057]

President George H.W. Bush pocket-vetoed the 1990 legislation, citing several concerns, including conference report language indicating congressional intent that the intelligence committees be notified "within a few days" when prior notice of a covert action was not provided, and that prior notice could only be withheld in "exigent circumstances."[3058] The legislation also contained language stipulating that a U.S. government request of a foreign government or a private citizen to conduct covert action would constitute a covert action.

[3056] W. Michael Reisman and James E. Baker, Regulating Covert Action, 1992, (Yale University Press) pp. 131-132.

[3057] S. 2834.

[3058] Memorandum of Disapproval issued by President George H.W. Bush, Nov. 30, 1990.

In 1991, after asserting in new conference language its intent as to the meaning of "timely fashion" and eliminating any reference to third-party covert action requests, Congress approved and the President signed into law the new measures.[3059] President Bush noted in his signing statement his satisfaction that the revised provision concerning "timely" notice to Congress of covert actions incorporates without substantive change the requirement found in existing law, and that any reference to third-party requests had been eliminated. Those covert action provisions remain in effect today.[3060]

Post 9/11 Concerns

Since the 9/11 terrorist attacks, concerns have surfaced with regard to the Pentagon's expanded intelligence counterterrorism efforts. Some lawmakers reportedly have expressed concern that the Pentagon is creating a parallel intelligence capability independent from the CIA or other American authorities, and one that encroaches on the CIA's realm.[3061] It has been suggested that the Pentagon has adopted a broad definition of its current authority to conduct "traditional military activities" and "prepare the battlefield."[3062] Senior Defense Department officials reportedly have responded that the Pentagon's need for

---

[3059] P.L. 102-88. See covert action requirements in Sec. 503 of the National Security Act of 1947 [50 U.S.C. 413b].

[3060] Although the covert action statute has remained virtually unchanged, Congress has addressed some related concerns. The FY2004 defense authorization law (P.L. 108-136) included a provision requiring the Secretary of Defense to report to Congress on the Special Operations Forces' changing role in counterterrorism, and on the implications of those changes, if any, on the Special Operations command. Also included was a provision requiring that any Special Operations Command-led missions be authorized by the President or the Secretary of Defense. In the 2004 intelligence authorization law, conferees reaffirmed the "functional definition of covert action" and cited the "critical importance to the requirements for covert action approval and notification" contained in the 1991 intelligence authorization law. For a more detailed discussion of these and related issues, see Helen Fessenden, CQ Weekly, "Intelligence: Hill's Oversight Role At Risk, Mar. 27, 2004, p. 734. In the FY2009 Duncan Hunter National Defense Authorization Act, Congress increased, from $25 to $35 million, the amount of annually authorized funds available to the Secretary of Defense, with the concurrence of the relevant Ambassador, "...to provide support to foreign forces, irregular forces, groups, or individuals supporting or facilitating ongoing military operations by United States special operations forces to combat terrorism." Congress also extended the Defense Secretary's authority to spend such funds through fiscal year 2011. Under previously existing law, the Secretary of Defense was required to notify the congressional defense committees "... expeditiously, and in any event in not less than 48 hours, of the use of such authority with respect to that operation." Under the new law, the Secretary is required to notify the committees within 48 hours of the use of such authority. Congress reaffirmed that the Secretary's authority does not constitute the authority to conduct a covert action. See Section 1208, P.L. 110-417.

[3061] Eric Schmitt, New York Times, "Clash Forseen Between CIA and Pentagon," May 10, 2006, p 1. For a discussion of this and related issues, see Jennifer D. Kibbe, "Covert and Action and the Pentagon," Intelligence and National Security, February, 2007.

[3062] Ibid.

intelligence to support ground troops after 9/11 requires a more extensive Pentagon intelligence operation, and they suggest that any difference in DOD's approach is due more to the amount of intelligence gathering that is necessarily being carried out, rather than to any difference in the activity it is conducting.[3063] These same officials, however, also reportedly contend that American troops were now more likely to be working with indigenous forces in countries like Iraq or Afghanistan to combat stateless terrorist organizations and need as much flexibility as possible.[3064]

Late 2008 media reports have stated that the U.S. military since 2004 has used broad, secret authority to carry out nearly a dozen previously undisclosed attacks against Al Qaeda and other militants in Syria, Pakistan and elsewhere.[3065] According to other media reports, DOD has been paying private contractors in Iraq to produce news stories and other media products to "engage and inspire" the local population to support U.S. objectives and the Iraqi government. The products may or may not be non-attributable to coalition forces.[3066]

Adding even more complexity to DOD and CIA mission differences, according to Director of National Intelligence Dennis C. Blair,[3067] is that there often is not a "bright line" between traditional secret intelligence missions carried out by the military and those by the CIA, requiring that such operations be considered on a case-by-case basis.[3068] The DNI said the executive branch would be guided by two criteria. First, the President and those in the military and intelligence chains of command would maintain the flexibility to design and execute an operation solely for the purpose of accomplishing the mission. Second, he said, such operations would be approved by the appropriate authorities, coordinated in the field, and reported to the relevant congressional committees, including the Intelligence, Armed Services and Appropriations Committees.

[3063] Ibid.

[3064] Ibid.

[3065] See Eric Schmitt and Mark Mazzetti, New York Times, "Secret Order Lets U.S. Raid Al Qaeda in Many Countries," November 10, 2008, p. A-1.

[3066] See Karen DeYoung and Walter Pincus, Washington Post, "U.S. to fund Pro-American Publicity in Iraqi Media," Oct. 3, 2008, p. A-1.

[3067] Admiral Dennis C. Blair was confirmed as Director of National Intelligence by the U.S. Senate by unanimous consent on a Jan. 28, 2009. He succeeded retired Admiral J. Michael McConnell.

[3068] See "Questions for the Record for Admiral Dennis C. Blair upon nomination to be Director of National Intelligence," Senate Select Committee on Intelligence, Jan. 22, 2009. See the Senate Intelligence Committee's website [http://intelligence.senate.gov], "Recent Action," "Responses to Dennis C. Blair Post-hearing Questions," and "Covert Action."

DNI Blair's views appear to comport with comments previously made by CIA Director Michael Hayden who reportedly stated that it has become more difficult to distinguish between traditional secret military and CIA intelligence missions and that any problems resulting from overlapping missions would be resolved case-by-case.[3069] Stating the military's perspective, General James R. Clapper, Jr., the Pentagon's Under Secretary of Defense for Intelligence, testified before the Senate Armed Services Committee that within the statutory context of the meaning of covert action, "covert activities are normally not conducted ... by uniformed military forces."[3070] In written responses to questions posed by the Senate Armed Services Committee in advance of the hearing, General Clapper asserted that it was his understanding that "military forces are not conducting 'covert action,'" but are instead confining their actions to clandestine activities.[3071] Although testifying that the term "clandestine activities" is not defined by statute, he characterized such activity as consisting of those actions that are conducted in secret, but which constitute "passive" intelligence information gathering. By contrast, covert action, he suggested, is "active," in that its aim is to elicit change in the political, economic, military, or diplomatic behavior of a target.[3072] In comments before the committee, he further noted that clandestine activity can be conducted in support of a covert activity.[3073] He also distinguished between a covert action, in which the government's participation is unacknowledged, and a clandestine activity, which although intended to be secret, can be publicly acknowledged if it is discovered or inadvertently revealed.[3074] Being able to publicly acknowledge such an activity provides the military personnel who are involved certain protections under the Geneva

---

[3069] See Karen DeYoung and Walter Pincus, Washington Post, "U.S. to fund Pro-American Publicity in Iraqi Media," Oct. 3, 2008, p. A-1. The Department of Defense makes the following distinction between a clandestine operation and a covert action: a clandestine operation is an operation sponsored or conducted by governmental departments or agencies in such a way as to assure secrecy or concealment. Such an operation differs from a covert action in that emphasis is placed on concealment of the operation rather than on the concealment of the identity of the sponsor. According to DOD, in special operations, an activity may be both covert and clandestine and may focus equally on operational considerations and intelligence-related activities. See "Department of Defense Dictionary of Military and Associated Terms," Joint Publication 1-02, August 8, 2006.

[3070] See U.S. Senate Armed Services Committee hearing transcript on Department of Defense Mar. 27, 2007.

[3071] See Advanced Questions for Lieutenant General James Clapper USAF (Ret.), Nominee for the Position of Under Secretary of Defense for Intelligence, at http://www.armed-services.senate.gov, Hearings, Mar. 27, 2007, Statement of James R. Clapper, Jr.

[3072] See U.S. Senate Armed Services Committee hearing transcript on Department of Defense, Mar. 27, 2007, p. 23.

[3073] Ibid.

[3074] Ibid.

Conventions, according to General Clapper, who suggested that those who participate in covert actions could jeopardize any rights they may have under the Geneva Conventions. He recommended "that, to the maximum extent possible, there needs to be a line drawn (between clandestine and covert activities) from an oversight perspective and as well [sic] as a risk perspective."[3075]

Some observers suggest that Congress needs to increase its oversight of military activities that some contend may not meet the definition of covert action, and may therefore, be exempt from the degree of congressional oversight accorded to covert actions. Others contend that increased oversight would hamper the military's effectiveness.[3076]

The Senate Intelligence Committee has expressed its concern that the USD(I) has interpreted Title 10 to expand "military source operations" authority, thus allowing the Services and Combatant Commands to conduct clandestine HUMINT operations worldwide. "These activities can come awfully close to activities that constitute covert action," the Committee stated in questions for the record posed to DNI following his confirmation hearing before the Committee.[3077]

Current Statute Governing Covert Actions

The current statute with regard to covert action remains virtually unchanged since it was signed into law in 1991.[3078] In essence it codified elements of the "Casey Accords," the President's 1988 national security directive and various legislative initiatives.

The legislation approved that year, according to the conferees,[3079] for the first time imposed the following requirements pertaining to covert action:

- A finding must be in writing.
- A finding may not retroactively authorize covert activities which have already occurred.

[3075] Ibid.

[3076] Helen Fessenden, CQ Weekly, "Intelligence: Hill's Oversight Role At Risk," Mar. 27, 2004, p. 734.

[3077] See "Questions for the Record for Admiral Dennis Blair Upon Nomination to be Director of National Intelligence, January 22, 2009," Covert Action [http://intelligence.senate.gov/090122/blairresponses2.pdf].

[3078] Sec. 503 of the National Security Act of 1947 [50 U.S.C. 413b].

[3079] Joint Explanatory Statement of the Committee of Conference, H.R. 1455, Jul. 25, 1991.

- The President must determine that the covert action is necessary to support identifiable foreign policy objectives of the United States.
- A finding must specify all government agencies involved and whether any third party will be involved.
- A finding may not authorize any action intended to influence United States political processes, public opinion, policies or media.
- A finding may not authorize any action which violates the Constitution of the United States or any statutes of the United States.
- Notification to the congressional leaders specified in the bill must be followed by submission of the written finding to the chairmen of the intelligence committees.
- The intelligence committees must be informed of significant changes in covert actions.
- No funds may be spent by any department, agency or entity of the executive branch on a covert action until there has been a signed, written finding.

The term "covert action" was defined for the first time in statute to mean "... an activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States will not be apparent or acknowledged publicly...."[3080]

In 1991, Congressional conferees said this new definition was intended to clarify understandings of intelligence activities requiring the President's approval, not to relax or go beyond previous understandings. Conferees also signaled their intent that government activities aimed at misleading a potential adversary to the true nature of U.S. military capabilities, intentions or operations, for example, would not be included under the definition. And they stated that covert action does not apply to acknowledged U.S. government activities which are intended to influence public opinion or governmental attitudes in foreign countries. To mislead or to misrepresent the true nature of an acknowledged U.S. activity does not make it a covert action, according to the conferees.[3081]

Exceptions Under the Statutory Definition of Covert Action

In approving a statutory definition of covert action, Congress also statutorily stipulated four categories of activities which would not constitute covert action. They are: (1) activities the primary purpose of which is to acquire intelligence, traditional counterintelligence activities, traditional activities to improve or maintain the operational security of U.S. government programs, or administrative activities; (2) traditional diplomatic or military activities or

---

[3080] Ibid.

[3081] Ibid.

routine support to such activities; (3) traditional law enforcement activities conducted by U.S. government law enforcement agencies or routine support to such activities; and (4) activities to provide routine support to the overt activities (other than activities described in the first three categories) of other U.S. government agencies abroad.[3082]

This report addresses the second category of activities—traditional military activities and routine support to those activities.

Traditional Military Activities

Conferees stated:

> *It is the intent of the conferees that "traditional military activities" include activities by military personnel under the direction and control of a United States military commander (whether or not the U.S. sponsorship of such activities is apparent or later to be acknowledged) preceding and related to hostilities which are either anticipated (meaning approval has been given by the National Command Authorities for the activities and or operational planning for hostilities) to involve U.S. military forces, or where such hostilities involving United States military forces are ongoing, and, where the fact of the U.S. role in the overall operation is apparent or to be acknowledged publicly. In this regard, the conferees intend to draw a line between activities that are and are not under the direction and control of the military commander. Activities that are not under the direction and control of a military commander should not be considered as "traditional military activities."*[3083]

Routine Support of Traditional Military Activities

Conferees further stated that whether or not activities undertaken well in advance of a possible or eventual U.S. military operation constitute "covert action" will depend in most cases upon whether they constitute "routine support" and referenced the report accompanying the Senate bill for an explanation of the term.[3084]

The report accompanying the Senate bill[3085] states:

[3082] Ibid.

[3083] Joint Explanatory Statement of the Committee of Conference, H.R. 1455, Jul. 25, 1991.

[3084] Ibid.

[3085] S.Rept. 102-85, S. 1325, 102nd Congress, 1st Session (1991).

> *The committee considers as "routine support" unilateral U.S. activities to provide or arrange for logistical or other support for U.S. military forces in the event of a military operation that is to be publicly acknowledged. Examples include caching communications equipment or weapons, the lease or purchase from unwitting sources of residential or commercial property to support an aspect of an operation, or obtaining currency or documentation for possible operational uses, if the operation as a whole is to be publicly acknowledged.*

The report goes on to state:

> *The committee would regard as "other-than-routine" support activities undertaken in another country which involve other than unilateral activities. Examples of such activity include clandestine attempts to recruit or train foreign nationals with access to the target country to support U.S. forces in the event of a military operation; clandestine [efforts] to influence foreign nationals of the target country concerned to take certain actions in the event of a U.S. military operation; clandestine efforts to influence and effect [sic] public opinion in the country concerned where U.S. sponsorship of such efforts is concealed; and clandestine efforts to influence foreign officials in third countries to take certain actions without the knowledge or approval of their government in the event of a U.S. military operation.*

As the congressional conferees declared in 1991, timing of such activities—whether proximate to a military operation, or well in advance—does not define "other-than-routine" support of military activities. Rather, whether such activities constitute "other-than-routine" support, and thus constitute covert action, will depend, in most cases, on whether such an activity is unilateral in nature, that is, whether U.S. government personnel conduct the activity, or whether they enlist the assistance of foreign nationals.

House Intelligence Committee Calls on DOD to Inform Committee of Intelligence Activities

In committee report language accompanying the FY2010 Intelligence Authorization Act, the House Permanent Select Committee on Intelligence (HPSCI) expressed its concern that the distinction between the CIA's intelligence-gathering activities and DOD's clandestine operations is becoming

blurred and called on the Defense Department to meets its obligations to inform the Committee of such activities.[3086]

The Committee said that DOD frequently labels its clandestine activities as "Operational Preparation of the Environment" (OPE) to distinguish particular operations as traditional military activities and not as intelligence functions. According to the Committee's report, the overuse of this term "has made the distinction all but meaningless" and that there are no clear guidelines or principles for making consistent determinations in this regard.[3087]

The Committee stated:

> *Clandestine military intelligence-gathering operations, even those legitimately recognized as OPE, carry the same diplomatic and national security risks as traditional intelligence-gathering activities. While the purpose of many such operations is to gather intelligence, DOD has shown a propensity to apply the OPE label where the slightest nexus of a theoretical, distant military operation might one day exist. Consequently, these activities often escape the scrutiny of the intelligence committees, and the congressional defense committees cannot be expected to exercise oversight outside of their jurisdiction.[3088]*

If DOD does not meet its obligations to inform the Committee of intelligence activities, the report warned, the Committee would consider clarifying the Department's obligation to do so.[3089]

Possible Policy Issues for the 111th Congress

The lines defining mission and authorities with regard to covert action are less than clear. The lack of clarity raises a number of policy questions for the 111th Congress, including the following far-from-exclusive list.

- How should Congress define its oversight role? Which committees should be involved?
- Can the U.S. military improve the effectiveness of its intelligence operations without at some point enlisting the support of foreign nationals

---

[3086] See H.Rept. 111-186, accompanying H.R. 2701, the FY2010 Intelligence Authorization Act. See "Committee Statement and Views, D., Areas of Special Interest," Oversight of Intelligence Activities.

[3087] Ibid.

[3088] Ibid.

[3089] Ibid.

in such a way that such activity could be viewed as "non-routine support" to traditional military activities, that is, a covert action?

- Is it appropriate to view U.S. counterterrorism efforts in the context of a global battlefield and to view the military as having the authority to "prepare" that battlefield, and can "anticipated" military action precede the onset of hostilities by months or years?
- Is it appropriate to view the military as being involved in "a war" against terrorists, and thus its activities as constituting "traditional military activities" as it wages that war?
- By asserting that its activities do not constitute covert actions, is the Pentagon trying to avoid the statutory requirements governing covert action, including a signed presidential finding, congressional notification, and oversight by the congressional intelligence committees? Or, as Pentagon officials suggest, is DOD, in the wake of 9/11, fulfilling a greater number of intelligence needs associated with combating terrorism that are sanctioned in statute and do not fall under the statutory definition of covert action?
- Since 1991, when Congress last comprehensively addressed the issue of covert action, has the environment in which the U.S. military operates changed sufficiently to warrant a review of the statute that applies to covert actions?

In his 1991 signing statement, President George H.W. Bush argued that Congress's definition of "covert action" was unnecessary. He went on to state that in determining whether particular military activities constitute covert actions, he would continue to bear in mind the historic missions of the Armed Forces to protect the United States and its interests, influence foreign capabilities and intentions, and conduct activities preparatory to the execution of operations.

Subchapter IV: Protection of Certain National Security Information (50 U.S.C. §§ 421-426)

Intelligence Identities Protection Act, RS21636 (October 3, 2003).

ELIZABETH B. BAZAN, CONGRESSIONAL RESEARCH SERV., INTELLIGENCE IDENTITIES PROTECTION ACT (2003), *available at* http://www.intelligencelaw.com/library/secondary/crs/pdf/RS21636_10-3-2003.pdf.

Order Code RS21636
October 3, 2003

Elizabeth B. Bazan
Legislative Attorney
American Law Division

Summary

Recent news accounts have focused attention on the question of whether disclosure of the identity of a United States intelligence agent could give rise to criminal liability. In 1982, Congress passed the Intelligence Identities Protection Act, P.L.97-200. The Act, as amended,[3090] is codified at 50 U.S.C. §§ 421-426. Under 50 U.S.C. § 421 criminal penalties are provided, in certain circumstances, for intentional, unauthorized disclosure of information identifying a covert agent, where those making such a disclosure know that the information disclosed identifies the covert agent as such and that the United States is taking affirmative measures to conceal the covert agent's foreign intelligence relationship to the United States. Other sections of the Act provide exceptions and defenses to prosecution, make provision for extraterritorial application of the offenses in section 421, include reporting requirements to Congress, and set forth definitions of the terms used in the Act. There do not appear to be any published cases involving prosecutions under this Act.

Introduction

In 1982, the Intelligence Identities Protection Act was enacted into law as an amendment to the National Security Act of 1947. This Act was a response to

---

[3090] Act of July 26, 1947, c. 343, Title VI, §§ 601-606, as added by P.L. 97-200, § 2(a), 96 Stat. 122 (June 23, 1982). The definitions section, 50 U.S.C. § 426, and fine provisions, 50 U.S.C. §§ 421(a), (b), and (c), were amended in 1999 by P.L. 106-120, Title III, §§ 304(a) and (b), 113 Stat. 1611 (Dec. 3, 1999), while the defenses and exceptions provision in 50 U.S.C. § 422 and the reporting requirements in 50 U.S.C. § 423 were amended in 2002 by P.L. 107-306, Title III, §§ 353(b)(1)(B), 353(b)(9), and Title VIII, § 811(b)(1)(E), 116 Stat. 2402, 2422 (Nov. 27, 2002).

concerns of members of the House and Senate Intelligence Committees and others in Congress "about the systematic effort by a small group of Americans, including some former intelligence agency employees, to disclose the names of covert intelligence agents."[3091] The Senate Judiciary Committee's report also discussed the efforts of Philip Agee, Lewis Wolf, and others to identify and disclose U.S. intelligence officers as part of "a systematic effort to destroy the ability of [U.S.] intelligence agencies to operate clandestinely," and their apparent repercussions.[3092] Such disclosures preceded and may have contributed to circumstances resulting in the death or attempted assassination of some CIA officers, expulsion of others from a foreign country following charges of spying, and impairment of relations with foreign intelligence sources. Two of Agee's books revealed over 1,000 names of alleged CIA officers. Wolf was co-editor of the "Covert Action Information Bulletin," a publication which contained a section entitled "Naming Names." Wolf claimed to have revealed the names of over 2,000 CIA officers. He also provided addresses, phone numbers, license tag numbers, and colors of the automobiles of some alleged intelligence agents.[3093] Such calculated disclosures set the stage for the consideration and passage of the Intelligence Identities Protection Act.

The criminal provisions of the Act are contained in 50 U.S.C. § 421:

> *§ 421. Protection of identities of certain United States undercover intelligence officers, agents, informants, and sources*
>
> (a) Disclosure of information by persons having or having had access to classified information that identifies covert agent
>
> *Whoever, having or having had authorized access to classified information that identifies a covert agent, intentionally discloses any information identifying such covert agent to any individual not authorized to receive classified information, knowing that the information disclosed so identifies such covert agent and that the*

[3091] S. Rep. 97-201, at 1, reprinted in 1982 U.S.C.C.A.N. 145. In this report, the Senate Judiciary Committee reviewed the legislative history of S. 391 and the companion bill, H.R. 4, and their predecessors beginning with proposals in the 94th and 95th Congresses. The Congress passed H.R. 4, in lieu of the Senate bill, after amending the House bill to encompass much of the language of the Senate bill.

[3092] S. Rep. 97-201,at 1-7, reprinted in 1982 U.S.C.C.A.N. at 145-51. S. Rep. 97-201, 7-10, reprinted in 1982 U.S.C.C.A.N. at 151-54. See also, H.R. 4, The Intelligence Identities Protection Act: Hearings before the Subcomm. on Legislation of the House Permanent Select Comm. on Intelligence,, 97th Cong., 1st Sess. (1981); Intelligence Identities Protection Act of 1981 — S. 391: Hearing before the Subcomm. on Security and Terrorism of the Senate Comm. on the Judiciary,97th Cong., 1st Sess. (1981).

[3093] S. Rep. 97-201, at 7-10, reprinted in 1982 U.S.C.C.A.N. at 151-54.

United States is taking affirmative measures to conceal such covert agent's intelligence relationship to the United States, shall be fined under Title 18 or imprisoned not more than ten years, or both.

(b) Disclosure of information by persons who learn identify of covert agents as result of having access to classified information

Whoever, as a result of having authorized access to classified information, learns the identity of a covert agent and intentionally discloses any information identifying such covert agent to any individual not authorized to receive classified information, knowing that the information disclosed so identifies such covert agent and that the United States is taking affirmative measures to conceal such covert agent's intelligence relationship to the United States, shall be fined under Title 18 or imprisoned not more than five years , or both.

(c) Disclosure of information by persons in course of pattern of activities intended to identify and expose covert agents

Whoever, in the course of a pattern of activities intended to identify and expose covert agents and with reason to believe that such activities would impair or impede the foreign intelligence activities of the United States, discloses any information that identifies an individual as a covert agent to any individual not authorized to receive classified information, knowing that the information disclosed so identifies such individual and that the United States is taking affirmative measures to conceal such individual's classified intelligence relationship to the United States, shall be fined under Title 18 or imprisoned not more than three years, or both.

(d) Imposition of consecutive sentences

A term of imprisonment imposed under this section shall be consecutive to any other sentence of imprisonment.

Each of these offenses is a felony. Under 18 U.S.C. § 3571, individuals convicted of a felony may be fined the greater of either the amount set forth in the offense statute or an amount not more than $250,000, while the maximum fine for an organization convicted of a felony would be the greater of the amount set forth in the offense statute or an amount of not more than $500,000. This section also provides for an alternative fine based on pecuniary gain or loss. If anyone has

derived pecuniary gain from the offense or if the offense results in pecuniary loss to any person, the defendant may be fined not more than the greater of twice the gross gain or twice the gross loss, unless the imposition of a fine under this subsection would unduly complicate or prolong the sentencing process.

The offenses set forth in 50 U.S.C. §§ 421 (a), (b), and (c) share some elements in common: (1) intentional disclosure[3094] of the identity of a covert agent[3095] (2) to someone not authorized to receive classified information, (3) knowing that the information disclosed identifies that agent, and (4) knowing further that the United States is taking affirmative measures to conceal the agent's intelligence relationship with the United States.

Subsections 421(a) and (b) contemplate offenses where the perpetrator has or has had authorized access to classified information, while subsection 421(c) has no similar requirement. Under 50 U.S.C. § 421(a), an offender must have or have had access to classified information which identifies a covert agent. Under 50 U.S.C. § 421(b), the perpetrator must have learned the identity of a covert agent as a result of having authorized access to classified information. In contrast to these provisions, subsection 421(c) does not require that the perpetrator have or have had authorized access to classified information. Rather, it provides that the perpetrator must disclose the identity of the covert agent (1) in the course of a pattern of activities intended to identify and expose covert agents, and (2) must make the disclosure with reason to believe that his or her activities would impair

---

[3094] 50 U.S.C. § 426 (3) defines "disclose" to mean "to communicate, provide, impart, transmit, transfer, convey, publish, or otherwise make available."

[3095] 50 U.S.C. § 426(4) defines "covert agent" to mean:

(A) a present or retired officer or employee of an intelligence agency or a present or retired member of the armed forces assigned to duty with an intelligence agency —

(i) whose identity as such an officer, employee, or member is classified information, and

(ii) who is serving outside the United States or has within the last five years served outside the United States; or

(B) a United States citizen whose intelligence relationship to the United States is classified information, and —

(i) who resides and acts outside the United States as an agent of, or informant or source of operational assistance to, and intelligence agency, or

(ii) who is at the time of the disclosure acting as an agent of, or informant to, the foreign counterintelligence or foreign counterterrorism components of the Federal Bureau of Investigation; or

(C) an individual, other than a United States citizen, whose past or present intelligence relationship to the United States is classified information and who is a present or former agent of, or a present or former informant or source of operational assistance to, an intelligence agency.

or impede U.S. foreign intelligence activities. Subsection 426(10) defines a "pattern of activities" as involving "a series of acts with a common purpose or objective."

Much of the focus of attention during the consideration of the measure was upon subsection 421(c), and its First Amendment implications.[3096] The Senate Judiciary and the Conference Committee addressed these concerns at length. Both concluded that the language of the measure would pass constitutional muster.[3097] The Conference Committee characterized the goal of the provision as follows:

> *The record indicates that the harm this bill seeks to prevent is most likely to result from disclosure of covert agents' identities in such a course designed, first, to make an effort at identifying covert agents and, second, to expose such agents publicly. The gratuitous listing of agents' names in certain publications goes far beyond information that might contribute to informed public debate on foreign policy or foreign intelligence activities. That effort to identify U.S. intelligence officers and agents in countries throughout the world and to expose their identities repeatedly ... serves no legitimate purpose. It does not alert to abuses; it does not further civil liberties; it does not enlighten public debate; and it does not contribute one iota to the goal of an educated and informed electorate. Instead, it reflects a total disregard for the consequences that may jeopardize the lives and safety of individuals and damage the ability of the United States to safeguard the national defense and conduct an effective foreign policy....*
>
> *The standard adopted in section 601(c) applies criminal penalties only in very limited circumstances to deter those who make it their business to ferret out and publish the identities of agents. At the same time, it does not affect the First Amendment rights of those who disclose the identities of agents as an integral part of another enterprise such as news media reporting of intelligence failures or abuses, academic studies of U.S. government policies and programs, or a private organization's enforcement of its internal rules.[3098]*

[3096] U.S. CONST. Amend I. H. Conf. Rep. 97-580, at 6-8; reprinted in 1982 U.S.C.C.A.N., at 17072.

[3097] S. Rep. 97-201, at 14-18; reprinted in 1982 U.S.C.C.A.N., at 158-62; H. Conf. Rep. 97-580, at 7-10; reprinted in 1982 U.S.C.C.A.N., at 171-75.

[3098] H. Conf. Rep. 97-580, at 7-8; reprinted in 1982 U.S.C.C.A.N., at 171-72.

The Conference Committee distinguished between the main purpose of a person engaged in "the business of 'naming names,'" whose intent is to identify and expose covert agents, and side effects of one's conduct that one "anticipates but allows to occur." "Those who republish previous disclosures and critics of U.S. intelligence would all stand beyond the reach of the law if they did not engage in a pattern of activities intended to identify and expose covert agents."[3099] Despite these assurances, some commentators have questioned the constitutional sufficiency of subsection 421(c) on First Amendment grounds, finding it overbroad, and questioning the absence of a specific intent requirement instead of the "reason to believe" standard.[3100] The courts have yet to consider the issue.

Under 50 U.S.C. § 422, it is a defense to a prosecution under 50 U.S.C. § 421 that, prior to the commission of the offense, the United States publicly acknowledged or revealed the intelligence relationship to the United States of the covert agent involved. In addition, this provision precludes prosecution of anyone other than the person who made the disclosure of the identity of a covert agent for a section 421 offense on the grounds of misprision of felony, aiding and abetting, or conspiracy, unless the elements of subsection 421(c) are satisfied. Nor is it an offense against section 421 for a person to transmit information directly to either the House or Senate intelligence committees. An agent cannot be prosecuted for disclosing just his own identification as a covert agent.

Section 423 requires the President, after receiving information from the Director of Intelligence, to report to the House and Senate intelligence committees annually on measures to protect covert agents, and other relevant information. Such reports are exempt from any publication or disclosure requirement.

Section 424 authorizes extraterritorial jurisdiction where the offender is a U.S. citizen or a permanent resident alien.

Under section 425, the Act may not be construed to permit withholding of information from Congress or a committee of the House or Senate. Finally, section 426 includes the definitions of terms used in this subchapter.

There do not appear to be any published cases involving prosecutions under this Act. Depending upon the circumstances of a given case, other criminal statutes may also be implicated.[3101]

[3099] H. Conf. Rep. 97-580, at 9-10; reprinted in 1982 U.S.C.C.A.N., at 173-74.

[3100] "Note: The Constitutionality of the Intelligence Identities Protection Act," 83 Colum. L. Rev. 727 (1983); "Note: The Intelligence Identities Protection Act of 1982: An Assessment of the Constitutionality of Section 601(c)," 49 Brooklyn L. Rev. 479 (1983).

[3101] See, e.g., 18 U.S.C. § 111 (assaulting, resisting or impeding federal officers or employees while engaged in or on account of the performance of official duties); 18 U.S.C. § 371 (conspiracy to

commit a federal offense); 18 U.S.C. § 641 (theft or knowing conversion to one's own use or the use of another of government property or thing of value); 18 U.S.C. § 793 (gathering, transmitting, or losing information relating to the national defense); 18 U.S.C. § 794 (gathering or delivering defense information to aid a foreign government; among other things, this section provides for a possible death penalty upon conviction upon a finding that the offense resulted in the identification by a foreign power of an individual acting as an agent of the United States and consequently resulted in the death of that individual); 18 U.S.C. § 1114 (killing or attempting to kill an officer or employee of the United States or an agency thereof while the officer or employee is engaged in or on account of performance of official duties). For a recent discussion of the application of 18 U.S.C. § 641 to leaks of confidential government information, see "Stealing Information: Application of a Criminal Anti-Theft Statute to Leaks of Confidential Government Information," 55 Fla. L. Rev. 1043 (2003).

50 U.S.C. Chapter 36: Foreign Intelligence Surveillance (50 U.S.C. §§ 1801-1885c)

Introductory Note

Government Collection of Private Information: Background and Issues Related to the USA PATRIOT Act Reauthorization, R40980 (March 2, 2010)

ANNA C. HENNING, ELIZABETH B. BAZAN, CHARLES DOYLE, & EDWARD C. LIU, CONGRESSIONAL RESEARCH SERV., GOVERNMENT COLLECTION OF PRIVATE INFORMATION: BACKGROUND AND ISSUES RELATED TO THE USA PATRIOT ACT REAUTHORIZATION (2010), , *available at* http://www.intelligencelaw.com/library/secondary/crs/pdf/R40980_3-2-2010.pdf.

Anna C. Henning, Coordinator
Legislative Attorney
ahenning@crs.loc.gov, 7-4067

Elizabeth B. Bazan
Legislative Attorney
ebazan@crs.loc.gov, 7-7202

Charles Doyle
Senior Specialist in American Public Law
cdoyle@crs.loc.gov, 7-6968

Edward C. Liu
Legislative Attorney
eliu@crs.loc.gov, 7-9166

March 2, 2010

Congressional Research Service

7-5700
www.crs.gov

Summary

Congress enacted the USA PATRIOT Act soon after the 9/11 terrorist attacks. The most controversial sections of the act facilitate the federal government's collection of more information, from a greater number of sources, than had previously been authorized in criminal or foreign intelligence investigations. The Foreign Intelligence Surveillance Act (FISA), the Electronic Communications Privacy Act (ECPA), and the national security letter (NSL) statutes were all bolstered. With the changes came greater access to records showing an individual's spending and communication patterns as well as increased authority to intercept e-mail and telephone conversations and to search homes and businesses. In some cases, evidentiary standards required to obtain court approval for the collection of information were lowered. Other approaches included expanding the scope of information subject to search, adding flexibility to the methods by which information could be collected, and broadening the purposes for which information may be sought.

Some perceived the changes as necessary to unearth terrorist cells and update investigative authorities to respond to the new technologies and characteristics of ever-shifting threats. Others argued that authorities granted by the USA PATRIOT Act and subsequent measures could unnecessarily undermine constitutional rights over time. In response to such concerns, sunset provisions were established for many of the changes.

Subsequent measures made most of the USA PATRIOT Act changes permanent. However, three authorities affecting the collection of foreign intelligence information are set to expire on February 28, 2011: the lone wolf, roving wiretap, and business record sections of FISA. The 111th Congress replaced an earlier expiration date with the 2011 date. Before that change was made, the impending expiration prompted legislative proposals which revisit changes made by the USA PATRIOT Act and related measures. Two such bills—the USA PATRIOT Act Sunset Extension Act of 2009 (S. 1692) and the USA PATRIOT Amendments Act of 2009 (H.R. 3845)—were reported from their respective judiciary committees.

In addition to the expiring provisions, these and other bills introduced during the 111th Congress (e.g., S. 1686, S. 1725, S. 1726, S. 2336, H.R. 1800, H.R. 3846, H.R. 3969, and H.R. 4005) address a range of issues, including national security letters, minimization requirements, nondisclosure requirements (gag orders), interception of international communications, and retroactive repeal of communication provider immunity for Terrorist Surveillance Program (TSP) assistance. This report surveys the legal environment in which the legislative proposals arise.

Introduction

Shortly after the 9/11 terrorist attacks, Congress enacted the USA PATRIOT Act, in part, to "provid[e] enhanced investigative tools" to "assist in the prevention of future terrorist activities and the preliminary acts and crimes which further such activities."[3102] To that end, the act eased restrictions on the government's ability to collect information regarding people's activities and conversations, both in domestic criminal investigations and in the realms of foreign intelligence gathering and national security. The changes are perceived by many to be necessary in light of the new breed of threats in a post-9/11 world.[3103] The expanded authorities also prompted concerns regarding the appropriate balance between national security interests and civil liberties.[3104] In part for that reason, the changes were revisited and modified in subsequent measures.[3105]

Several bills introduced during the 111th Congress propose further adjustments to USA PATRIOT Act provisions and related authorities for the government's collection of private information. Two relevant bills—the USA PATRIOT Act Sunset Extension Act of 2009 (S. 1692) and the USA PATRIOT Amendments Act of 2009 (H.R. 3845)—were reported from their respective judiciary committees.[3106]

These and other legislative proposals were catalyzed, in part, by a sunset date (originally December 31, 2009) for three amendments which expanded authorities for the collection of foreign intelligence information.[3107] The sunset

---

[3102] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, P.L. 107-56; H.Rept. 107-236, pt. 1, at 41 (2001).

[3103] See, e.g., Reauthorizing the USA PATRIOT Act: Ensuring Liberty and Security: Hearing Before the S. Judiciary Comm., 111th Cong. (Sept. 23, 2009) (statement of Kenneth L. Wainstein, Partner, O'Melveny & Myers and former Ass't Atty'y Gen. for National Security).

[3104] See, e.g., Unchecked National Security Letter Powers and Our Civil Liberties: Hearing Before the House Perm. Select Comm. on Intelligence, 110th Cong. (Mar. 28, 2007) (statement of Lisa Graves, then Deputy Director, Center for National Security Studies).

[3105] See, e.g., USA PATRIOT Improvement and Reauthorization Act of 2005, P.L. 109-177; An act to amend the USA PATRIOT Act to extend the sunset of certain provisions of that act to July 1, 2006, P.L. 109-160; USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006, P.L. 109-178; Protect America Act of 2007, P.L. 110-55; FISA Amendments Act of 2008, P.L. 110-261.

[3106] Additional relevant proposals include, for example, S. 1686, S. 1725, S. 1726, S. 2336, H.R. 1800, H.R. 3846, H.R. 3969, and H.R. 4005.

[3107] Although the three expiring provisions are thought of as the "expiring Patriot Act provisions," see, e.g., Reauthorizing the USA PATRIOT Act: Ensuring Liberty and Security: Hearing Before the Senate Comm. on the Judiciary, 111th Cong. (Sept. 23, 2009) (statement of Sen. Leahy), only two of the three expiring provisions were enacted in the Patriot Act. See P.L. 107-56, § 206, 50 U.S.C. § 1805(c)(2)(B) (known as the "roving wiretap" provision); Id. at § 215, 50 U.S.C. §§ 1861-2

date is now February 28, 2011.[3108] However, bills introduced during the 111th Congress cover a range of authorities expanded by the USA PATRIOT Act in addition to the expiring provisions.

This report discusses the history of constitutional interpretations and legislative responses relevant to the collection of private information for criminal investigation, foreign intelligence gathering, and national security purposes. Next, it summarizes the relevant statutory frameworks and changes made by the USA PATRIOT Act and subsequent measures. It then examines congressional oversight, judicial review, and "minimization procedures" designed to limit the extent of government intrusions where possible. Finally, it discusses several related matters likely to play a role in the legislative debate surrounding reauthorization of the expiring provisions.

Constitutional Limitations

Constitutional limitations restrict the government's ability to access private information. The Fourth Amendment to the U.S. Constitution is particularly relevant. To the extent that government activity burdens individuals' freedom of speech and related rights, the First Amendment may also play a role.

Fourth Amendment

The Fourth Amendment to the U.S. Constitution provides a right "of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[3109] Many of the government activities discussed in this report have the potential to constitute a search as that term is defined in Fourth Amendment jurisprudence. Namely, government action constitutes a search when it intrudes upon a person's "reasonable expectation of privacy," which requires both that an "individual manifested a subjective expectation of privacy in the searched object" and that "society is willing to recognize that expectation as reasonable."[3110]

Thus, the Fourth Amendment ultimately limits the government's ability to conduct a range of activities, such as physical searches of homes or offices and

---

(known as the "business records" or "library" provision). The third provision, known as the "lone wolf" provision, is Section 6001(a) of the Intelligence Reform and Terrorism Protection Act (IRTPA). P.L. 108-458, 50 U.S.C. § 1801(b)(1)(C).

[3108] P.L. 111-141 (extending the date for the expiring provisions from February 28, 2010, to February 28, 2011). See also Department of Defense Appropriations Act, 2010, P.L. 111-118, § 1004 (extending the date for the expiring provisions from December 31, 2009, to February 28, 2010).

[3109] U.S. Const. amend. IV.

[3110] Kyllo v. United States, 533 U.S. 27, 33 (2001) (citing California v. Ciraolo, 476 U.S. 207, 211 (1986)).

listening to phone conversations. As a general rule, the Fourth Amendment requires the government to demonstrate "probable cause" and obtain a warrant (unless a recognized warrant exception applies) before conducting a search.[3111] This rule applies most clearly in criminal investigations. For example, an officer conducting a criminal investigation typically may not search a person's belongings without first obtaining a warrant that describes the property for which sufficient evidence justifies a search.

The extent to which the Fourth Amendment warrant requirement applies to the government's collection of information for intelligence gathering and other purposes unrelated to criminal investigations is unclear. Although the surveillance of wire or oral communications for criminal law enforcement purposes was held to be subject to the warrant requirement of the Fourth Amendment in 1967,[3112] neither the Supreme Court nor Congress sought to regulate the use of such surveillance for national security purposes at that time. Several years later, the Supreme Court invalidated warrantless electronic surveillance of domestic organizations for national security purposes, but indicated that its conclusion might differ if the electronic surveillance targeted foreign powers or their agents.[3113] A lower court has since upheld the statutory scheme governing the gathering of foreign intelligence information against a Fourth Amendment challenge, despite an assumption that orders issued pursuant to the statute might not constitute "warrants" for Fourth Amendment purposes.[3114] The Supreme Court has not yet directly addressed the issue. However, even if the warrant requirement was found not to apply to searches for foreign intelligence or national security purposes, such searches would

---

[3111] See, e.g., Atwater v. City of Lago Vista, 532 U.S. 318, 354 (2001) (recognizing a warrant exception for arrest of an individual who commits a crime in an officer's presence, as long as the arrest is supported by probable cause). Probable cause is "a fluid concept—turning on the assessment of probabilities in particular factual contexts." Illinois v. Gates, 462 U.S. 213, 232 (1983). For example, for issuance of a search warrant, probable cause requires an issuing magistrate to determine, based on specific evidence, whether there exists a "fair probability" that, for example, an area contains contraband. Id. at 238. Exceptions to the warrant requirement include, for example, "exigent circumstances" where people's lives are at risk or illegal items in "plain view" during a search authorized for other items.

[3112] Katz v. United States, 389 U.S. 347, 353 (1967), overruling Olmstead v. United States, 277 U.S. 438 (1928).

[3113] United States v. U.S. District Court, 407 U.S. 297, 313-14, 321-24 (1972) (also referred to as the Keith case, so named for the District Court judge who initially ordered disclosure of unlawful warrantless electronic surveillance to the defendants). See also In re Directives, 551 F.3d 1004, 1011 (Foreign Intell. Surveillance Ct. Rev. 2008) (holding that the foreign intelligence surveillance of targets reasonably believed to be outside of the U.S. qualifies for the "special needs" exception to the warrant requirement).

[3114] In re Sealed Case, 310 F.3d 717, 738-46 (Foreign Intell. Surveillance Ct. Rev. 2002).

presumably be subject to the general Fourth Amendment "reasonableness" test.[3115]

In contrast with its rulings on surveillance, the Supreme Court has not historically applied the protections of the Fourth Amendment to documents held by third parties. In 1976, it held that financial records in the possession of third parties could be obtained by the government without a warrant.[3116] Later, it likewise held that the installation and use of a pen register—a device used to capture telephone numbers dialed—does not constitute a Fourth Amendment search.[3117] The reasoning was that individuals have a lesser expectation of privacy with regard to information held by third parties.

First Amendment

The First Amendment to the U.S. Constitution restricts government efforts to prohibit the free exercise of religion or to abridge free speech, freedom of the press, the right to peaceful assembly, or the right to petition for redress of grievances.[3118] Two First Amendment concerns arise with regard to electronic surveillance, access to records, and related investigatory activities. One addresses direct restrictions on speech that may accompany government collection of private information, such as non-disclosure requirements accompanying orders compelling government access to business records, discussed infra. A second concern is that overly broad authorities permitting government intrusion may lead to a "chilling" (i.e., stifling) effect on public discourse.[3119] Some post-9/11 laws address the latter issue directly, for example by prohibiting investigations based solely on a person's First Amendment activities.[3120] Despite safeguards,

---

[3115] The "general reasonableness," or "totality-of-the circumstances," test requires a court to determine the constitutionality of a search or seizure "by assessing, on the one hand, the degree to which [a search or seizure] intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests." Samson v. California, 547 U.S. 843, 848 (2006).

[3116] United States v. Miller, 425 U.S. 435 (1976).

[3117] Smith v. Maryland, 442 U.S. 735, 745-46 (1979).

[3118] U.S. Const. amend. I.

[3119] See U.S. District Court, 407 U.S. at 314 ("The price of lawful public dissent must not be a dread of subjection to an unchecked surveillance power. Nor must the fear of unauthorized official eavesdropping deter vigorous citizen dissent and discussion of Government action in private conversation. For private dissent, no less than open public discourse, is essential to our free society.").

[3120] See, e.g., 50 U.S.C. § 1842(c).

there is concern that post-9/11 authorities may have been used to circumvent First Amendment limitations on analogous authorities.[3121]

History of Congressional Action Congress addressed the federal government's access to private information following key Supreme Court decisions interpreting the Fourth Amendment. In 1968, it enacted legislation, Title III of the Omnibus Crime Control and Safe Streets Act, which outlawed the unauthorized interception of wire or oral communications and authorized interception under court supervision for law enforcement purposes.[3122] Later, it passed the Electronic Communications Privacy Act (ECPA), which incorporated and modernized Title III to cover electronic as well as wire and oral communications.[3123]

In the years following the Supreme Court's 1972 ruling on surveillance (the "Keith case"), Congress actively examined the intelligence practices of past presidential administrations and found that every administration since Franklin D. Roosevelt engaged in electronic surveillance without prior judicial approval.[3124] It also found that the authority was sometimes abused.[3125] Partly in light of these findings, Congress enacted the Foreign Intelligence Surveillance Act (FISA)[3126] to create a statutory framework for the use of electronic surveillance to collect foreign intelligence information.

[3121] See, e.g., Office of the Inspector General, Department of Justice, A Review of the FBI's Use of Section 215 Orders for Business Records in 2006, Mar. 2008, http://www.usdoj.gov/oig/special/s0803a/final.pdf, at 5 (expressing concern that the FBI had issued a national security letter after the FISA court had twice declined to grant an order for the same material due to First Amendment objections).

[3122] P.L. 90-351, 18 U.S.C. §§ 2510-2520 (1970 ed. Supp.IV).

[3123] P.L. 99-508, 18 U.S.C. §§ 2510-2520 (1988 ed. Supp.II).

[3124] See S. Rept. 95-604(I), at 7, 1978 U.S.C.C.A.N. 3904, 3908.

[3125] The report of a congressional committee convened to examine intelligence gathering after Watergate stated: "Too many people have been spied upon by too many government agencies and too much information has been collected. The government has often undertaken the secret surveillance of citizens on the basis of their political beliefs, even when those beliefs posed no threat of violence or illegal acts on behalf of a hostile foreign power. The Government, operating primarily through secret informants, but also using other intrusive techniques such as wiretaps, microphone 'bugs', surreptitious mail opening, and break-ins, has swept in vast amounts of information about the personal lives, views, and associations of American citizens." See Intelligence Activities and the Rights of Americans, Final Report of the Select Committee to Study Governmental Operations with respect to Intelligence Activities and the Rights of Americans, United States Senate, Book II, S. Rept. 94-755, at 5 (1976) (hereinafter Church Committee Final Report). See also Supplementary Detailed Staff Reports on Intelligence Activities and the Rights of Americans, Church Committee Final Report,, Book III, S. Rept. 94-755, at 271-351.

[3126] P.L. 95-511, 50 U.S.C. § 1801 et seq.

Similarly, in response to the Supreme Court's rulings regarding the Fourth Amendment's non-application to documents held by third parties, Congress enacted the Right to Financial Privacy Act (RFPA)[3127] to constrain government authorities' access to individuals' financial records. Although these privacy protections are subject to a foreign intelligence exception,[3128] government authorities were not authorized to compel financial institutions to secretly turn over financial records until 1986.[3129] That year, the FBI was also given authority, in the form of FBI-issued "national security letters," to access customer records held by telephone companies and other communications service providers in specified instances justified by a national security rationale.[3130] Two additional national security letter authorities were enacted in the mid-1990s. The first provided access to credit and financial records of federal employees with security clearances.[3131] The second gave the FBI access to credit agency records in order to facilitate the identification of financial institutions utilized by the target of an investigation.[3132]

Intelligence gathering laws were expanded during the same time period. In 1994, FISA was amended to cover physical searches for foreign intelligence purposes.[3133] Four years later, Congress amended FISA to permit the Foreign Intelligence Surveillance Court to issue orders authorizing

(1) the use of pen registers and trap and trace devices to track calling patterns;[3134] and (2) the production of some business records not available through existing national security letter authorities.[3135]

The USA PATRIOT Act,[3136] enacted in 2001, represented a broad expansion of existing statutory authorities. It eliminated barriers to cooperation between law

---

[3127] P.L. 95-630, § 1114, 12 U.S.C. § 3401 et seq.

[3128] 12 U.S.C. § 3414(a)(1)(A), (B).

[3129] P.L. 99-569, § 404, 12 U.S.C. § 3414(a)(5)(A).

[3130] Electronic Communications Privacy Act, P.L. 99-508, § 201(a), 18 U.S.C. § 2709.

[3131] P.L. 103-359, § 802, 50 U.S.C. § 436.

[3132] P.L. 104-93, § 601(a), 15 U.S.C. § 1681u.

[3133] P.L. 103-359, § 807(a)(3), 50 U.S.C. §§ 1821-1829.

[3134] Pen registers capture the numbers dialed on a telephone line; trap and trace devices identify the originating number of an incoming call on a particular phone line. See 18 U.S.C. § 3127(3)-(4).

[3135] P.L. 105-272, §§ 601, 602.

enforcement and foreign intelligence investigations, modified surveillance authorities under both FISA and ECPA, and created a fifth category of national security letters. Many of these provisions were made temporary, subject to sunset in 2005.[3137]

In 2004, Congress enacted the Intelligence Reform and Terrorism Prevention Act. Among other things, the act amended FISA to allow targeting so-called "lone wolves" or individuals believed to be engaged in terrorism, but who were not linked to a known terrorist organization.[3138] The "lone wolf" provision was given an expiration date to match that which applied to many of the USA PATRIOT Act provisions.

The next year, Congress reauthorized the USA PATRIOT Act, making the majority of its expiring provisions permanent.[3139] However, two of its most controversial provisions, discussed infra, together with the 2004 lone wolf provision, were given a new sunset date of December 31, 2009.[3140]

Also in 2005, President Bush acknowledged that he had authorized a Terrorist Surveillance Program (TSP), which captured some international communications apparently procured without judicial or statutory authority. As discussed infra, Congress subsequently enacted the Protect America Act and the FISA Amendments Act of 2008, which addressed issues raised in response to the TSP.

In December 2009 and again in February 2010, Congress temporarily extended the sunset date for the lone wolf and two USA PATRIOT Act provisions which were scheduled to sunset in 2009.[3141] They are now set to expire on February 28, 2011.

Statutory Framework

The applicable statutory regime or procedural rules differ according to the purpose for which the federal government collects private information. In criminal law enforcement investigations, the Federal Rules of Criminal Procedure, ECPA, and other provisions in Title 18 of the U.S. Code apply. In

---

[3136] P.L. 107-56.

[3137] Id. at § 224.

[3138] P.L. 108-458, § 6001.

[3139] P.L. 109-177, § 102(a).

[3140] Id. at §§ 102(b), 103.

[3141] Department of Defense Appropriations Act, 2010, P.L. 111-118, § 1004 (extending the expiration date to February 28, 2010); P.L. 111-141 (extending the date to February 28, 2011).

contrast, the collection of foreign intelligence information is governed by FISA. Finally, five national security statutes, discussed infra, regulate the issuance of national security letters. Statutes in these areas provide analogous authorities for various government activities but require that different standards and procedures be satisfied.

Federal Rules of Criminal Procedure and Subpoena Authorities

In criminal cases, federal officials ordinarily gain access to spaces, documents, and other private materials pursuant to a warrant (during investigation) or a subpoena (during prosecution). In criminal investigations, Federal Rule of Criminal Procedure 41 provides procedures applicable to search warrants to obtain evidence of a crime; contraband, fruits of crime, or other items illegally possessed; or property "designed for use, intended for use, or used in committing a crime."[3142]

During the indictment phase, federal grand juries have the power to investigate the possibility that a federal crime has been committed within the judicial district in which they are convened and enjoy the benefit of the subpoena power of the court within whose district they sit.[3143] However, grand jury subpoenas are limited. Namely, like criminal search warrants, their purpose must have a criminal nexus.

Other subpoena authorities include those issued during the discovery or trial phases of a criminal prosecution and those issued by federal agencies pursuant to specific statutes.[3144] Although they are analogous to authorities relied upon to acquire third party documents in national security or foreign intelligence gathering investigations, agency administrative subpoenas and grand jury subpoenas are unlikely to provide an alternative means to acquire third party

[3142] Fed. R. Crim. Pro. 41(c). See also 18 U.S.C. § 3103a (adding to the grounds provided in Rule 41 that "a warrant may be issued to search for or seize any property that constitutes evidence of a criminal offense in violation of the laws of the United States," and permitting delayed notice of a search in some circumstances). In general, statutes in Title 18 of the U.S. Code governing searches and seizures in criminal cases incorporate relevant sections of Federal Rule of Criminal Procedure 41 by reference. See, e.g., 18 U.S.C. § 3103 (incorporating the grounds for which a search warrant may be issued). However, some provisions add statutory requirements. See, e.g., 18 U.S.C. § 3109 (adding procedures for breaking doors or windows to execute a search warrant).

[3143] United States v. Williams, 504 U.S. 36, 48 (1992).

[3144] For example, administrative subpoenas are available for use in the investigation by the Drug Enforcement Administration; by federal agency inspectors general; and in health care fraud, child abuse, and presidential protection investigations. See 21 U.S.C. § 876; 5 U.S.C. App. (III) § 6; 18 U.S.C. § 3486.

documents in a national security investigation and thus have not been a significant issue in post 9/11 legislation.[3145]

Electronic Communications Privacy Act (ECPA)

The Electronic Communications Privacy Act (ECPA) provides three sets of general prohibitions accompanied by law enforcement exceptions that operate under judicial supervision.[3146] These address (1) the interception of wire, oral or electronic communications (wiretapping);[3147] (2) access to the content of stored electronic communications and to communications transaction records;[3148] and (3) the use of trap and trace devices and pen registers (essentially in and out secret "caller id" devices).[3149]

ECPA generally prohibits interception of wire, oral, or electronic communications by means of an electronic, mechanical or other device but sets forth a number of exceptions to the general prohibition.[3150] It limits the types of criminal cases in which electronic surveillance may be used and requires court orders authorizing electronic surveillance to be supported by probable cause to believe that the target is engaged in criminal activities, that normal investigative techniques are insufficient, and that the facilities that are the subject of surveillance will be used by the target.[3151] It also limits the use and dissemination of information

---

[3145] Subpoena authorities are unlikely to substitute for authorities applicable in national security investigations. For administrative subpoenas, one reason is that relevant statutes do not impose a gag order component; thus, national security information might be compromised. More importantly, national security investigations and the type of investigations in which such subpoenas may be used will only rarely coincide. However, criminal investigations in which grand jury subpoenas are sought may intersect with foreign intelligence investigations under FISA in situations involving criminal conduct that also has national security implications, such as international terrorism or espionage.

[3146] See CRS Report 98-326, Privacy: An Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping, by Gina Stevens and Charles Doyle, for a more detailed discussion of the federal laws governing wiretapping and electronic eavesdropping, along with appendices including copies of the texts of ECPA and FISA.

[3147] 18 U.S.C. §§ 2510-2522.

[3148] 18 U.S.C. §§ 2701-2712.

[3149] 18 U.S.C. §§ 3121-3127. Pen registers capture the numbers dialed on a telephone line; trap and trace devices identify the originating number of a call on a particular phone line. See 18 U.S.C. § 3127(3)-(4).

[3150] 18 U.S.C. § 2511.

[3151] 18 U.S.C. §§ 2516, 2518(3).

intercepted.[3152] In addition, when an interception order expires, authorities must notify those whose communications have been intercepted.[3153] Moreover, it declares that the FISA and ECPA procedures are the exclusive means for accomplishing electronic surveillance as defined in FISA and for intercepting wire, oral, or electronic communications.[3154]

Whereas provisions governing interception of communications in criminal investigations reflect a concern for Fourth Amendment requirements,[3155] portions of ECPA which address stored communications and the use of pen registers and trap and trace devices are less demanding and reflect Supreme Court jurisprudence suggesting that third party business records and communications entrusted to third parties are not typically protected.[3156] Government authorities may have access to communications stored with providers, and related communications records, under a search warrant, subpoena, or court order,[3157] or when voluntarily surrendered by providers in emergency circumstances.[3158] However, as with the interception of communications, ECPA limits the government's use and dissemination of information and requires that targets be notified.[3159]

Foreign Intelligence Surveillance Act (FISA)

FISA governs the gathering of information about foreign powers, including international terrorist organizations such as al Qaeda, and their agents.[3160]

[3152] 18 U.S.C. § 2517.

[3153] 18 U.S.C. § 2518(8).

[3154] 18 U.S.C. § 2511(2)(f). FISA defines electronic surveillance to include more than the interception of wire, oral, or electronic communications, 50 U.S.C. § 1801(f), but places limitations on its definition based upon the location or identity of some or all of the parties to the communications involved.

[3155] Berger v. New York, 388 U.S. 41 (1967); Katz v. United States, 389 U.S. 347 (1967); S. Rept. 90-1097, at 66 (1967).

[3156] Smith v. Maryland, 442 U.S. 735 (1979); United States v. Miller, 425 U.S. 435 (1976); S. Rept. 99-541, at 3 (1986).

[3157] 18 U.S.C. § 2503. But communications held by electronic communications providers for less than 180 days require a warrant, 18 U.S.C. § 2703(a).

[3158] 18 U.S.C. § 2702.

[3159] 18 U.S.C. §§ 2517, 2518(8).

[3160] See 50 U.S.C. § 1801(a) (definition of "foreign power").

Although it is often discussed in relation to the prevention of terrorism, it applies to the gathering of foreign intelligence information for other purposes.[3161]

Although some exceptions apply,[3162] government agencies typically must obtain authorization from the Foreign Intelligence Surveillance Court (FISC), a neutral judicial decision maker, when gathering foreign intelligence information pursuant to FISA. Orders issued by the FISC authorize federal officials to conduct electronic surveillance[3163] or physical searches;[3164] utilize pen registers and trap and trace devices;[3165] access specified business records and other tangible things;[3166] or target U.S. persons reasonably believed to be abroad.[3167]

Although requiring a nexus to a foreign power or foreign intelligence is a common theme, different standards apply for each type of FISA order. For electronic surveillance orders, FISA currently requires that an application include, among other things, a "statement of the facts and circumstances relied upon" to justify the government's belief that a target is a foreign power or its agent.[3168] It must also describe the identity, if known, or a description of the

---

[3161] For example, it extends to the collection of information necessary for the conduct of foreign affairs. See 50 U.S.C. § 1801(e) (definition of "foreign intelligence information").

[3162] For example, FISA provides for emergency authorization of electronic surveillance or a physical search by the Attorney General in some circumstances, while an order is sought. 50 U.S.C. §§ 1805(e) and 1824(e), respectively. It also allows physical searches to be conducted in absence of a court order for periods of up to one year where the target is a foreign nation or component of a foreign nation, a faction of a foreign nation or nations not substantially composed of U.S. persons, or an entity openly acknowledged by a foreign government or governments to be directed and controlled by such government or governments, as long as the Attorney General: (1) certifies that the physical search is directed solely at a foreign power, there is no substantial likelihood that the search will "involve the premises, information, material, or property of a United States person," and proposed minimization procedures meet specified standards; and (2) fulfills various reporting requirements regarding minimization procedures. 50 U.S.C. § 1822. See also 50 U.S.C. § 1802 (electronic surveillance of such foreign powers for up to one year without a court order).

[3163] 50 U.S.C. §§ 1801-1808. FISA authorizes electronic surveillance without a FISA order in specified instances involving communications between foreign powers. 50 U.S.C. § 1802.

[3164] 50 U.S.C. §§ 1822-1826.

[3165] 50 U.S.C. §§ 1841-1846.

[3166] 50 U.S.C. §§ 1861-1862.

[3167] 50 U.S.C. §§ 1881b, 1881c. As discussed infra, FISA also currently includes a statutory framework for targeting non-U.S. persons abroad to acquire foreign intelligence information pursuant to a joint Attorney General/Director of National Intelligence (DNI) authorization in specified circumstances. 50 U.S.C. § 1881a.

[3168] 50 U.S.C. § 1804(a)(4).

specific target of the electronic surveillance and the nature and location of each of the facilities or places at which the electronic surveillance will be directed, if known.[3169] When the nature and location are unknown, the FISC must direct the relevant officials to provide notice to the FISC of specific information within 10 days of the date on which surveillance begins to be directed at a new facility or place.[3170] FISA also requires that less intrusive means of information gathering be used before an electronic surveillance order may be granted. Specifically, an application for an order authorizing electronic surveillance must include a certification that the information sought under the order is foreign intelligence information, and that the information may not reasonably be obtained by normal investigative techniques, together with a statement of the basis upon which such certifications rest.[3171] Relatedly, an application for an electronic surveillance order must specify proposed "minimization procedures."[3172]

For physical searches, the government typically must provide, among other things, "the identity, if known, or a description of the target of the search," and "a statement of the facts and circumstances relied upon by the applicant to justify the applicant's belief that ... the target of the physical search is a foreign power or an agent of a foreign power."[3173]

For FISA orders authorizing pen registers and trap and trace devices, although limited exceptions apply,[3174] an application generally must certify that "the information likely to be obtained is foreign intelligence information not concerning a United States person or is relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities."[3175]

Finally, for orders to access records and other tangible things, FISA currently requires both "a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to a [foreign intelligence,

---

[3169] 50 U.S.C. §§ 1804(a)(2); 1805(c)(1)(A) and (B).

[3170] 50 U.S.C. § 1805(a)(3).

[3171] 50 U.S.C. § 1804(a)(7)(C) and (E).

[3172] Id. at § 1804(a)(5). Minimization procedures, examined in greater detail infra, are safeguards which limit the government's use of collected information.

[3173] 50 U.S.C. § 1823(a).

[3174] The exceptions authorize: (1) emergency authorization by the Attorney General for up to 48 hours, if specified criteria are met, while an application for a FISC order is pursued; and (2) the installation and use of pen registers and trap and trace devices for up to 15 calendar days following a congressional declaration of war). 50 U.S.C. §§ 1843, 1844.

[3175] 50 U.S.C. § 1842(c).

international terrorism, or espionage investigation]" and an "enumeration of minimization procedures" to be applied.[3176] These provisions also include recipient non-disclosure provisions, grounds for recipients to challenge such production or nondisclosure requirements, and government reporting requirements.[3177]

Many of these statutes include a requirement intended to safeguard individuals' freedom of speech and other First Amendment protections. In particular, investigations generally must not be based solely on a U.S. citizen's exercise of his or her First Amendment rights.[3178]

National Security Letter Statutes

Five federal statutes require businesses—namely communications providers, financial institutions, and consumer credit entities—to produce specified records to federal officials in national security investigations.[3179] Absent a statutory prohibition or some other specific legal impediment, federal authorities are free to request, and to receive voluntarily, access to third party business records. These national security letter (NSL) statutes are designed to carve out narrow national security exceptions to prohibitions on government information gathering in ECPA, the Right to Financial Privacy Act, and the Fair Credit Reporting Act.

Unlike with warrants in criminal investigations or orders issued under FISA, NSLs are issued directly by federal officials, without approval by any judicial body. They are analogous to orders for tangible things issued in intelligence gathering investigations pursuant to FISA because they are a demand for business records and their use is confined to national security investigations. Yet unlike FISA orders, they are not issued by a court and are available for only the records of three narrow categories of businesses. Moreover, the FBI issues tens of

---

[3176] 50 U.S.C. § 1861(b)(2).

[3177] 50 U.S.C. §§ 1861-1862.

[3178] See, e.g., 50 U.S.C. §§ 1805(a)(2)(A) (electronic surveillance), 1824(a)(2)(A) (physical searches),1842(c) (pen register or trap and trace device).

[3179] The NSL statutes are: 18 U.S.C. § 2709 of ECPA; section 1114(a)(5) of the Right to Financial Privacy Act (12 U.S.C. § 3414(a)(5)); sections 626 and 627 of the Fair Credit Reporting Act (15 U.S.C. §§1681u and 1681v); and section 802 of the National Security Act of 1947 (50 U.S.C. § 436). For a more detailed discussion of the NSL statutes and the proposals to amend them see, CRS Report RL33320, National Security Letters in Foreign Intelligence Investigations: Legal Background and Recent Amendments, by Charles Doyle, and CRS Report R40887, National Security Letters: Proposed Amendments in the 111th Congress, by Charles Doyle.

thousands of NSLs a year,[3180] while the FISA court approves only a handful of tangible-item orders a year.[3181]

Only the FBI may issue NSLs under the communications provider, financial institution, and the narrower of the two consumer credit agency statutes. Authority under the other consumer credit agency statute is available to the agencies of the intelligence community, and authority under the National Security Act extends to both intelligence and law enforcement agencies.

The information available under each of the statutes varies. The National Security Act statute reaches an extensive array of financial and consumer credit records, but only applies to federal employees and individuals who have consented to disclosure of the information.[3182] The more sweeping consumer credit statute extends to any consumer information held by a consumer credit reporting agency but only when sought in connection with an investigation into international terrorism.[3183] The communications provider NSL statute applies to provider transaction records concerning customers' names, addresses, length of service, and billing records sought in connection with an inquiry into international terrorism or clandestine intelligence activities.[3184] The more circumspect of the consumer credit NSL statutes covers credit agency records concerning consumers' names, current and former addresses, current and former places of employment, and the identification of financial institutions in which they have or had accounts—sought in connection with an inquiry into international terrorism and clandestine intelligence activities.[3185] The financial institution NSL statute reaches customer transaction records of banks, credit unions, and a long list of other businesses that often deal in cash (pawn shops, casinos, car dealerships, jewelers, etc.), again sought in connection with an inquiry into international terrorism and clandestine intelligence activities.[3186]

[3180] According to reports by the Department of Justice Inspector General's Office, the FBI issued 39,346 NSL requests in 2003, 56,507 in 2004, 47,221 in 2005, and 49,425 in 2006. Office of the Inspector General, U.S. Department of Justice, A Review of the Federal Bureau of Investigation's Use of National Security Letters (March 2008) at 110.

[3181] The Justice Department reported that the FISA court issued 13 tangible item orders in 2008 and 17 in 2007, Letters dated May 14, 2009 from Ass't Att'y Gen. Ronald Weich to Vice-President Biden, Senators Reid and McConnell, Speaker Pelosi, and Congressmen Hoyer and Boehner, http://www.justice.gov/nsd/foia/reading_room/2008fisa-ltr.pdf.

[3182] 50 U.S.C. § 436.

[3183] 15 U.S.C. § 1681v.

[3184] 18 U.S.C. § 2709.

[3185] 15 U.S.C. § 1681u.

[3186] 12 U.S.C. § 3414(a)(5).

NSL recipients may be bound by nondisclosure requirements under each of the statutes.[3187] However, they may seek judicial review of any secrecy requirement imposed and of the NSL itself.[3188]

Changes Made by the USA PATRIOT Act and Subsequent Measures

The USA PATRIOT Act and subsequent measures made far-reaching changes expanding the government's authority to collect private information pursuant to FISA, ECPA, and the NSL statutes.[3189] Absent congressional intervention, three of the amendments to FISA—the lone wolf, roving wiretap, and business record provisions—will expire on February 28, 2011.

Lowering of the Wall Between Criminal Investigations and Foreign Intelligence Gathering

The USA PATRIOT Act lowered somewhat the wall traditionally separating criminal investigation from foreign intelligence gathering. Prior to the act, FISA required that foreign intelligence gathering be the sole or primary purpose of an investigation; thus, activities conducted with an additional rationale of criminal investigation were required to adhere to criminal procedure requirements. Section 218 of the act amended the standard to require that foreign intelligence gathering be a "significant" rather than "the [sole]" purpose of surveillance or a search for which a court order is sought under FISA.[3190] Thus, the presence of ancillary criminal investigation purposes no longer eliminates the ability to rely on FISA authorities, so long as a significant foreign intelligence purpose also exists. Relatedly, as discussed infra, the USA PATRIOT Act and subsequent measures increased the scope of international terrorism-related activities which now fall within the ambit of the federal criminal code.

The act also attempted to improve communication between foreign intelligence and criminal law enforcement agencies. To that end, it includes several provisions that authorize information sharing. For example, section 504

[3187] The terms "nondisclosure requirements," "secrecy requirements," and "gag orders" are used interchangeably throughout this report.

[3188] 18 U.S.C. § 3511; John Doe, Inc. v. Mukasey, 549 F.3d 861 (2d Cir. 2008). See also discussion regarding judicial oversight, infra.

[3189] Expansions were also made to some related authorities. For example, the USA PATRIOT Act and subsequent legislation amended the grand jury secrecy rule to permit prosecutors to disclose grand jury information to federal, state, local, or foreign law enforcement or intelligence officials under certain circumstances.

[3190] 50 U.S.C. § 1804(a)(7)(B) (electronic surveillance); 50 U.S.C. § 1823(a)(7)(B) (physical searches).

authorizes federal officers to consult with criminal law enforcement officers regarding information obtained from a physical search in order "to coordinate efforts to investigate or protect against" various national security threats.[3191]

Expansion of Persons Subject to Investigation

Several post-9/11 measures addressed threshold or definitional issues affecting the range of persons whose communications, records, or effects might be investigated as part of foreign intelligence gathering. The controversial 2004 lone wolf provision, one of the three expiring provisions, is especially significant. It expanded the definition of "agent of a foreign power" in FISA to include a non-U.S. person who "knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power."[3192] Because FISA orders—including those for surveillance, physical searches, pen registers, trap and trace devices, and business records—require evidence indicating that a target is a foreign power or its agent, the broadened definition makes the authorities applicable to targets for which a link to an international terrorist organization or other foreign power is not yet supported by probable cause.[3193]

Another important expansion followed in the wake of revelations regarding the Terrorist Surveillance Program. Two measures, discussed in greater detail infra,[3194] eased federal officials' ability to gather foreign intelligence information between persons in the United States and others thought to be located outside of the United States. In the first, now expired, measure, Congress exempted "surveillance directed at a person reasonably believed to be located outside of the United States" from the definition of "electronic surveillance" under FISA.[3195] Although this made it unnecessary to obtain a FISA order to conduct such surveillance, Congress simultaneously established temporary procedures governing the capture of communications for specified groups of targets

---

[3191] 50 U.S.C. § 1806(k)(1) (electronic surveillance); 50 U.S.C. § 1825 (physical searches).

[3192] Id. at § 6001(a); 50 U.S.C. § 1801(b)(1)(C).

[3193] But see Letter from Assistant Attorney General Ronald Weich to Hon. Patrick J. Leahy, at 5 (Sept. 14, 2009), http://judiciary.senate.gov/resources/documents/111thCongress/upload/091409WeichtoLeahy.pdf (indicating that the lone wolf provision has not yet been relied upon in a federal investigation). For more information regarding the lone wolf provision and the other expiring amendments to FISA, see CRS Report R40138, Amendments to the Foreign Intelligence Surveillance Act (FISA) Set to Expire February 28, 2011, by Anna C. Henning and Edward C. Liu.

[3194] See discussion regarding the aftermath of the Terrorist Surveillance Program.

[3195] The Protect America Act of 2007, P.L. 110-55.

reasonably believed to be located overseas.[3196] The second measure provides separate authorities with differing standards for targeting non-U.S. persons and U.S. persons reasonably believed to be located outside the United States.[3197]

Finally, by authorizing the collection of information believed to be relevant to a national security or foreign intelligence investigation, the USA PATRIOT Act and its successors in several instances widened the circle of persons whose communications or effects might fall within the ambit of authorities for intelligence gathering.[3198] Authorities had previously limited that circle to persons believed to be agents of foreign powers.

Expansion of Electronic Surveillance Authorities

The USA PATRIOT Act amended electronic surveillance authorities in ECPA and FISA. The amendments to ECPA primarily address matters other than the interception of the content of communications. However, the act did add several terrorism-related offenses to the list of federal crimes that may serve as the basis for an interception order.[3199] It also authorizes intercepting officers to share information with various federal intelligence and law enforcement officials[3200] and provides explicit disciplinary provisions for intentional violations by federal employees.[3201]

Moreover, section 217 created a new exception to ECPA's general prohibition on the interception of electronic communications. The exception permits law enforcement officials to intercept the communications of an intruder into someone else's computer or computer system with the consent of system's owner or operator.[3202] The exception is limited to the trespasser's communications to, through, and from the invaded system.

An additional important amendment to ECPA broadened the stored communication language in an effort to treat stored voice mail in the same

---

[3196] Id.

[3197] The FISA Amendments Act of 2008, P.L. 110-261.

[3198] See, e.g., P.L. 109-177, § 106(b), 50 U.S.C. §§ 1861-1863; P.L. 107-56, § 505(a)(3), 18 U.S.C. § 2709.

[3199] P.L. 107-56, §§ 201, 202, 18 U.S.C. § 2516(1).

[3200] P.L. 107-56, § 203(b), 18 U.S.C. §§ 2510(19), 2517(1).

[3201] P.L. 107-56, § 223(a), 18 U.S.C. § 2520(f).

[3202] P.L. 107-56, § 217, 18 U.S.C. §§ 2511(2)(i), 2510(21).

manner as e-mail.[3203] Finally, section 220 amended ECPA to permit nationwide service of search warrants of material held by service providers,[3204] and section 212 amended it to allow for emergency disclosures by service providers.[3205]

Likewise, the USA PATRIOT Act and its progeny made several changes to FISA's electronic surveillance authorities. The so-called "roving wiretap" provision, section 206 of the USA PATRIOT Act, permits roving or multipoint wiretaps where the Foreign Intelligence Surveillance Court finds that the actions of the target of the application for electronic surveillance under FISA may have the effect of thwarting the identification of a specific communications or other common carrier, landlord, custodian, or specified person to whom the order to furnish information, facilities, or technical assistance in connection with the wiretap should be directed.[3206] As amended by P.L. 109-177, this finding must be based upon specific facts provided in the application.[3207] In addition, section 207 of the USA PATRIOT Act extended the duration of FISA wiretaps and extensions thereof.[3208]

Section 225 added a new provision to FISA that bars suits against any wire or electronic service provider, custodian, landlord, or other person that furnishes information, facilities, or technical assistance in connection with electronic surveillance pursuant to a FISC order or with a request for emergency assistance under FISA.[3209]

Expansion of Authorities to Conduct Physical Searches

"Physical searches," as defined by FISA, are analogous to searches authorized by warrants in criminal investigations.[3210] The most notable amendment specific to

---

[3203] P.L. 107-56, § 209, 18 U.S.C. §§ 2703, 2510(14).

[3204] P.L. 107-56, § 220, 18 U.S.C. §§ 2711, 2703.

[3205] P.L. 107-56, § 212, 18 U.S.C. § 2702.

[3206] 50 U.S.C. § 1805(c)(2)(B).

[3207] Id.

[3208] P.L. 107-56, § 207, 50 U.S.C. § 1805(e).

[3209] P.L. 107-56, § 225, 50 U.S.C. § 1805(i). This section was expanded by section 314(a)(2)(D) of the Intelligence Authorization Act for Fiscal Year 2002, P.L. 107-108, to cover those who provide such assistance in connection with a FISA order authorizing a physical search or emergency assistance.

[3210] The definition of "physical search" in FISA incorporates the standard—"reasonable expectation of privacy"—which typically triggers the Fourth Amendment warrant requirement in criminal investigations. See 50 U.S.C. § 1821(5) (defining "physical search" as: "any physical

FISA provisions governing orders for physical searches, made by section 207 of the USA PATRIOT Act, increased the maximum duration of physical search orders targeting persons other than a foreign power.[3211] The maximum duration of such orders was 45 days but is now 120 days for searches targeting an agent of a foreign power and 90 days for other targets.[3212]

Expansion of Authorities for Pen Registers and Trap and Trace Devices

The USA PATRIOT Act amended both FISA and ECPA provisions relevant to the use of pen register and trap and trace devices. The most notable amendment to FISA was made in section 214. Previously, the use of pen registers and similar devices could be authorized only for investigations to gather foreign intelligence information or information concerning international terrorism. Section 214 broadened the purposes for which the devices may be authorized by allowing their use in "any investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities."[3213] However, it prohibits any investigation involving a United States person that is "conducted solely upon the basis of activities protected by the first amendment to the Constitution."[3214]

Section 216 amended the ECPA to authorize courts to issue orders for the use of pen registers and trap and trace devices anywhere within the United States.[3215] The statute previously limited their application to the issuing court's jurisdiction. It also authorizes the use of such devices to capture source and addressee information for computer conversations (e.g., e-mail) as well as telephone conversations.[3216]

---

intrusion within the United States into premises or property (including examination of the interior of property by technical means) that is intended to result in a seizure, reproduction, inspection, or alteration of information, material, or property, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, but does not include (A) "electronic surveillance" ... or (B) the acquisition by the United States Government of foreign intelligence information from international or foreign communications, or foreign intelligence activities conducted in accordance with otherwise applicable Federal law ....") (emphasis added).

[3211] P.L. 107-56, §207, 50 U.S.C. § 1824(d). The maximum duration of a physical search order targeting a foreign power was and is one year.

[3212] Id.

[3213] P.L. 107-56, §214, 50 U.S.C. § 1842(a)(1).

[3214] Id.

[3215] P.L. 107-56, §216, 18 U.S.C. § 3123(a).

[3216] 18 U.S.C. §§ 3121, 3123.

Expanded Access to Records and Other Tangible Things

As mentioned, the USA PATRIOT Act focused in part on the statutory tools available in antiterrorism investigations. Some of those tools enable agents to unearth documents that reveal the paper trail of crime and of the activities of international terrorist organizations and other foreign powers and their agents—grand jury, administrative, and judicial subpoenas; search warrants; court orders under the Electronic Communications Privacy Act (ECPA) and the Foreign Intelligence Surveillance Act (FISA); and national security letters (NSLs). The most important changes were made to FISA and the national security letter statutes. The USA PATRIOT Act and the related legislation that followed sought to make those implements more effective within a system of reinforced civil liberties safeguards.

National Security Letters

The USA PATRIOT Act expanded authorities for agency-issued national security letters. It authorized their issuance with the approval of the Special Agents in Charge of FBI field offices (SACs); broadened the range of permissible targets; and enacted the community-wide-all-consumer credit-information national security letter statute.[3217] Prior to the USA PATRIOT Act, the national security letter statutes permitted issuance only upon government certification of specific and articulable facts, giving reason to believe that the information sought pertained to a foreign power or one of its agents.[3218] Now, they require a certification that the information is relevant to, or is sought for, a particular national security investigation.[3219] The change means that national security letters may be issued at a stage in the investigation when the precise relationship (if any) of a subject to a specific terrorist organization or other foreign power has yet to be established. It also means that information is more likely to be gathered from people several steps removed from a foreign power or its agents and is more likely to pertain to individuals not ultimately of interest.

Reports of the inspector general of the Department of Justice indicate that the FBI previously did not find pre-amendment national security letters particularly useful but now considers them indispensable.[3220] Information gleaned from

---

[3217] P.L. 107-56, §§ 328(g), 505.

[3218] See, e.g., 18 U.S.C. § 2709 (2000 ed.). A textual comparison of the NSL statutes now and prior to the USA PATRIOT Act appears as an appendix in CRS Report R40887, National Security Letters: Proposed Amendments in the 111th Congress, by Charles Doyle.

[3219] See, e.g,, 18 U.S.C. § 2709.

[3220] Office of the Inspector General, U.S. Department of Justice, A Review of the Federal Bureau of Investigation's Use of National Security Letters (March 2007) (IG Rept. I) at 43-5; Office of the

national security letter responses is used to produce analytical intelligence reports; further investigations; provide the basis for FISA orders and pursue other investigative techniques; and help decide whether to open, continue, or close an investigation or line of inquiry.[3221] However, the inspector general also found that, at least initially, "the FBI used national security letters in violation of applicable national security letter statutes, Attorney General Guidelines, and internal FBI policies."[3222]

FISA Orders for Business Records and Other Tangible Things

Section 215 of the USA PATRIOT Act, one of the three amendments to FISA scheduled to expire on February 28, 2011, was perhaps the act's most controversial provision. It expanded the authority for FISA orders compelling records and other tangible things in two ways. First, it enlarged the scope of materials that may be sought. Prior to the enactment of the USA PATRIOT Act, FISA authorized court orders for access to only four types of business records: car rental records, housing accommodation (e.g., hotel/motel) records, storage rental records, and travel (e.g., airline/train) records.[3223] As amended, the section authorizes the FISC to issue orders for access to "any tangible things."[3224] Second, the section lowered the standard which must be met before the court may issue such orders. The previous standard required a showing of specific and articulable facts giving reason to believe the information related to a foreign power or the agent of a foreign power. As amended, the provision now requires "a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to a [foreign intelligence, international terrorism, or espionage investigation.]"[3225]

Specific concerns regarding the provision's potential application to library records and other materials thought to be particularly private or sensitive prompted further revisions to the relevant FISA authorities. In 2006, Congress modified the tangible item provisions to restrict the officials who may apply for orders covering library, bookstore, gun sale, tax or medical records to senior FBI

Inspector General, U.S. Department of Justice, A Review of the Federal Bureau of Investigation's Use of National Security Letters (March 2008) (IG Rept. II) at 114-16.

[3221] IG Rept. I at 46.

[3222] Id. at 124. Second IG's report indicated it was too soon to tell whether the FBI had eliminated the problems identified in the first report, IG Rept. II at 161.

[3223] 50 U.S.C. §§ 1861-1862 (2000 ed.).

[3224] 50 U.S.C. § 1861(a)(1).

[3225] 50 U.S.C. §§ 1861-1863.

headquarters officials; for other types of materials, FBI field office SACs may also apply.[3226]

The 2006 measures also called for audits of the use of section 215 authority by the Justice Department's inspector general.[3227] The resulting reports indicate that the authority was exercised only relatively infrequently and most often in part to secure information that is now available under FISA trap and trace authority.[3228] Prior to the 2006 amendments, FISA trap and trace authority did not permit the order to include a demand for related customer record information, a problem authorities overcame by submitting a FISA tangible item order request in combination with a FISA trap and trace order request.[3229] The 2006 amendments enlarged FISA trap and trace authority so that such "combo" FISA applications are no longer necessary.[3230] The FISA court approved six "pure" section 215 requests in 2004; 14 in 2005; 15 in 2006; 17 in 2007; and 18 in 2008.[3231] The IG reports suggest several reasons for the sparse use. The approval process is less familiar, multi-layered, sometimes cumbersome, and time consuming.[3232] Moreover, voluntary compliance, NSLs, grand jury subpoenas, or FISA trap and trace orders can often provide access to the same documents more quickly.[3233] Nevertheless, the Justice Department considers section 215 authority to be a valuable tool when these alternative means are not available.[3234]

A final important change affected the burden of proof for the standard of relevancy. Record checks are often the "stuff" of running down leads. Before 2006, FISA tangible-item orders were available when "sought" for certain national security investigations—that is, sometimes to determine whether they

---

[3226] 50 U.S.C. § 1861(a).

[3227] P.L. 109-177, §§ 102(b), 106A.

[3228] Office of the Inspector General, U.S. Department of Justice, A Review of the Federal Bureau of Investigation's Use of Section 215 Orders for Business Records (March 2007) (IG 215 Rept. I); Office of the Inspector General, U.S. Department of Justice, A Review of the Federal Bureau of Investigation's Use of Section 215 Orders for Business Records in 2006 (March 2008) (IG 215 Rept. II).

[3229] IG 215 Rept.I at 16-7.

[3230] Id. at 17; 50 U.S.C. § 1842(d)(2)(C).

[3231] IG 215 Rept. I at 17; IG 215 Rept. II at 15.

[3232] IG 215 Rept. II at 57.

[3233] Id.

[3234] Id. at 58.

would be relevant, not because they were determined to be relevant.[3235] In such cases, FISA responses not infrequently included irrelevant information. After the 2006 amendments, the orders authorize government access only to relevant information.[3236] However, records are declared "presumptively relevant" if they pertain to a foreign power or one of its agents, to the suspected agent who is the subject of the investigation, or to an individual in contact with, or known to, such an agent.[3237] The relevancy presumption seems to make acquisition of information pertaining to "innocent" Americans more likely. Foreign agents may "know" many people, some involved in their nefarious activities, others not. The amendment creates a presumption of relevancy for information pertaining to both groups.

New Statutory Authority to Conduct "Sneak and Peek" Searches

As a general rule, the Federal Rules of Criminal Procedure require officers executing a search warrant to give notice that they have done so and to leave an inventory of the property they have seized.[3238] Section 213 of the USA PATRIOT Act, as amended, permits delayed notice search warrants under some circumstances.[3239] A delayed notice, or "sneak and peek," search warrant is one that authorizes law enforcement officers to secretly enter a home or business, either physically or virtually, conduct a search, take pictures or copy documents, and depart without taking any tangible evidence or leaving notice of their presence. Before section 213, the federal courts agreed that such warrants might be issued under certain exigent circumstances, but disagreed over whether an unnoticed search in the absence of sufficient exigent circumstances constituted a Fourth Amendment violation as well as a violation of the federal rules. They also disagreed as to whether notice might be delayed for longer than seven days or some similar short period of time without court approval.[3240]

The law now permits a delayed notification for 30 days or more for such warrants. In addition, the period of delay may be renewed and extended for intervals of 90 days or more if there is reason to believe that immediate notification will "result in (A) endangering the life or physical safety of an individual; (B) flight from prosecution; (C) destruction of or tampering with

---

[3235] 50 U.S.C. § 1861(b) (2000 ed., Supp. I).

[3236] 50 U.S.C. § 1861(b).

[3237] 50 U.S.C. § 1861(b)(2).

[3238] Fed. R. Crim. P. 41(f).

[3239] 18 U.S.C. § 3103a(b).

[3240] See United States v. Pangburn, 983 F.2d 449 (2d Cir. 1993); United States v. Freitas, 800 F.2d 1451 (9th Cir. 1986); United States v. Simmons, 206 F.3d 392 (4th Cir. 2000).

evidence; (D) intimidation of potential witnesses; or (E) otherwise seriously jeopardizing an investigation."[3241]

In FY2008, federal courts issued 763 delayed notice warrants, most often for 90 days.[3242] Drug cases accounted for 474 of the initial warrants and for 369 of the 528 extensions granted; terrorism cases accounted for three of the warrants and two of the extensions.[3243] Thus, even when there is a criminal nexus, delayed notice search warrants do not appear to be a regular employed investigative tool in national security investigations.

Judicial Oversight and Minimization Procedures

Congress relies on three types of safeguards to protect against abuse of the new authority established by the USA PATRIOT Act and its successors: congressional oversight, judicial oversight, and minimization procedures.

Congressional Oversight

Measures following the USA PATRIOT Act established various reporting and notification requirements, presumably to provide transparency regarding the use of enhanced authorities. For example, section 6002 of the FISAAmendments Act of 2004,P.L. 108-458, requires the Attorney General, on a semiannual basis, to report to relevant committees regarding the use of various FISA authorities, Foreign Intelligence Surveillance Court decisions, and related matters for each preceding six-month period.[3244]

Congress instituted additional reporting requirements when it reauthorized and made permanent many USA PATRIOT Act provisions in 2005. For example, section 114 of the USA PATRIOT Improvement and Reauthorization Act of 2005 enhanced congressional oversight of delayed notice search warrants by requiring that no later than 30 days after the expiration or denial of such a warrant, the issuing or denying judge notify the Administrative Office of the U.S. Courts of (1) an application for a delayed notice search warrant; (2) whether the warrant was either granted, modified, or denied; (3) the length of time of the delay in giving

---

[3241] 18 U.S.C. §§ 3103a(b), 2705(b). In other Fourth Amendment cases, the Supreme Court has identified the destruction of evidence, threats to individual safety, and risk of the suspect's flight as among the permissible exigent circumstances justify delayed notice. See, e.g., Wilson v. Arkansas, 514 U.S. 927, 936 (1995).

[3242] Administrative Office of the United States Courts, Report of the Director of the Administrative Office of the United States Courts on Applications for Delayed-Notice Search Warrants and Extensions, EC-2350, 155 Cong. Rec. S7555 (daily ed. July 15, 2009) at 1-2.

[3243] Id. at 6.

[3244] P.L. 108-458, § 6002, 50 U.S.C. 1801 note.

notice; and (4) the offense specified in the warrant or the application.[3245] In addition, it requires the Director of the Administrative Office to submit an annual report to Congress summarizing the use of delayed notice warrants.[3246]

Similarly, section 209 of the 2005 reauthorization measure instituted a semi-annual reporting requirement, whereby the Attorney General must report to the Senate Judiciary Committee and the House and Senate Intelligence Committees regarding physical searches conducted pursuant to FISA, and must submit to those committees and the House Judiciary Committee a report with statistical information concerning the number of emergency physical search orders authorized or denied by the Attorney General.[3247] Likewise, section 128 requires that the Judiciary Committees receive full reports on the use of the FISA's pen register and trap and trace authority every six months.[3248]

Judicial Oversight

Notification requirements facilitate judicial oversight as well. For example, section 216 of the USA PATRIOT Act requires law enforcement officers to submit a detailed report to the court authorizing the search describing information collected via pen registers and trap and trace devices.[3249] The requirement was likely a response to objections that e-mail header information, now authorized to be collected, can be more revealing than a telephone number.

Congress and the courts have also addressed individuals' direct access to judicial review. For example, section 223 of the USA PATRIOT Act amended ECPA to authorize a cause of action against the United States for willful violation by federal employees of the stored communications and records provisions, of the court-ordered interception provisions, and of the FISA electronic surveillance, physical search, pen register, or trap and trace device provisions.[3250]

The federal courts have in some cases determined that insufficient access to judicial review raises constitutional problems. In the context of national security letters, the U.S. Court of Appeals for the Second Circuit, in John Doe, Inc. v.

[3245] P.L. 109-177, § 114, 18 U.S.C. § 3103a(d)(1).

[3246] Id.

[3247] P.L. 109-177, § 109(a), 50 U.S.C. § 1826.

[3248] P.L. 109-177, § 128(b), 50 U.S.C. § 1846(a).

[3249] P.L. 107-56, § 216, 18 U.S.C. § 3123(a)(3).

[3250] P.L. 107-56, § 223(c), 18 U.S.C. §§ 2510(19), 2712.

Mukasey,[3251] held that the current gag order and accompanying judicial review provisions only survive First Amendment scrutiny if the government takes specified actions. Namely, it must promptly petition for judicial review (at the recipient's option) and convince the district court that the proposed secrecy provision is narrowly crafted to meet the statutorily identified adverse consequences of disclosure.[3252] The John Doe, Inc. court also found unconstitutional the statutory requirement (18 U.S.C. § 3511(b)) that a reviewing court give conclusive weight to the government's certification that disclosure might have adverse consequences.[3253]

Judicial review of nondisclosure orders accompanying FISA tangible items orders would seem to stand on different footing. The First Amendment defect in the NSL provisions is the want of prompt judicial involvement. The nondisclosure orders under FISA are issued by the FISC, a neutral judicial body, and consequently would seem to suffer no such malady. The statute, however, establishes an intricate procedure under which a recipient must wait a year before filing a motion to modify or set aside a nondisclosure requirement.[3254] Petitions, which survive a screening process designed to weed out frivolous challenges, may be granted only if the judge concludes that there is no reason to believe that disclosure would endanger national security or individual safety or would interfere with a diplomatic relations or a criminal, counter-terrorism, or counter-intelligence investigation.[3255] As in the NSL statute provision to which the Second Circuit objected,[3256] the government's certification of a possible adverse impact on national security or diplomatic relations is conclusive.[3257] If a petition is denied, a renewed petition may not be filed until a year later.[3258]

[3251] 549 F.3d 861 (2d. Cir. 2008).

[3252] For national security letters, such consequences include danger to the national security or to individual safety, or interference with diplomatic relations or with a criminal counter-intelligence, or counter-terrorism investigation. In a criminal context, disclosure of an officer's purpose to execute a warrant may be excused if disclosure is likely to result in adverse consequences such as the loss of evidence, flight of a suspect, or a danger to individual safety, Wilson v. Arkansas, 514 U.S. 927, 935-36 (1995).

[3253] Mukasey, 549 F.3d at 883.

[3254] 50 U.S.C. § 1861(f).

[3255] 50 U.S.C. § 1861(f)(2).

[3256] 549 F.3d 861, 882-83 (2d Cir. 2008) ("the fiat of a governmental official, though senior in rank and doubtless honorable in the execution of official duties, cannot displace the judicial obligation to enforce constitutional requirements").

[3257] 50 U.S.C. § 1861(f)(2)(C)(ii).

[3258] 50 U.S.C. § 1861(f)(2)(C)(iii).

Although FISA does not say so in so many words, the recipient of a FISA order who disobeys an order of the court probably stands in contempt of court.[3259] It may be assumed that FISA court-issued orders would be beyond reproach on First Amendment grounds when issued. Yet, the time bars on release from a gag order for which the need has passed might be thought troubling. The time bars notwithstanding, however, a recipient might find an effective avenue for timely review by refusing to comply with the order to produce followed by a challenge to the gag order at the subsequent show cause or habeas hearing.

Minimization Procedures

Minimization means different things in different contexts. In an abstract sense, it means capturing, keeping, using, and passing on to others no more information than is necessary to satisfy the purposes for which the statutory authority to do so was given. Under ECPA, it means procedures to minimize the interception of communications other than those for which the Title III order was granted.[3260] Under FISA, minimization means, roughly, procedures to curtail the interception of the communications of Americans consistent with national security needs.[3261] FISA also has provisions governing the use of FISA-generated evidence in subsequent federal or state proceedings under which district courts may review the legality of the use of FISA authority and suppress the resulting evidence when appropriate.[3262] As discussed supra, in addition to requiring minimization procedures specific to an investigation, both ECPA and FISA also place general limitations on the use of authorities and the information collected. For example, ECPA restricts the use and dissemination of information collected.[3263]

Today, the national security letter statutes have no comparable provisions, although most have dissemination limits.[3264] Section 119 of the USA PATRIOT Improvement and Reauthorization Act of 2005 directed the Attorney General to report on the feasibility of establishing national security letter minimization procedures.[3265] A report prepared by the Justice Department's inspector general discussed efforts of the Justice Department to formulate such procedures and

---

[3259] Cf., 18 U.S.C. §§ 401, 402.

[3260] 18 U.S.C. § 2518(5).

[3261] 50 U.S.C. § 1801(h).

[3262] 50 U.S.C. §§ 1806, 1825.

[3263] 18 U.S.C. §§ 2517, 2518(8).

[3264] 18 U.S.C. § 2709(d); 12 U.S.C. § 3414(a)(5)(B); 15 U.S.C. § 1681u(f); 50 U.S.C. § 436(e).

[3265] P.L. 109-177, § 119(f).

reservations concerning the initial proposals.[3266] The inspector general has also testified that such procedures are needed and overdue, but acknowledged that the task has proven challenging.[3267] He expressed the view that the national security letter minimization procedures should address "collection of information through national security letters, how the FBI can upload national security information in FBI databases, the dissemination of NSL information, the appropriate tagging and tracking of national security letter derived information in FBI databases and files, and the time period for retention of national security letter obtained information."[3268]

Unlike the NSL statutes, section 215 of the USA PATRIOT Act, as amended, has an explicit minimization component, which calls for procedures governing the retention and dissemination of records and other tangible things collected pursuant to FISA orders.[3269] The Justice Department, however, failed to reach internal consensus on issues such as "the time period for retention of information, definitional issues of 'U.S. person identifying information,' and whether to include procedures for addressing material received in response to, but beyond the scope of, the FISA Court order; uploading information into FBI databases; and handling large or sensitive data collections."[3270] Accordingly, it issued interim procedures, which the inspector general concluded "do not adequately address the intent and requirements of the [law] for minimization requirements."[3271]

Related Matters

A few key ancillary matters are likely to be raised in the legislative debate surrounding reauthorization of the USA PATRIOT Act and related authorities. One is the increasingly murky relationship between intelligence gathering authorities and the federal criminal code. Provisions enacted in the wake of the Terrorist Surveillance Program, including retroactive immunity for communications providers and authorities regarding persons located outside the United States that are set to expire in 2012 may also be explored.

Nexus Between Intelligence Gathering and Federal Criminal Statutes

---

[3266] IG Rept. II at 64-72.

[3267] Reauthorizing the USA Patriot Act: Hearings Before the Senate Comm. on the Judiciary, 111th Cong. (2009) (statement of U.S. Department of Justice Inspector General Glenn A. Fine).

[3268] Id.

[3269] 50 U.S.C. § 1861(g).

[3270] IG 215 Rept. II at 76.

[3271] Id. at 87.

Despite some lessening of traditional divisions between criminal law enforcement and foreign intelligence gathering resulting from the USA PATRIOT Act and subsequent measures, the purpose of government activity, and the resulting statutory framework, continues to have important consequences for the scope and nature of information collection likely to be authorized. Searches and surveillance in criminal investigations must be justified by indicia of criminal conduct.[3272] In contrast, a significant purpose of an electronic surveillance or a physical search conducted pursuant to FISA must be the collection of foreign intelligence information,[3273] and those activities must be supported by probable cause to believe both (1) that the person targeted by the order is a foreign power or its agent, and (2) that the subject of the search (i.e., the telecommunications at which the surveillance is directed or place to be searched) is owned, possessed, in transit to or from, or is being or is about to be used by the target.[3274] Likewise, the use of national security letters is generally limited to investigations of international terrorism or for clandestine intelligence activities.

Thus, the presence of a criminal law enforcement rationale is significant. Federal intelligence agents may avail themselves of grand jury subpoenas and other criminal law enforcement tools when there is a nexus to a criminal offense. The existence of that nexus often depends upon the reach of federal substantive anti-terrorism law. Federal law prohibits certain violent acts of terrorism such as aircraft sabotage and the use of weapons of mass destruction.[3275] It also condemns misconduct committed in anticipation of violent acts of terrorism such as providing material support to terrorism organizations or accepting military training from terrorist organizations.[3276] Moreover, terrorist offenses often serve as an element of other federal crimes such as racketeering or supply the basis for expanded procedural options in areas such as the statute of limitations.[3277] For example, federal law extends the general five-year statute of limitations for

---

[3272] See Fed. R. Crim. P. 41(c); 18 U.S.C. § 2518(3).

[3273] See, e.g., 50 U.S.C. § 1804(a)(7)(B) (2008). Prior to 2001, the statute had required that "the purpose" of a FISA warrant be foreign intelligence collection.

[3274] 50 U.S.C. § 1805(a)(2)(A) and (B) (electronic surveillance); 50 U.S.C. § 1824(a)(2) (physical search). In contrast, federal criminal search warrants require probable cause to believe that instrumentalities, evidence, or fruits of a crime will be found in the place to be searched. See Fed. R. Crim. P. 41(c).

[3275] 18 U.S.C. § 32 (destruction aircraft or aircraft facilities); 18 U.S.C. § 2332a (use of weapons of mass destruction).

[3276] 18 U.S.C. § 2339B (providing material support); 18 U.S.C. § 2339D (military training). While section 2339B covers attempted violations, section 2339D does not.

[3277] 18 U.S.C. §§ 1961-1962 (racketeering); 18 U.S.C. § 3286 (statute of limitations).

prosecution of a federal crime to eight years when the offense is one defined as a federal crime of terrorism.[3278]

Two federal statutes, both amended by the USA PATRIOT Act, outlaw providing material support for terrorists. One prohibits providing support for federal crimes of terrorism or similar offenses;[3279] the other providing support for designated terrorist organizations.[3280] The second declares in part that "[w]hoever knowingly provides material support or resources to a foreign terrorist organization, or attempts or conspires to do so, shall be fined under this title or imprisoned not more than 15 years, or both."[3281] Conviction requires proof that the defendant either knew that the organization had been designated a foreign terrorist organization or that it engaged in terrorism.[3282] It does not require the government to prove that the support was provided with the intent to further the organization's illicit activities.[3283] The Ninth Circuit has held that the terms "training" and "service" as used in these sections to describe prohibited forms of material support are unconstitutionally vague.[3284] The Supreme Court has agreed to hear arguments which assert that they are incompatible with the prohibitions of the First Amendment and unconstitutionally vague.[3285]

In addition to the racketeering and statute of limitation provisions, federal crimes of terrorism appear in a number of federal statutes. In some instances, the presence of a federal crime of terrorism is an element of the offense.[3286] In others,

---

[3278] 18 U.S.C. § 2332b(g)(5) classifies over forty federal offenses as "federal crimes of terrorism."

[3279] 18 U.S.C. § 2339A.

[3280] 18 U.S.C. § 2339B. Neither section explicitly covers material support of the families of terrorist suicide bombers.

[3281] 18 U.S.C. § 2339B(a)(1).

[3282] More precisely, it requires that it had been designated or that the organization has or is engaged in terrorist activity as defined in 8 U.S.C. § 1182(a)(3)(B), or in terrorism as defined in 22 U.S.C. § 2656f(d)(2).

[3283] Humanitarian Law Project v. Mukasey, 552 F.3d 916, 927 (9th Cir. 2009), cert. granted, _____ S.Ct. _____ (Sept. 30, 2009); United States v. Warsame, 537 F.3d 1005, 1021-22 (D. Minn. 2008).

[3284] Humanitarian Law Project v. Mukasey, 552 F.3d 916, 928-30 (9th Cir. 2009), cert. granted, _____ S.Ct. _____ (Sept. 30, 2009).

[3285] Humanitarian Law Project v. Holder (Doc. No. 08-1498), _____ S.Ct. _____ (Sept. 30, 2009); Holder v. Humanitarian Law Project (Doc. No. 09-89), _____ S.Ct. _____ (Sept. 30, 2009).

[3286] 18 U.S.C. § 2283 (transportation of explosives or weapons of mass destruction knowing they are intended to be used commit a federal crime of terrorism) and § 2284 (transportation of a terrorist who intends to commit, or is in flight following commission of, a federal crime of terrorism).

investigation of a federal crime of terrorism constitutes an exception to an otherwise applicable privacy restriction.[3287] As a general rule, the Sentencing Guidelines recommend more severe sentences for federal crimes of terrorism.[3288]

In addition to the material support crime, federal law uses an alternative terrorism cross reference with at least equal regularity. Namely, 18 U.S.C. § 2331 provides an element for some offenses, such as one which makes it a federal crime to commit bribery affecting port security with the intent to commit international or domestic terrorism.[3289] It too supplies the grounds for an exception to otherwise binding privacy restrictions.[3290] And, several federal crimes are more severely punished when they are committed in furtherance of international or domestic terrorism.[3291]

The difference between the two cross references is one of specificity on one hand and a terrorism nexus on the other. 18 U.S.C. § 2332b(g)(5)(B) provides a relatively limited list of specific federal crimes that need not necessarily be committed in a terrorist context.[3292] 18 U.S.C. § 2331, on the other hand, includes any federal, state, or foreign crime of violence, but only if committed for terrorist purposes.[3293] The domestic terrorism definition of section 2331 originated in the USA PATRIOT Act.[3294] Critics have suggested that its want of specificity threatens possible misuse against political dissents.[3295]

[3287] 20 U.S.C. §§ 1232g(j), 9573(e) (court orders for access to confidential educational records).

[3288] U.S.S.G. § 3A1.4.

[3289] 18 U.S.C. § 226.

[3290] 20 U.S.C. § 1232g(j), § 9573(e) (court orders for access to confidential educational records).

[3291] E.g., 18 U.S.C. § 1001 (false statements), § 1028 (fraud relating to identification documents), § 1505 (obstruction of administrative proceedings).

[3292] 18 U.S.C. § 2332b(g)(5) consists of two elements: a terrorism element ("an offense that is calculated to influence or affect the conduct of government by intimidation or coercion, or to retaliate against government conduct," 18 U.S.C. § 2332b(g)(5)(A)) and one listing specific federal crimes ("an offense that … is a violation of [specified sections]," 18 U.S.C. § 2332b(g)(5)(B)). Most statutes cross reference only to section 2332b(g)(5)(B).

[3293] See 18 U.S.C. § 2331(1) (defining "international terrorism"); 18 U.S.C. § 2331(5) (defining "domestic terrorism").

[3294] P.L. 107-56, § 802.

[3295] See e.g., How the USA PATRIOT Act Will permit Governmental Infringement upon the Privacy of Americans in the Name of "Intelligence" Investigations, 150 U. Pa. L. Rev. 1651, 1688-692 (2002).

Aftermath of the Terrorist Surveillance Program (TSP)

In late 2005, the New York Times reported that the federal government had "monitored the international telephone calls and international e-mail messages of hundreds, perhaps thousands, of people in the United States without warrants."[3296] Subsequently, President Bush acknowledged that, after the attacks of September 11, 2001, he had authorized the National Security Agency to "intercept international communications into and out of the United States" by "persons linked to al Qaeda or related terrorist organizations" based upon "his constitutional authority to conduct warrantless wartime electronic surveillance of the enemy,"[3297] despite the general rule that electronic surveillance by the federal government is unlawful unless conducted pursuant to the Foreign Intelligence Surveillance Act (FISA) or Title III of the Omnibus Crime Control and Safe Streets Act (Title III).[3298] Now discontinued, the TSP appears to have been active from shortly after September 11, 2001, to some time in January of 2007.[3299]

Following these revelations, Congress enacted the Protect America Act, P.L. 110-55, and the FISA Amendments Act of 2008, P.L. 110-261. They addressed several issues raised in public discussions regarding the TSP. Two provisions likely to arise in the current legislative debate include (1) retroactive immunity for telecommunications providers who played a role in the TSP; and (2) temporary provisions applying different procedures and standards to targets under FISA depending upon the person's nationality and geographic location.

Retroactive Immunity for Telecommunications Providers

After private citizens and interest groups became aware of the TSP, they filed dozens of lawsuits alleging various statutory and constitutional violations by the telecommunications companies that participated in the program.[3300] During

---

[3296] James Risen and Eric Lichtblau, Bush Lets U.S. Spy on Callers Without Courts, N.Y. Times, Dec. 16, 2005, at 1.

[3297] U.S. Department of Justice, Legal Authorities Supporting the Activities of the National Security Agency Described by the President, at 5, 17, Jan. 19, 2006, http://www.usdoj.gov/opa/whitepaperonnsalegalauthorities.pdf. See also CRS Report R40888, Presidential Authority to Conduct Warrantless Electronic Surveillance to Gather Foreign Intelligence Information, by Elizabeth B. Bazan and Jennifer K. Elsea.

[3298] The "procedures in [Title III of the Omnibus Crime Control and Safe Streets Act] and the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which electronic surveillance, as defined in section 101 of FISA, and the interception of domestic wire, oral, and electronic communications may be conducted." 18 U.S.C. § 2511(2)(f) (emphasis added).

[3299] S.Rept. 110-209, at 4. See also Letter from Attorney General Gonzales to Senate Judiciary Committee Chairman Patrick Leahy and Senator Arlen Specter (January 17, 2007).

[3300] Id. at 7.

litigation, the government moved for the dismissal of the cases on the basis of the state secrets privilege, which bars the disclosure during litigation of information that, "in the interest of national security, should not be divulged."[3301] While the district court left open the possibility that the privilege might lead to dismissal at a later date, it declined to dismiss the suits before the discovery stage in the litigation.[3302]

Insofar as many of the details of the TSP remain classified, it is likely that assertions of the state secrets privilege would have been central to the disposition of the civil suits against telecommunications providers. However, the enactment of the 2008 FISAAmendments Act provided the Attorney General with the authority to seek the dismissal of these lawsuits.[3303] Under the 2008 law, no civil case against a covered telecommunications company could proceed if the Attorney General certified that any assistance given by the defendant was given in connection with the TSP between September 11, 2001, and January 17, 2007, and the defendant received written assurances that the TSP was authorized by the President and determined to be lawful.[3304] Dismissal was required if the court found that the certified facts were supported by "substantial evidence." In September of 2008, Attorney General Mukasey made the necessary certification and moved to dismiss the civil suits against the telecommunications providers.[3305] In June of 2009, the consolidated suits were dismissed after the district court found the certification to be supported by substantial evidence.[3306] That decision was appealed to the Ninth Circuit, and is currently pending.

Were Congress to act subsequently to repeal the retroactive immunity provided by the FAA, the defendants might argue that such a repeal violates their due process rights[3307] or the constitutionally required separation of powers.[3308]

[3301] United States v. Reynolds, 345 U.S. 1, 10 (1953).

[3302] Hepting v. AT&T, 439 F. Supp. 2d 974, 994 (N.D. Cal. 2006).

[3303] 50 U.S.C. § 1885a.

[3304] Alternatively, the Attorney General can certify that the alleged assistance was not in fact provided by the defendant. 50 U.S.C. § 1885a(a)(5).

[3305] See Public Certification of the Attorney General of the U.S., In re Nat'l Security Telecommunications Records Litigation, MDL Dkt. No. 06-1791-VRW (N.D. Cal. Sep. 19, 2008) (on file with author).

[3306] In re NSA Telcoms. Records Litig., 633 F. Supp. 2d 949 (N.D. Cal. 2009).

[3307] Chase Sec. Corp. v. Donaldson, 325 U.S. 304, 315-316 (1945) (noting in dicta that "some rules of law probably could not be changed retroactively without hardship and oppression" to the extent that it would be considered a violation of the Due Process Clause).

However, courts have generally only upheld such claims where the party was in possession of a final, unreviewable judgment. Although, at this time, the cases have been dismissed by the district court, that dismissal has not been reduced to a final, unreviewable judgment as it is currently being reviewed by the Ninth Circuit. Therefore, legislative modification of the retroactive immunity enjoyed by these defendants under the FISA Amendments Act remains a possibility.

Provisions Expiring in 2012

After the TSP activities were concluded in 2007, Congress enacted the Protect America Act, which established a mechanism for the acquisition, via a certification by the Director of National Intelligence (DNI) and the Attorney General but without a court order, of foreign intelligence information concerning a person reasonably believed to be outside the United States.[3309] This temporary authority ultimately expired after approximately six months, on February 16, 2008. Several months later, the Congress enacted the FISA Amendments Act of 2008, which created separate procedures for targeting non-U.S. persons and U.S. persons reasonably believed to be outside the United States under a new Title VII of FISA.[3310] Title VII is set to expire on December 31, 2012.

Pursuant to Title VII, non-U.S. persons reasonably believed to be abroad may be targeted to acquire foreign intelligence information pursuant to a joint Attorney General/Director of National Intelligence (DNI) authorization if certain criteria are met.[3311] The authority may not be used for reverse targeting—in situations where the true focus of the collection effort is a person in the United States.[3312] Title VII requires a FISC order to authorize the targeting U.S. persons reasonably believed to be abroad.[3313] The targeting procedures, minimization procedures, and supporting certifications by the Attorney General and the DNI, applicable to the targeting of non-U.S. persons reasonably believed to be outside the United States, are subject to judicial review by the FISC. In addition, electronic communications service providers directed by the Attorney General and the DNI to provide assistance in connection with such acquisitions from targeted non-U.S. persons may challenge such directives before the FISC, with appeal to the Foreign

---

[3308] See Plaut v. Spendthrift Farm, Inc., 514 U.S. 211 (1995) (federal law that reopened final judgment in cases where statute of limitations barred claim was a violation of the separation of powers).

[3309] P.L. 110-55, 50 U.S.C. §§ 1805a-1805c.

[3310] P.L. 110-261, § 101, 50 U.S.C. §§ 1881-1881g.

[3311] 50 U.S.C. § 1881a.

[3312] 50 U.S.C. § 1881a(b)(2).

[3313] 50 U.S.C. §§ 1881b and 1881c.

Intelligence Surveillance Court of Review, and, if necessary, to the Supreme Court. Probable cause determinations, minimization procedures, and certifications with respect to the targeting of U.S. persons reasonably believed to be outside the United States are also subject to judicial review.

Conclusion

As with previous USA PATRIOT Act reauthorization debates, the slated expiration of FISA amendments in 2011 (and provisions concerning persons reasonably believed to be abroad in 2012) may prompt an examination of authorities for government collection of private information. As mentioned, bills introduced in the 111th Congress (before a key expiration date was temporarily extended) propose significant changes to existing authorities. Congress is likely to revisit those proposals when it considers a longer-term extension of expiring provisions.

Arguments raised in the debate in the 111th Congress reflect fundamental questions regarding the level of government intrusion necessary to ensure the country's safety. Referring to the expiring provisions, the U.S. Department of Justice asserts that the expanded authorities have proven to be important and effective intelligence gathering tools.[3314] Thus, although it is "willing to consider" proposals to modify authorities to provide additional privacy protections, the Justice Department warns that care should be taken to ensure that any changes to existing authorities "do not undermine the effectiveness of [the expiring FISA amendments]."[3315]

Countervailing arguments assert that amendments enacted following the 9/11 terrorist attacks undermined citizens' civil liberties unnecessarily.[3316] Specifically, they argue that the broader the authorities for the collection of foreign intelligence information, the greater the likelihood that U.S. citizens' private conversations or documents will be swept within the scope of an authorized investigation. For example, a concern might be that the authority for "roving wiretaps" increases the likelihood that innocent conversations involving U.S. citizens will be the subject of electronic surveillance. Likewise, at least one commentator asserts that national security letters have a "too diffuse" focus, which leads to anecdotal evidence showing that "their effectiveness is disproportionately small compared with the extent of ... the invasion of privacy

---

[3314] Letter from the U.S. Department of Justice to Hon. Patrick J. Leahy (Sept. 14, 2009), http://judiciary.senate.gov/resources/documents/111thCongress/upload/091409WeichtoLeahy.pdf.

[3315] Id.

[3316] See e.g., Restoring the Rule of Law: Hearing Before the Senate Comm. on the Judiciary, Subcomm. on the Constitution, 110th Cong. (Sept. 16, 2008) (statement of Suzanne E. Spaulding, Esq.).

they represent."[3317] Reflecting the arguments on both sides, the legislative debate is likely to address ways in which the need for rigorous investigative tools might be balanced with the safeguarding of constitutional guarantees.

[3317] Unchecked National Security Letter Powers and Our Civil Liberties: Hearing Before the House Perm. Select Comm. on Intelligence, 110th Cong. (Mar. 28, 2007) (statement of Lisa Graves, then Deputy Director, Center for National Security Studies).

Terrorism: Section by Section Analysis of the USA PATRIOT Act, RL31200 (December 10, 2001).

CHARLES DOYLE, CONG. RESEARCH. SERV., TERRORISM: SECTION BY SECTION ANALYSIS OF THE USA PATRIOT ACT (2001), *available at* http://www.intelligencelaw.com/library/secondary/crs/pdf/RL31200_12-10-2001.pdf.

Order Code RL31200
CRS Report for Congress

Received through the CRS Web
Updated December 10, 2001

Charles Doyle
Senior Specialist American Law Division
Congressional Research Service ˜
The Library of Congress

Summary

The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act, P. L. 107-56, is part of the Congressional response to September 11. It is the merger of two similar bills. S.1510 passed the Senate on October 11, 147 Cong.Rec. S10604, and H.R.2975 passed the House on October 12 after substituting the language of H.R.3108 for its text, 147 Cong.Rec. H6775. Having informally resolved their differences, the House enacted the measure in final form on October 24, 147 Cong.Rec. H7282, and the Senate on October 25, 147 Cong.Rec. S11059.

The Act consists of ten titles which, among other things:

- give federal law enforcement and intelligence officers greater authority (at least temporarily) to gather and share evidence particularly with respect to wire and electronic communications;
- amend federal money laundering laws, particularly those involving overseas financial activities;
- create new federal crimes, increase the penalties for existing federal crimes, and adjust existing federal criminal procedure, particularly with respect to acts of terrorism;
- modify immigration law, increasing the ability of federal authorities to prevent foreign terrorists from entering the U.S., to detain foreign terrorist suspects, to deport foreign terrorists, and to mitigate the adverse immigration consequences for the foreign victims of September 11; and

- authorize appropriations to enhance the capacity of immigration, law enforcement, and intelligence agencies to more effectively respond to the threats of terrorism.

Several proposals, offered while the Act was under consideration, were not among the provisions ultimately enacted, e.g., revision of the McDade-Murtha Amendment (relating to the application of professional conduct standards to federal prosecutors), measures to combat illegal Internet gambling, and are thus beyond the scope of this report.

Introduction

The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act, Public Law 107-56, is part of the Congressional response to September 11. It is the merger of two similar bills. S.1510 passed the Senate on October 11, 147 Cong.Rec. S10604, and H.R.2975 passed the House on October 12 after substituting the language of H.R.3108 for its text, 147 Cong.Rec. H6775. Having informally resolving their differences, the House enacted the measure in final form on October 24, 147 Cong.Rec. H7282, and the Senate on October 25, 147 Cong.Rec. S11059.

The report of the House Committee on the Judiciary, H.Rept. 107-236 on H.R.2975, and the report of the House Committee on Financial Services, H.Rept. 107-250 on H.R. 3004, each explain some of the issues ultimately resolved in the Act.

This is a section by section analysis of the Act as enacted. The analysis borrows the explanations of the House Committee of the Judiciary, in a number of those instances where the language of the Committee bill and the language of the Act are identical.

Section 1. Short Title and Table of Contents

The Act may be cited as the "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001."

Section 2. Construction; Severability

Section 2 confirms that the Act's provisions should be given maximum effect and that should any provision be found invalid or unenforceable it should be severed and the remainder the Act allowed to remain in effect.

Title I – Enhancing Domestic Security Against Terrorism

Section 101. Counterterrorism Fund

Congress created a Counterterrorism Fund to reimburse the Department of Justice for the costs of reestablishing operating capacity lost as a consequence of

the destruction of the Alfred P. Murrah Federal Building in Oklahoma City and for other counterterrorism expenditures, Public Law 104-19, 109 Stat. 249 (1995). This section takes a similar course in order to reimburse the Justice Department for the costs of (1) reestablishing the operating capacity of facilities damaged or destroyed by terrorists; (2) preventing, investigating and prosecuting terrorism by various means including the payment of rewards (without limitation); and (3) conducting terrorism threat assessments of federal facilities. The Fund is also available to reimburse federal agencies for costs associated with overseas detention of individuals accused of terrorism in violation of United States law.

Section 102. Sense of Congress Condemning Discrimination Against Arab and Muslim Americans

It is the sense of Congress that the civil rights and civil liberties of all Americans, including Arab Americans, Muslim Americans, and Americans from South Asia, should be protected; that violence and discrimination against any American should be condemned; and that the patriotism of Americans from every ethnic, racial, and religious background should be acknowledged.

Section 103. Increased Funding for the Technical Support Center at the Federal Bureau of Investigation

This section authorizes appropriations of $200 million for each of fiscal years 2002, 2003, and 2004 for the FBI's Technical Support Center, created by section 811 of the Antiterrorism and Effective Death Penalty Act of 1996 (Public Law 104-132, 110 Stat. 1314 (1996).

Section 104. Requests for Military Assistance to Enforce Prohibition in Certain Emergencies

The Posse Comitatus Act and its administrative auxiliaries, 18 U.S.C. 1385, 10 U.S.C. 375, ban the use of the armed forces to execute civilian law, absent explicit statutory permission. Pre-existing statutory exceptions covered Department of Justice requests for technical assistance in connection with emergencies involving biological, chemical or nuclear weapons, 18 U.S.C. 2332e, 175a, 229E, 831(e), and 10 U.S.C. 382. This section amends section 2332e to include emergencies involving other weapons of mass destruction.

Section 105. Expansion of National Electronic Crime Task Force Initiative

In order to counter various forms of electronic crime including those directed against the Nation's critical infrastructure and financial systems, this section instructs the Director of the United States Secret Service to establish a network of electronic crime task forces modeled after the New York Electronic Crimes Task Force.

Section 106. Presidential Authority

The International Emergency Economic Powers Act (IEEPA), 50 U.S.C. 1701 et seq., grants the President emergency economic powers when faced with extraordinary threats to our national security, foreign policy or economic well being. Under such conditions, for example, he may freeze the assets located in this country of a foreign nation or national responsible for the threat. During war time, the Trading with the Enemy Act (TWEA) gives him the power to confiscate enemy property located in the United States , 50 U.S.C. App. 1 et seq.

Section 106 amends section 703 of IEEPA, 50 U.S.C. 1702, to permit the President to confiscate foreign property in response to foreign aggression. The authority becomes available when the United States is engaged in armed hostilities or has been attacked by a foreign country or its nationals. At that time, the property of any foreign person, organization, or nation which planned, authorized, aided or engaged in the hostilities or attack becomes forfeitable. The President or his delegate may determine the particulars under which the property is confiscated, administered and disposed of, subject to an innocent owner defense created by section 316 of the USA PATRIOT Act. Elsewhere, the USA PATRIOT Act gives the President an alternative means to confiscate the same property on similar grounds (section 806).

Section 106 is intriguing because on one hand it seems a logical extension of IEEPA and TWEA, but on the other it appears to revive the constitutionally suspect forfeiture of estate. Forfeiture of estate was a creature of the common law.[3318] Upon conviction and attainder, a felon or traitor forfeited all of his property. Statutory forfeiture, a more familiar feature of American law, consists of the confiscation of contraband, the fruits of crimes, and the means to commit a crime – untaxed whiskey, the drug dealer's profits, and the rum runner's ship.

Three distinguishing features characterize forfeiture of estate. The property is lost solely by reason of its ownership by the felon or traitor; there need be no other nexus to the crime. As a consequence, it works the confiscation of all of a felon's property, not just his crime-related property. Third, it extinguishes his future right to hold property and no title to property may pass through him to his heirs.[3319]

[3318] "Three kinds of forfeiture were established in England at the time the Eighth Amendment was ratified in the United States: deodand, forfeiture, and statutory forfeiture. . . . Of England's three kinds of forfeiture, only the third took hold in the United States," Austin v. United States, 509 U.S. 602, 611-12 (1993).

[3319] Statutory forfeitures have often been accomplished through civil proceedings conducted in rem with the offending property treated as defendant. As a result, some came to believe that the necessity of the property owner's criminal conviction constituted the essential distinction between forfeiture of estate and statutory forfeiture. Yet, occasional forfeiture statutes have predicated confiscation upon the owner's conviction throughout our history. Moreover, it defies credibility to claim that forfeiture of estate's only ameliorating attribute is its only essential element.

It is this last feature, this "corruption of the blood", which the authors of the Constitution found most distasteful. They decreed that "no attainder of treason shall work corruption of blood, or forfeiture except during the life of the person attainted," U.S.Const. Art. III, §3, cl.2. And when first assembled in Congress, they extended the ban to all federal crimes: "no conviction or judgment for any offences aforesaid, shall work corruption of blood, or any forfeiture of estate," 1 Stat. 117 (1790).[3320]

During the Civil War, Congress authorized the confiscation of the property of supporters of the Confederacy, 12 Stat. 589 (1862), but in deference to President Lincoln's constitutional doubts interest in the property reverted to the offender's heirs upon his death, 12 Stat. 627 (1862).

On the other hand, confiscation under the Trading With the Enemy Act (TWEA), looks for all intents and purposes like the confiscation of estate of the property of an enemy nation or national, 50 U.S.C. App. 5(b). Yet the Supreme Court has upheld TWEA as a valid exercise of the war power without mentioning of any obstacle interposed by constitutional reservations concerning forfeiture of estate, Silesian American Corp. v. Clark, 332 U.S. 469 (1947).[3321]

Section 106 also amends IEEPA to cover situations where either the covered foreign person or the covered property are within this country or otherwise subject to the jurisdiction of the United States. It allows the President to freeze assets during the pendency any International Emergency Economic Act investigation rather than await its outcome as was previously the case. Finally, it permits the government to present, in secret (ex parte and in camera), any classified information upon which an IEEPA decision has been based should the decision be subject to judicial review.

Title II – Enhanced Surveillance Procedures

Section 201. Authority to Intercept Wire, Oral, and Electronic Communications Relating to Terrorism

Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. 2510 et seq. establishes a judicially supervised procedure under which law

---

[3320] The statutory ban, and its successors, remained in effect until 1984 when it was repealed through misunderstanding as part of comprehensive revision of federal criminal law, 18 U.S.C. 3563 (1982 ed.).

[3321] Cf., Societe Internationale v. Rogers, 357 U.S. 197, 211 (1958)("this summary power to seize property which is believed to be enemy-owned is rescued from constitutional invalidity under the Due Process and Just Compensation Clauses of the Fifth Amendment only by those provisions of the Act which afford a non-enemy claimant a later judicial hearing as to the propriety of the seizure")(no suggestion that due process likewise condemns forfeiture of estate in cases that do not involve treason).

enforcement authorities may intercept wire, oral, or electronic communications. The procedure, however, is only available in connection with the investigations of specifically designated serious crimes. Section 201 adds several terrorism offenses to Title III's list of designated offenses:

- chemical weapons offenses, 18 U.S.C. 229;
- use of weapons of mass destruction, 18 U.S.C. 2332a;
- violent acts of terrorism transcending national borders, 18 U.S.C. 2332b;
- financial transactions with countries which support terrorism, 18 U.S.C. 2332d;
- material support of terrorists, 18 U.S.C. 2339A; and
- material support of terrorist organizations, 18 U.S.C. 2339B.

The section makes a technical correction in 18 U.S.C. 2516 by designating as 18 U.S.C. 2516(1)(r) one of the two paragraphs previously identified as 18 U.S.C. 2516(1)(p). Section 201 is subject to the sunset provisions of section 224.

Section 202. Authority to Intercept Wire, Oral, and Electronic Communications Relating to Computer Fraud and Abuse Offenses

Section 202 adds computer fraud and abuse to the Title III predicate offense list. This section is subject to the sunset provisions of section 224.

Section 203. Authority to Share Criminal Investigative Information

Previously, federal law enforcement officers who uncovered details of the activities of international terrorist organizations or of foreign agents in this country were often not free to pass the information on to federal intelligence officers. This section allows federal law enforcement officers to share a limited range of foreign intelligence information, notwithstanding earlier limitations such as those involving the use of grand jury information or Title III evidence.

Rule 6(e) of the Federal Rules of Criminal Procedure prohibits disclosure of matters occurring before a federal grand jury. The Rule recognizes exceptions for disclosures in other judicial proceedings, to prevent abuse of the grand jury process, for presentation of evidence to other grand juries, and to state law enforcement officials.

Section 203 creates an exception for intelligence matters. It covers information (1) related to the protection of the United States against a foreign attack or other foreign hostile action, against sabotage or international terrorism by a foreign power or its agents, or against foreign clandestine intelligence activities; (2) concerning a foreign power or territory related to the national defense, security, or foreign affairs activities of the United States; or (3) constituting foreign intelligence or counterintelligence as defined in section 3 of the National Security Act of 1947 (that is, (a) "information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, or foreign persons" or (b) "information gathered and activities conducted to protect

against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons," 50 U.S.C. 401a(2), (3)).

Now when such information comes to light during the course of a federal grand jury investigation, it may be passed on to other Federal law enforcement, intelligence, protective, immigration, national defense, or national security officials, but only for use in the official duties. Within a reasonable time thereafter, Federal prosecutors must notify the court of the disclosure under seal. Prosecutors must also follow disclosure procedures outlined by the Attorney General when sharing intelligence information that identifies an American citizen or a permanent resident alien.

When authorities executing a Title III interception order discover this same type of intelligence evidence, they may reveal it to any of these same officers for use in their official duties. Before the passage of section 203, such information could only be shared for law enforcement purposes, 18 U.S.C. 2517. As in the case of grand jury information, Title III intelligence information that identifies an American citizen or a permanent resident alien can be divulged only pursuant to disclosure procedures outlined by the Attorney General.

Finally, section 203 creates a generic exception to any other law which purports to bar federal law enforcement officials from disclosing this type of intelligence information to these federal officers for official use. The section's amendments to Title III are subject to the sunset provisions of section 224, the grand jury and generic exceptions are not.

Section 204. Clarification of Intelligence Exceptions From Limitations on Interception and Disclosure of Wire, Oral and Electronic Communications

Title III at one time stated that the interception of wire or oral communications for foreign intelligence purposes should be governed by the provisions of the Foreign Intelligence Surveillance Act (FISA) rather than those of Title III or of chapter 121 of title 18 of the United States Code (relating to stored wire and electronic communications and transactional records access) or of the Federal Communications Act, 18 U.S.C. 2511(2)(f). Section 204 amends this instruction in 18 U.S.C. 2511(2)(f) to confirm that in foreign intelligence investigations, FISA governs the interception of electronic communications and the use of pen registers and trap and trace devices as well. This section is subject to the sunset provisions of section 224.

Section 205. Employment of Translators by the Federal Bureau of Investigation

Existing law sometimes waives personnel requirements and limitations in order to fill positions requiring foreign language skills, e.g., 22 U.S.C. 1474(1)(relating to employment of translators with respect to United States Information and

Educational Exchange Programs); 22 U.S.C. 4024(a)(4)(B) (relating to the employment of linguists in connection United States Foreign Service training).

Section 205 waives otherwise applicable personnel requirements and limitations to permit the Federal Bureau of Investigation (FBI) to hire translators expeditiously to support counterintelligence investigations and operations. The Director of the FBI will see to the necessary security requirements. The Attorney General will report to the Committees on the Judiciary on the number of translators employed by the FBI and by the Department of Justice, on the impediments to using translators employed by other government agencies, on the FBI's needs, and on his recommendations to meet the FBI's needs for translation services. This section is not subject to the sunset provisions of section 224.

Section 206. Roving Surveillance Authority Under the Foreign Intelligence Surveillance Act of 1978

Speaking of identical language in an earlier bill, the House Committee on the Judiciary explained: "Section 1805(c)(2)(B) of title 50, permits the FISA court to order third parties, like common carriers, custodians, landlords and others, who are specified in the order, (specified persons) to provide assistance and information to law enforcement authorities in the installation of a wiretap or the collection of information related to a foreign intelligence investigation.

"Section 152 amends 1805(c)(2)(B) to insert language that permits the FISA court to direct the order to <other persons' if the court finds that Section 1805(c)(2)(B) of title 50, permits the FISA court to order third parties, like common carriers, custodians, landlords and others, who are specified in the order, (specified persons) to provide assistance and information to law enforcement authorities in the installation of a wiretap or the collection of information related to a foreign intelligence investigation. Section 152 amends 1805(c)(2)(B) to insert language that permits the FISA court to direct the order to <other persons' if the court finds that the `actions of the target of the application may have the effect of thwarting the identification of a specified person,' who would be required to assist in the installation of any court-authorized intercept. This amendment is intended to expand the existing authority to allow for circumstances where the court finds that the actions of a target may thwart the identification of a specified person in the order. This is usually accomplished by the target moving his location. The move necessitates the use of third parties other than those specified in the original order to assist in installation of the listening device.

"This amendment allows the FISA court to compel any such new necessary parties to assist in the installation and to furnish all information, facilities, or technical assistance necessary without specifically naming such persons. Nevertheless, the target of the electronic surveillance must still be identified or described in the order as under existing law.

"For example, international terrorists and foreign intelligence officers are trained to thwart surveillance by changing hotels, cell phones, Internet accounts, etc. just prior to important meetings or communications. Under present law, each time this happens the government must return to the FISA court for a new order just to change the name of the third party needed to assist in the new installation. The amendment permits the court to issue a generic order that can be presented to the new carrier, landlord or custodian directing their assistance to assure that the surveillance may be undertaken as soon as technically feasible," H.Rept. 107-256, at 59-60 (2001). This section is subject to the sunset provisions of section 224.

Section 207. Duration of FISA Surveillance of Non-United States Persons Who are Agents of a Foreign Power

Prior to the USA PATRIOT Act, unless directed at a foreign power, FISA surveillance orders and extensions expired after ninety days, and FISA physical search orders and extensions were effective for no more forty-five days, 50 U.S.C. 1805(e), 1824(d)(2000 ed.). Section 207 extends the tenure of physical search orders to ninety days. Surveillance and physical search orders may now remain in effect for up to 120 days with extensions for up to a year, 50 U.S.C. 1805(e), 1824(d). This represents a compromise over the Justice Department's original proposal which would have set the required expiration date for orders at one year instead of 120 days. This section is subject to the sunset provisions of section 224.

Section 208. Designation of Judges

FISA is in essence a series of procedures available to secure court orders in certain foreign intelligence cases. It operates through a special court which before passage of section 208 consisted of seven judges, scattered throughout the country, two of whom are now from the Washington, D.C. area. Section 208 authorizes the appointment of four additional judges and requires that three members of the court reside within twenty miles of the District of Columbia, 50 U.S.C. 1803(a). This section is not subject to the sunset provisions of section 224.

Section 209. Seizure of Voice-Mail Messages Pursuant to Warrants

Section 209 treats voice mail like e-mail. Thus, Federal officers may gain access with a warrant or court order. They need no longer resort to the more demanding regime of Title III that applies in the case of live telephone conversations, United States v. Smith, 155 F.3d 1050, 1055-56 (9th Cir. 1998). This section is subject to the sunset provisions of section 224.

Section 210. Scope of Subpoenas for Records of Electronic Communications

"Terrorists and other criminals often use aliases in registering for Internet and telephone services. This creates a problem for law enforcement attempting to identify the suspects of terrorist acts or criminal acts that often support the terrorists. While the government currently can subpoena electronic

communications or a remote computing services provider for the name, address and length of service of a suspect, this information does not help when the suspected terrorist or criminal lies about his or her identity. Permitting investigators to obtain credit card and other payment information by a subpoena, along with subscriber information (already permitted to be obtained under current law), will help law enforcement track a suspect and establish his or her true identity.

"This section amend[s] 18 U.S.C. 2703(c) to authorize a subpoena for transactional records to include information regarding the form of payment in order to assist law enforcement in determining the user's identity," H.Rept. 107-236, at 56-7 (2001). This section is not subject to the sunset provisions of section 224.

Section 211. Clarification of Scope

Telephone and electronic communications providers may be required to provide law enforcement officials with customer identifying information without notifying their customers, 18 U.S.C. 2705(b). Cable companies are prohibited from disclosing customer identifying information without customer approval, 47 U.S.C. 551 et. seq. When cable companies began to offer communications services, uncertainty arose over whether law enforcement access to their customers records was to be governed by the standards applicable to the communications industry or by the earlier cable standards, see In re Application of U.S.A. for an Order Pursuant to 18 U.S.C. 2703(d), 158 F.Supp.2d 644 (D.Md. 2001)(holding the cable provisions implicitly repealed and summarizing existing ambivalent case law).

Section 211 resolves the question by amending the Communications Act, 47 U.S.C. 551, to make it clear that when a cable company offers communications services it is subject to the provisions of Title III, and chapters 121 and 206 of title 18 of the United States Code (relating to stored wire and electronic communications and transactional records access and to pen registers and trap and trace devices, respectively). Cable customer video subscription records, however, remain in the shelter of the Communications Act protection. Section 211 is not subject to the sunset provisions of section 224.

Section 212. Emergency Disclosure of Electronic Communications to Protect Life and Limb

As the House Committee on the Judiciary observed with respect to a substantively identical provision: "This section amends 18 U.S.C. 2702 to authorize electronic communications service providers to disclose the communications (or records relating to such communications) of their customers or subscribers if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person requires disclosure of the information without delay.

"This section would also amend the law to allow communications providers to disclose non-content information (such as the subscriber's login records). Under current law, the communications provider is expressly permitted to disclose content information but not expressly permitted to provide non-content information. This change would cure this problem and would permit the disclosure of the less-protected information, parallel to the disclosure of the more protected information." H.Rept. 107-236, at 58 (2001). This section is subject to the sunset provisions of section 224.

Section 213. Authority for Delaying Notice of the Execution of a Warrant

Standing alone, Rule 41 of the Federal Rules of Criminal Procedure seems to preclude delayed notification of the execution of "sneak and peek" warrants. A sneak and peek warrant is one that authorizes officers to secretly enter (either physically or electronically), conduct a search, observe, take measurements, conduct examinations, smell, take pictures, copy documents, download or transmit computer files, and the like; and depart without taking any tangible evidence or leaving notice of their presence. The Rule on its face requires that after the execution of a federal search warrant officers leave a copy of the warrant and an inventory of what they have seized and advise the issuing court what they have done, F.R.Crim.P. 41(d).

The lower federal courts are divided over the extent to which the Rule reflects Fourth Amendment requirements. The Ninth Circuit sees the Fourth Amendment in Rule 41, United States v. Freitas, 800 F.2d 1451, 1453 (9th Cir. 1986). The Fourth Circuit finds no Fourth Amendment offense in search warrants secretly executed and seizures of intangible evidence that remain unannounced until weeks thereafter, United States v. Simons, 206 F.3d 392 (4th Cir. 2000). The Second Circuit, whose views the Congress found persuasive, 147 Cong.Rec. H7197 (daily ed. Oct. 23, 2001), thinks the validity of sneak and peek warrants and of delayed notice are better judged by Rule 41 standards, United States v. Pangburn, 983 F.2d 449 (2d Cir. 1993).

Section 213 rests on the belief that the Fourth Amendment does not condemn either sneak and peek warrants or delayed notice. For searches conducted under a warrant issued pursuant to Rule 41 or under a warrant or court order issued pursuant to any other rule of law, it adopts the delayed notification standards of 18 U.S.C. 2705 (relating to delayed notification of the execution of a court order authorizing government access to electronic communications held in third party storage for longer than 180 days). An issuing court may order notice delayed for a reasonable period of time and with good cause extensions, if it finds reasonable cause to believe that contemporaneous notification may have any of the adverse consequences described in section 2705. Section 2705 mentions "(A) endangering the life or physical safety of an individual; (B) flight from prosecution; (C) destruction of or tampering with evidence; (D) intimidation of potential witnesses; or (E) otherwise seriously jeopardize an investigation or

unduly delay a trial" as the kinds of adverse consequences that justify delay. Unless the court concludes seizure is reasonably necessary, the section only permits delayed notification if the warrant prohibits the seizure of any stored wire or electronic information (unless otherwise authorized), of any tangible property, or of any wire or oral communications. Section 213 is not subject to the sunset provisions of section 224.

Section 214. Pen Register and Trap and Trace Authority Under FISA

Trap and trace devices and pen registers are devices which secretly identify the source and destination of calls made to and from a particular telephone. Intelligence officers may use them pursuant to a court order authorized in the Foreign Intelligence Surveillance Act. Section 214 grants the request of the Department of Justice for elimination of the requirements which limited FISA pen register and trap and trace device orders to facilities used by foreign agents or those engaged in international terrorist or clandestine intelligence activities, 50 U.S.C. 1842(c)(3)(2000 ed.). Applicants must still certify that the devices are likely to reveal information relevant to a foreign intelligence investigation.

Section 214 also adjusts the language of the FISA pen register-trap and trace authority to permit its use to capture source and destination information for electronic communications (e.g., e-mail) as well as telephone communications, 50 U.S.C. 1842(d). Finally, the section makes it clear that requests for a FISA pen register-trap and trace order, like requests for other FISA orders, directed against Americans and permanent resident aliens (U.S. persons) may not be based solely on activities protected by the First Amendment, 50 U.S.C. 1842, 1843. Section 214 is subject to the sunset provisions of section 224.

Section 215. Access to Records and Other Items Under the Foreign Intelligence Surveillance Act

FISA previously allowed senior officials of the Federal Bureau of Investigation to apply for a court order, in connection with a foreign intelligence investigation, for access to the records of common carriers, public accommodation providers, physical storage facility operators, and vehicle rental agencies, 50 U.S.C. 1861-1863 (2000 ed.).

Section 215 rewrites those provisions. Assistant Special Agents in Charge of the FBI field offices may now also apply. The court orders extend to any tangible object held by anyone. Items sought need not relate to an identified foreign agent or foreign power as was once the case, but they may only be sought as part of an investigation to protect the United States from international terrorism or clandestine intelligence activities. Nor may they be sought in conjunction with the investigation of an American or permanent resident alien predicated solely on the basis of activities protected by the First Amendment. There is a good faith defense for anyone who produces items in response to a court order under the

section and production does not constitute a waiver of applicable privilege. Section 215 is subject to the sunset provisions of section 224.

Section 216. Modification of Authorities Relating to Use of Pen Registers and Trap and Trace Devices

With one critical exception, Section 216 tracks language in a similar section of H.R. 2975. The House Committee on Judiciary's description of that section is instructive: "Under 18 U.S.C. 3121(b), law enforcement may obtain authorization from a court, upon certification that the information to be obtained is relevant to a pending criminal investigation, to install and use a 'pen register' device that identifies the telephone numbers dialed or pulsed from (outgoing calls) or a 'trap and trace' device that identifies the telephone numbers to a particular telephone (incoming calls). These court authorizations do not permit capturing or recording of the content of any such communication under the terms of the court order.

"Currently, the government must apply for a new pen/trap order in every jurisdiction where the target telephone is located. This can cause serious delays that could be devastating to an investigation, particularly where additional criminal or terrorist acts are planned.

"Section [216] does not change the requirement under 18 U.S.C. 3121 that law enforcement seek a court order to install and use pen registers/trap and trace devices. It does not change the law requiring that the attorney for the government certify to the court that the information sought is relevant to an ongoing criminal investigation.

"This section does change the current law requiring the government to obtain the order in the jurisdiction where the telephone (or its equivalent) is located. This section authorizes the court with jurisdiction over the offense of the investigation to issue the order, thus streamlining an investigation and eliminating the need to intrude upon the resources of courts and prosecutors with no connection to the investigation.

"Under the bill, 18 U.S.C. 3123(a) would authorize courts to issue a single pen register/trap and trace order that could be executed in multiple jurisdictions anywhere in the United States. The bill divides the existing 18 U.S.C. 3123(a) into two paragraphs. The new subsection (a)(1) applies to Federal investigations and provides that the order may be issued to any provider of communication services within the United States whose assistance is appropriate to the effectuation of the order. Subsection (a)(2) applies to State law enforcement and does not change the current authority granted to State officials.

"This section updates the language of the statute to clarify that the pen/register authority applies to modern communication technologies. Current statutory references to the target <line,' for example, are revised to encompass a <line or other facility.' Such a facility includes: a cellular telephone number; a specific

cellular telephone identified by its electronic serial number (ESN); an Internet user account or e-mail address; or an Internet Protocol (IP) address, port number, or similar computer network address or range of addresses. In addition, because the statute takes into account a wide variety of such facilities, section 3123(b)(1)(C) allows applicants for pen register or trap and trace orders to submit a description of the communications to be traced using any of these or other identifiers.

"Moreover, the section clarifies that orders for the installation of pen register and trap and trace devices may obtain any non-content information – 'dialing, routing, addressing, and signaling information' – utilized in the processing or transmitting of wire and electronic communications.[3322] Just as today, such an order could not be used to intercept the contents of communications protected by the wiretap statute. The amendments reinforce the statutorily prescribed line between a communication's contents and non-content information, a line identical to the constitutional distinction drawn by the U.S. Supreme Court in Smith v. Maryland, 442 U.S. 735, 741 43 (1979).

"Thus, for example, an order under the statute could not authorize the collection of email subject lines, which are clearly content. Further, an order could not be used to collect information other than 'dialing, routing, addressing, and signaling' information, such as the portion of a URL (Uniform Resource Locator) specifying Web search terms or the name of a requested file or article.

"This concept, that the information properly obtained by using a pen register or trap and trace device is non-content information, applies across the board to all communications media, and to actual connections as well as attempted connections (such as busy signals and similar signals in the telephone context and packets that merely request a telnet connection in the Internet context).

"Further, because the pen register or trap and trace 'device' is often incapable of being physically 'attached' to the target facility due to the nature of modern communication technology, section 101 makes two other related changes. First, in recognition of the fact that such functions are commonly performed today by software instead of physical mechanisms, the section allows the pen register or trap and trace device to be 'attached or applied' to the target facility. Likewise, the definitions of 'pen register' and 'trap and trace device' in section 3127 are revised to include an intangible 'process' (such as a software routine) which collects the same information as a physical device.

[3322] "Thus, for example, non-content information contained in the 'options field' of a network packet header constitutes 'signaling' information and is properly obtained by an authorized pen register or trap and trace device."

"Section [216](c) amends the definition section to include a new nexus standard under 3127(2)(A) to provide that the issuing court must have jurisdiction over the crime being investigated rather than the communication line upon which the device is to be installed. This section is also amended to account for the new technologies relating to the different modes of communication.

"Section [216](d) amends section 3124(d) to ensure that communication providers continue to be covered under that section. Technology providers are concerned that the single order provisions of section 101 of the bill eliminates the protection of 3124(d) of title 18 that provides that 'no cause of action shall lie in any court against any provider of a wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order.' Once there is a nation-wide order it will not specify the provider and thus, the providers believe they could become liable upon compliance with the order. The intent of the current statutory language is to protect providers who comply with court orders, which direct them to assist law enforcement in obtaining the non-content information. The bill removes the phrase 'the terms of' so that the phrase reads 'in accordance with a court order.' This will keep the requirement of a court order but protect the providers even when that order does not specify the provider.

"Current practice includes compliance with pen registers and trap and trace orders by the service provider using its systems and technologies to provide the government all non-content information ordered by the order without the installation of an additional device by the government to capture that order. It is intended that these alternative compliance procedures should continue when the provider is willing and technologically able to comply with the order by these means in an efficient, complete and timely manner.

"Additionally, this section clarifies that upon request, those being served with the generic pen/trap order created under this section shall receive written or electronic certification from the serving officer or official stating that the assistance provided is related to the order," H.Rept. 107-236, at 52-4 (2001).

The critical difference in section 216 is its reporting feature. Federal agents executing a pen register or trap and trace order involving an electronic communications service to the public must report the details of the device's installation and use to the issuing court within 30 days of termination of the order. This section is not subject to the sunset provisions of section 224.

Section 217. Interception of Computer Trespasser Communications

"Cyberattacks may be the work of terrorists or criminals. These attacks come in many forms that cost companies and citizens millions of dollars and endanger public safety. For instance, the denial-of-service attacks, where the objective of the attack is to disable the computer system, can shut down businesses or emergency responders or national security centers. This type of attack causes the

target site's servers to run out of memory and become incapable of responding to the queries of legitimate customers or users. The victims of these computer trespasser's should be able to authorize law enforcement to intercept the trespasser's communications. Section [217] amends current law to clarify that law enforcement may intercept such communications when authorized by the victims, under limited circumstances.

"Section [217](1) of the bill adds to the definitions under 18 U.S.C. 2510 the term: (1) <protected computer' and provides that the term has the same meaning set forth in 1030 of title 18; and (2) the term <computer trespasser' means a person who is accessing a protected computer without authorization and thus has no reasonable expectation of privacy in any communication transmitted to, through, or from the protected computer.

"Section [217](2) of the bill amends current law to allow victims of computer intrusions to authorize law enforcement to intercept the communications of a computer trespasser [that have been transmitted to, from or through the protected computer], under limited circumstances. The circumstances are: (1) the owner or operator of the protected computer must authorize the interception of the trespasser's communications; (2) the person who intercepts the communication must be lawfully engaged in an investigation; (3) the person acting under color of law has reasonable grounds to believe that the contents of the computer trespasser's communication to be intercepted will be relevant to the investigation; and (4) the investigator may only intercept communications of the computer trespasser," H.Rept. 107-236, at 55-6 (2001). This section is subject to the sunset provisions of section 224.

Section 218. Foreign Intelligence Information

The USA PATRIOT Act contemplates a closer working relationship between criminal and intelligence investigators than has previously been the case. As originally enacted the application for a FISA surveillance order required certification of the fact that "the purpose for the surveillance is to obtain foreign intelligence information," 50 U.S.C. 1804(a)(7)(B)(2000 ed.)(emphasis added). From the beginning, defendants have questioned whether authorities had used a FISA surveillance order against them in order to avoid the predicate crime threshold for a Title III order. Out of these challenges arose the notion that perhaps "the purpose" might not always mean the sole purpose.[3323]

[3323] In United States v. Truong Dinh Hung, 629 F.2d 908, 915 (4th Cir. 1980), decided after FISA became effective but on the basis of pre-existing law, the court declared, "as the district court ruled, the executive should be excused from securing a warrant only when the surveillance is conducted <primarily' for foreign intelligence reasons. We think that the district court adopted the proper test, because once surveillance becomes primarily a criminal investigation, the courts are entirely competent to make the usual probable cause determination, and because, importantly, individual privacy interests come to the fore and government foreign policy concerns

The Justice Department sought FISA surveillance and physical search authority on the basis of "a" foreign intelligence purpose. Section 218 instead demands certification that foreign intelligence gathering is a "significant purpose" for the FISA surveillance or physical search order application, 50 U.S.C. 1804(a)(7)(B), 1823(a)(7)(B). This a more exacting standard than the "a purpose" threshold proposed by the Justice Department, but a clear departure from the original "the purpose" entry point. FISA once described a singular foreign intelligence focus prerequisite for any FISA surveillance application, a focus that implicitly discouraged law enforcement participation. Section 218 encourages coordination between intelligence and law enforcement officials. Section 504, discussed below, confirms that such coordination is no impediment to a "significant purpose" certification, 50 U.S.C. 1806(k), 1825(k). Section 218 is subject to the sunset provisions of section 224.

Section 219. Single-Jurisdiction Search Warrants for Terrorism

"Rule 41(a) of the Federal Rules of Criminal Procedure currently requires that a search warrant be obtained within the judicial district where the property to be searched is located. The only exception is where property or a person now in the district might leave before the warrant is executed. This restriction often causes unnecessary delays and burdens on law enforcement officers investigating

---

recede when the government is primarily attempted to form the basis for a criminal prosecution." Subsequent case law, however, is not as clear as it might be: e.g., United States v. Duggan, 743 F.2d 59, 77 (2d Cir. 1984)("FISA permits federal officials to obtain orders authorizing electronic surveillance for the purpose of obtaining foreign intelligence information. The requirement that foreign intelligence information be the primary objective of the surveillance is plain not only from the language of Sec. 1802(b) but also from the requirements in Sec. 1804 as to what the application must contain. The application must contain a certification by a designated official of the executive branch that the purpose of the surveillance is to acquire foreign intelligence information, and the certification must set forth the basis for the certifying officials's belief that the information sought is the type of foreign intelligence information described"); United States v. Pelton, 835 F.2d 1067, 1075-76 (4th Cir. 1987)("We also reject Pelton's claim that the 1985 FISA surveillance was conducted primarily for the purpose of his criminal prosecution, and not primarily for the purpose of obtaining foreign intelligence information. . . . We agree with the district court that the primary purpose of the surveillance, both initially and throughout was to gather foreign intelligence information. It is clear that otherwise valid FISA surveillance is not tainted simply because the government can anticipate that the fruits of the surveillance may later be used . . . as evidence in a criminal trial"); United States v. Sarkissian, 841 F.2d 959, 907-8 (9th Cir. 1988)("Defendants rely on the primary purpose test articulated in United States v. Truong Dinh Hung. . . . One other court has applied the primary purpose test. Another court has rejected it . . . distinguishing Truong. A third court has declined to decide the issue. We also decline to decide the issue"); United States v. Johnson, 952 F.2d 565, 572 (1st Cir. 1991)("Appellants attack the government's surveillance on the ground that it was undertaken not for foreign intelligence purposes, but to gather evidence for a criminal prosecution. FISA applications must contain, among other things, a certification that the purpose of the requested surveillance is the gathering of foreign intelligence information. . . .Although the evidence obtained under FISA subsequently may be used in criminal prosecutions, the investigation of criminal activity cannot be the primary purpose of the surveillance").

terrorist activities that have occurred across multiple judicial districts. These delays can have serious adverse consequences on an ongoing terrorism investigation," H.Rept. 107-236, at 72 (2001).

Section 219 allows a magistrate in the district in which a domestic or international terrorism investigation is being conducted to issue a warrant to be executed either "within or outside the district," F.R. Crim. P. 41(a)(3). Although most useful in criminal investigations spanning a number of states within the United States, nothing in the section expressly precludes its application overseas when the law of the place permits such execution.

The Fourth Amendment does not apply to the overseas searches of the property of foreign nationals, United States v. Verdugo-Urquidez, 494 U.S. 259 (1990), but it does reach the search of American property overseas by American authorities, United States v. Barona, 56 F.3d 1087, 1092 (9th Cir. 1995). Yet neither Rule 41 nor any other provision of prior federal law apparently contemplated extraterritorial execution of federal search warrants, cf., F.R.Crim.P.41, Advisory Committee Notes: 1990 Amendment (discussing a proposal for exterritorial execution that the Supreme Court rejected).[3324] Section 219 is not subject to the sunset provisions of section 224.

Section 220. Nationwide Service of Search Warrants for Electronic Evidence

"Title 18 U.S.C. 2703(a) requires a search warrant to compel service providers to disclose unopened e-mails. This section does not affect the requirement for a search warrant, but rather attempts to address the investigative delays caused by the cross-jurisdictional nature of the Internet. Currently, Federal Rules of Criminal Procedure 41 requires that the 'warrant' be obtained 'within the district' where the property is located. An investigator, for example, located in Boston who is investigating a suspected terrorist in that city, might have to seek a suspect's electronic e-mail from an Internet service provider (ISP) account located in California. The investigator would then need to coordinate with agents, prosecutors and judges in the district in California where the ISP is located to obtain a warrant to search. These time delays could be devastating to an investigation, especially where additional criminal or terrorist acts are planned.

[3324] The Code does still carry remnants of the consular courts which speak of the overseas execution of arrest warrants in places where the United States has "extraterritorial jurisdiction," 18 U.S.C. 3042. The history of the provision makes it clear that the phrase "extraterritorial jurisdiction" was intended to coincide with those places in which we had consular courts, see, S.ReptNo. 73-217, at. 3 (1934), reprinted, 78 Cong.Rec. 4982-983 (1934)("The countries to which the proposed bill, if enacted into law, would relate are the following, in which the United States exercises extraterritorial jurisdiction: China, Egypt, Ethiopia, Muscat, and Morocco"); 22 U.S.C. 141 (1926 ed.)(conferring judicial powers on consular courts there identified as those located in China, Egypt, Ethiopia, Muscat, Morocco, Siam and Turkey).

"Section [220] amends 2703 to authorize the court with jurisdiction over the investigation to issue the warrant directly, without requiring the intervention of its counterpart in the district where the ISP is located," H.Rept. 107-236, at 57 (2001). Section 220 is subject to the sunset provisions of section 224.

Section 221. Trade Sanctions

The Trade Sanctions Reform and Export Enhancement Act of 2000, Title IX of Public Law 106-387, 114 Stat. 1549A-67, restricts the President's authority to impose unilateral agricultural and medical sanctions, subject to certain exceptions. One of the exceptions permits an export ban on products that might be "used to facilitate the development or production of a chemical or biological weapon or weapon of mass destruction,"§904(2)(C). Section 221 amends paragraph 904(2)(C) to enlarge the ban to reach products that might facilitate the design, development or production of such weapons. The section amends subsection 906(a) of the trade sanctions act to allow for the sale of agricultural and medical products to entities in Syria and North Korea and to permit such sales under license to areas of Afghanistan controlled by the Taliban.

The section further declares that the trade sanctions act should not be construed to curtail criminal or civil penalties available with respect to the export of agricultural products, medicine, or medical devices in violation of restrictions on dealings with:

- a foreign individual or entity designated pursuant to Executive Order 12947, 50 U.S.C. 1701 note (Prohibiting Transactions With Terrorists);
- a foreign terrorist organization, 18 U.S.C. 2339B;
- a foreign individual or entity designated pursuant to Executive Order 13224, 66 Fed.Reg. 49077 (Sept. 25, 2001)(Blocking Property . . . [of] Persons Who . . . Support Terrorism);
- a narcotics trafficker designated pursuant to Executive Order 12979, 50 U.S.C. 1701 note (Blocking Assets . . . With Significant Narcotics Traffickers) or to the Foreign Narcotics Kingpin Designation Act, Public Law 106-120; or
- any foreign individual or entity subject to restriction for involvement in weapons of mass destruction or missile proliferation.

This section is not subject to the sunset provisions of section 224.

Section 222. Assistance to Law Enforcement Agencies

FISA, Title III, and the related provisions of law now compel communications service providers to assist in the execution of court orders issued under those authorities, e.g., 50 U.S.C. 1805(c)(2)(B), 18 U.S.C. 2518(4). The House Committee on the Judiciary observed with regard to an earlier version of this section that, "this Act is not intended to affect obligations under the Communications Assistance for Law Enforcement Act, 47 U.S.C. 1001 et seq., nor

does the Act impose any additional technical obligation or requirement on a provider of wire or electronic communication service or other person to furnish facilities or technical assistance," H.Rept. 107-236, at 62-3 (2001). In its final form, the section guarantees reasonable reimbursement for the costs of service providers, landlords, custodians and others who supply facilities and technical assistance pursuant to section 216 (relating to law enforcement pen registers and trap and trace orders). This section is not subject to the sunset provisions of section 224.

Section 223. Civil Liability of Certain Unauthorized Disclosures

Section 223 establishes a claim against the United States for not less than $10,000 and costs for violations of Title III, chapter 121, or the Foreign Intelligence Surveillance Act (FISA), and emphasizes the prospect of administrative discipline for offending federal officials. This section is subject to the sunset provisions of section 224.

Section 224. Sunset

Several of the amendments which grant federal law enforcement or intelligence officers expanded interception powers expire with respect to any foreign intelligence investigation initiated after January 1, 2006 and to any criminal investigation of misconduct occurring only after that date. The provisions which expire are:

- section 201 (authority to intercept wire, oral, and electronic communications relating to terrorism);
- section 202 (authority to intercept wire, oral, and electronic communications relating to computer fraud and abuse offenses);
- subsection 203(b) (authority to share electronic, wire, and oral interception information);
- subsection 203(d) (general authority to share foreign intelligence information);
- section 204 (clarification of intelligence exceptions from limitations on interception and disclosure of wire, oral, and electronic communications);
- section 206 (roving surveillance authority under the Foreign Intelligence Surveillance Act of 1978);
- section 207 (duration of FISA surveillance of non-United States persons who are agents of a foreign power),
- section 209 (seizure of voice-mail messages pursuant to warrants);
- section 212 (emergency disclosure of electronic surveillance);
- section 214 (pen register and trap and trace authority under FISA);
- section 215 (access to records and other items under the Foreign Intelligence Surveillance Act);
- section 217 (interception of computer trespasser communications);
- section 218 (foreign intelligence information);

- section 220 (nationwide service of search warrants for electronic evidence);
- section 223 (civil liability for certain unauthorized disclosures); and
- section 225 (immunity for compliance with FISA wiretap).

The permanent sections and subsections of title II, which do not expire, are:

- subsection 203(a) (sharing grand jury information);
- subsection 203(c) (Attorney General guidelines for sharing grand jury
- information);
- section 205 (employment of FBI translators);
- section 208 (number and residence of FISA court judges);
- section 210 (nationwide subpoenas for electronic communications records),
- section 211 (clarification of scope of cable provider obligations);
- section 213 (delayed notification of sneak and peek warrant execution);
- section 216 (modification of authorities relating to pen registers and trap and trace devices);
- section 219 (single-jurisdiction search warrants for terrorism);
- section 221 (trade sanctions); and
- section 222 (assistance to law enforcement agencies).

Section 225. Immunity for Compliance With FISA Wiretap

The Foreign Intelligence Surveillance Act orders may include instructions requiring communications service providers and others to assist officers in the execution of the order, 50 U.S.C. 1805(c)(2)(B), 1824(c)(2)(B), 1842(c)(2)(B). Section 225 immunizes those who do from civil liability, 50 U.S.C. 1805(h). This section is subject to the sunset provisions of section 224.

Title III – International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001[3325]

Section 301. Short Title

The popular name for Title III of the USA PATRIOT Act is the International Money Laundering Abatement and Financial Anti-Terrorism Act of 2001.

Section 302. Findings and Purposes

Section 302 describes the findings and purposes for the enactment of the International Money Laundering Abatement and Financial Anti-Terrorism Act.

[3325] M. Maureen Murphy, a legislative attorney in the American Law Division prepared the section by section analysis of Title III.

Section 303. 4-Year Congressional Review; Expedited Consideration

The International Money Laundering Abatement and Financial Anti-Terrorism Act of this title will sunset after four years upon passage of joint resolution of repealed. Any joint resolution of repeal is to be afforded "fact track" consideration.

Subtitle A–International Counter Money Laundering and Related Measures

Section 311. Special Measures for Jurisdictions, Financial Institutions, or International Transactions of Primary Money Laundering Concern

Section 311 authorizes the Secretary of the Treasury (the Secretary) to impose certain regulatory restrictions, known as "special measures," upon finding that a jurisdiction outside the U.S., a financial institution outside the U.S., a class of transactions involving a jurisdiction outside the U.S., or a type of account, is "of primary money laundering concern." To make this finding, the Secretary must consult with the Secretary of State and the Attorney General and consider certain factors relating to the foreign jurisdiction or the particular institution targeted. Among the factors relating to a jurisdiction are: involvement with organized crime or terrorists, bank secrecy laws and regulations, the existence a mutual legal assistance treaty with the U.S., and level of official corruption. The special measures generally involve detailed record keeping and reporting requirements relating to underlying transactions and beneficial ownership of accounts. Special measures could involve prohibiting the maintenance of payable-through or correspondent accounts for such institutions or jurisdictions, provided that there has been consultation with the Secretary of State, the Attorney General, and the Chairman of the Federal Reserve Board, as well as with other appropriate federal banking agencies and consideration has been given to whether other nations have taken similar action, whether there would be a significant competitive disadvantage on U.S. financial institutions, and effect upon the international payment system. "Account" is defined for banks, with authority delegated to the Secretary to define the term for other financial services businesses upon consultation with the appropriate federal regulators. The Secretary is required to issue a regulation defining "beneficial ownership" for purposes of this legislation.

Section 312. Special Due Diligence for Correspondent Accounts and Private Banking Accounts

Section 312 requires every financial institution with a private banking or correspondent account for a foreign person or bank to establish policies and controls designed to detect and report money laundering through the accounts. If a correspondent account is maintained for a foreign bank that operates under an offshore license–i.e., does not and may not do banking business in the chartering country–or that is licensed by a jurisdiction designated for special measures or listed as non-cooperative by an international organization in which the U.S. participates and concurs, enhanced due diligence policies are required.

For correspondent accounts for foreign banks, U.S. banks, at the minimum, must secure ownership information on the foreign bank, maintain enhanced scrutiny of the account, and ascertain due diligence information on the foreign banks for which the target bank provides correspondent banking services. For foreign private banking clients, i.e., those with aggregated deposits of $1,000,000, information must be secured on the identity of the owners of the accounts, including beneficial owners, and the source of the funds; enhanced scrutiny is required for accounts held for senior foreign political figures. This section becomes effective 9 months after enactment; regulations must be issued within 6 months of enactment.

Section 313. Prohibition on United States Correspondent Accounts with Foreign Shell Banks

Section 313 prohibits U.S. banks, thrifts, private banks, foreign bank agencies and branches operating in the U.S., and brokers and dealers licensed under the Securities Exchanges Act of 1934, 15 U.S.C. 78a et seq., from maintaining correspondent accounts for foreign shell banks–banks that have no physical presence in any country. It requires that the covered institutions take reasonable steps to preclude their providing services to such shell banks through other banks and requires the Secretary to issue implementing regulations.

Section 314. Cooperative Efforts to Deter Money Laundering

Section 314 requires the Secretary to issue regulations within 120 days of enactment to encourage further cooperation among financial institutions and regulatory and law enforcement authorities to promote sharing information on individuals, entities, and organizations engaged inor suspected of engaging interrorist acts or money laundering. In these regulations, the Secretary may require each financial institution to designate persons to receive information and to monitor accounts and to establish procedures to protect the shared information. No information received by a financial institution under this provision may be used for any purpose other than identifying and reporting activities involving terrorism or money laundering. If a financial institution uses this information for those purposes, it may not be held liable for unauthorized disclosure or failure to provide a notice under any law or regulation, state or federal, or any contract or agreement. The Secretary is required to provide a semiannual report analyzing suspicious activity reports.

Section 315. Inclusion of Foreign Corruption Offenses As Money Laundering Crimes

Section 315 adds to the list of offenses under foreign law, the proceeds of which may form an element of a federal money laundering prosecution: any crime of violence; bribery of a public official; theft, embezzlement, or misappropriation of public funds; certain smuggling or export control violations; and, offenses for which the U.S. would be obliged to extradite alleged offenders. Also added would

be certain offenses under the U.S. criminal code relating to customs, importation of firearms, firearms trafficking, computer fraud and abuse, and felony violations of the Foreign Agents Registration Act.

Section 316. Anti-Terrorist Forfeiture Protection

Prior to enactment of the USA PATRIOT Act, the President had authority to order the vesting of seized foreign assets under the Trading With the Enemy Act §5(b), 50 U.S.C. App. 5(b), which applies when there has been a declaration of war, but not under the International Emergency Economic Powers Act (IEEPA), 50 U.S.C. 1702), which applies when the President has declared the existence of an unusual or extraordinary threat to the U.S. national security, foreign policy, or economy having its source, in whole or substantial part, outside the United States. Section 106 of the new law amends IEEPA to authorize the President, "when the United States is engaged in armed hostilities or has been attacked by a foreign country or foreign nationals," to "confiscate any property, subject to the jurisdiction of the United States, of any foreign person, foreign organization, or foreign country that he determines has planned, authorized, aided, or engaged in such hostilities or attacks against the United States."

Section 316 authorizes judicial review of confiscation of terrorist related assets and sets forth two defenses for those claiming the property that must be proven by a preponderance of the evidence: (1) that the property is not subject to forfeiture under the applicable law, and (2) the innocent owner defense detailed in the criminal forfeiture provision of 18 U.S.C. 983(d). It also authorizes the government to offer otherwise inadmissible evidence provided the court finds that complying with the Federal Rules of Evidence would jeopardize national security. There is also a clause alluding to the right to raise Constitutional claims and claims under the Administrative Procedure Act and a savings clause preserving other remedies.

Section 317. Long-Arm Jurisdiction Over Foreign Money Launderers

Section 317 provides jurisdiction over foreign persons, including financial institutions, for substantive money laundering offenses under 18 U.S.C. 1956 and 1957, provided there is a valid service of process and either the offense involved a transaction in the U.S. or the property has been the subject of a forfeiture judgment or a criminal sentence. The district courts are authorized to appoint a receiver to take control of the property.

Section 318. Laundering Money Through a Foreign Bank

Section 318 amends the substantive money laundering criminal statute, 18 U.S.C. 1956, to cover laundering money through a foreign bank.

Section 319. Forfeiture of Funds in United States Interbank Accounts

Section 319 amends 18 U.S.C. 981 to permit forfeiture, including forfeiture under the Controlled Substances laws, of accounts in offshore offices of foreign banks by substituting funds in interbank accounts in U.S. financial institutions up to the value of the funds in the targeted account. The section authorizes the Attorney General to suspend or terminate such a forfeiture action on conflict-of-law grounds or upon a finding that to do so would be in the interest of justice and would not harm the national interests of the U.S.

Section 319, effective within 60 days of enactment, amends the Currency and Transaction Reporting Act, 31 U.S.C. 5311, et seq., to require U.S. banks, thrifts, private banks, foreign bank agencies and branches operating in the U.S., and brokers and dealers licensed under the Securities Exchanges Act of 1934, 15 U.S.C. 78a et seq., to provide federal regulators, upon request, information on the institution's compliance with anti-money laundering requirements or on a customer's account, within 120 hours. It also authorizes the Secretary of the Treasury or the Attorney General to subpoena records from a foreign bank that has a correspondent account in the U.S. that relate to that account, including records maintained abroad. It requires U.S. institutions maintaining correspondent accounts for foreign banks to maintain records identifying the owners of such foreign banks and indicating the name and address of a U.S. resident authorized to accept service of legal process for records relating to the correspondent account. U.S. institutions having such correspondent accounts are required to provide federal law enforcement officers with these names and addresses within 7 days of receiving a request and are required to terminate correspondent accounts within 10 business days of receiving a notice from the Secretary or the Attorney General that the foreign bank has failed to comply with a subpoena or to contest its issuance. U.S. financial institutions are not to be held liable for terminating such accounts and are subject to civil penalties of $10,000 per day for failing to do so.

This section also amends the criminal forfeiture provisions of the Controlled Substances Act, 21 U.S.C. 853(p) and 853(e) to permit a court to order return to the jurisdiction of substitute assets, property that may be substituted for unreachable property subject to forfeiture, and to issue a pre-trial order to a defendant to repatriate such substitute assets.

Section 320. Proceeds of Foreign Crimes

Section 320 authorizes the forfeiture of property derived from or traceable to violations of felonious foreign controlled substances laws, provided the offense is punishable by death or a term of imprisonment of more than one year under the law of the foreign nation and under U.S. law, had it occurred within the jurisdiction of the U.S.

Section 321. Financial Institutions Specified in Subchapter II of Chapter 53 of Title 31, United States Code

Section 321 adds credit unions and CFTC-regulated or registered futures commission merchants, commodity trading advisors, and commodity pool operators to the specific list of financial institutions subject to the requirements of the Currency and Foreign Transaction Reporting Act. Pre-existing law did not specifically include these entities although it delegated broad authority to the Secretary to apply the requirements to "any other business ... whose cash transactions have a high degree of usefulness in criminal, tax, or regulatory matters."

Section 322. Corporation Represented by a Fugitive

Section 322 amends 28 U.S.C. 2466 to include corporations having a majority stockholder who is a fugitive, thus, disallowing such corporations to file innocent owner to successfully pursue innocent owner claims in a civil or criminal forfeiture cases.

Section 323. Enforcement of Foreign Judgments

Section 323 amends 28 U.S.C. 2467 to extend authority for judicial enforcement of foreign confiscation from the previous provisions limiting such enforcement to confiscations related to drug trafficking offenses. Under the newly enacted provision U.S. district courts may enforce foreign confiscations related to any offense under foreign law that, if committed under U.S. law, would have permitted forfeiture.

Section 324. Report and Recommendation

Section 324 requires the Secretary of the Treasury, within 30 months of enactment, to report on operations respecting the provisions relating to international counter-money laundering measures and any recommendations to Congress as to advisable legislative action.

Section 325. Concentration Accounts at Financial Institutions

Section 325 authorizes the Secretary of the Treasury to prescribe regulations governing maintenance of concentration accounts by financial institutions. If issued, such regulations must prohibit financial institutions from allowing clients to direct transactions through those accounts, prohibit financial institutions from informing customers of the means of identifying such accounts, and require each financial institution to establish written procedures to document all transactions involving a concentration account that amounts belonging to each customer may be identified.

Section 326. Verification of Identification

Section 326 requires the Secretary of the Treasury, jointly with appropriate regulators of financial institutions, within a year of enactment, to prescribe

minimum standards for identifying customers opening accounts at financial institutions. These are to include procedures to verify customer identity and maintain records of information used to verify identity. They are also to require that government lists of terrorists and terrorist organizations be consulted. Under this section, the Secretary is required to submit a report to Congress within six months of enactment, recommending a means of insuring similarly accurate identification of foreign nationals, requiring an identification number similar to a Social Security number or a tax identification number for foreign nationals opening accounts at financial institutions, and setting up a system for financial institutions to review information held by government agencies to verify identities of foreign nationals opening accounts.

Section 327. Consideration of Anti-Money Laundering Record

Section 327 amends the Bank Holding Company Act and The Federal Deposit Insurance Act, to require that, before approving certain acquisition or merger applications under the Bank Holding Company Act or the Federal Deposit Insurance Act, the Board of Governors of the Federal Reserve System and the Federal Deposit Insurance Corporation must consider the institution's effectiveness in combating money laundering.

Section 328. International Cooperation on Identification of Originators of Wire Transfers

Section 328 requires the Secretary of the Treasury to encourage foreign governments to require the name of the originator in wire transfer instructions and include it from origination to disbursement. The Secretary is to report annually on progress toward this end to House Financial Services Committee and Senate Banking, Housing, and Urban Affairs Committee.

Section 329. Criminal Penalties

Section 329 criminalizes the soliciting of a bribe by anyone acting on behalf of an entity of the Federal Government in connection with the administration of the International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001, subject to a fine of up to three time the value of the thing of value constituting the bribe, 15 years imprisonment, or both.

Section 330. International Cooperation in Investigations of Money Laundering, Financial Crimes, and the Finances of Terrorist Groups

Section 330 states the sense of Congress that international negotiations should be pursued for further cooperative efforts to insure that foreign financial institutions maintain adequate records relating to foreign terrorist organizations and money launderers and make such records available to U.S. law enforcement officials and domestic financial institution supervisors.

Subtitle B–Bank Secrecy Act Amendments and Related Improvements

Section 351. Amendments Relating to Reporting of Suspicious Activities

Section 351 amends the Currency and Foreign Transactions Reporting Act, 31 U.S.C. 5318(g)(3), to extend the safe harbor provisions for financial institutions and their employees who provide information as to possible law violations to cover all voluntary disclosures of possible law violations made to any federal government agency. Also covered are employees or agents of institutions who require others to make such disclosures. The immunity provided under the legislation covers potential liability under contracts and other legally enforceable agreements. Previously, immunity was provided only for disclosures of violation of law or regulation pursuant to law or regulation; there was no specific immunity for those requiring others to make disclosures; and, immunity extended only to liability under laws or regulations of the United States or constitution, law, or regulation of a state or political subdivision thereof. The section makes it clear that the liability does not extend to prosecutions brought by governmental entities. Disclosure to the subject of the tip-off is prohibited. Information disclosed about potential law violations may be used in employment references to other financial institutions as well as, under the rules of the securities exchanges, in termination notices.

Section 352. Anti-Money Laundering Programs

Section 352, effective 180 days after enactment, requires each financial institution to develop an anti-money laundering program to include development of internal policies, designation of a compliance officer, ongoing employee training, and an independent audit function to test the programs. It authorizes the Secretary of the Treasury to prescribe minimum standards for such programs and to exempt those financial institutions that are not covered by the regulations promulgated under the Currency and Foreign Transactions Reporting Act. It requires the Secretary to prescribe regulations that consider the extent to which the requirements imposed under this section comport with the size, location, and activities of the financial institutions to which they apply.

Section 353. Penalties for Violations of Geographic Targeting Orders and Certain Recordkeeping Requirements, and Lengthening Effective Period of Geographic Targeting Orders

Section 353 extends the civil and criminal penalties under the Currency and Foreign Transactions Reporting Act, 31 U.S.C. 5321(a) and 5322, to include violations of geographic targeting orders issued under that Act and willful violations of regulations prescribed under the record keeping requirements of the Bank Secrecy Act, found in Section 21 of the FDIA, 12 U.S.C. 1829(b), or violations of regulations covering uninsured financial institutions issued by Treasury under the authority of 12 U.S.C. 1951 -1959. Before enactment of USA-PATRIOT, 12 U.S.C. 1829(b) carried no criminal penalties and set civil penalties

for violations of regulations issued under 12 U.S.C. 1829(b) at up to $10,000. Section 1955 of Title 12, U.S.C. carried civil penalties of up to $10,000; and, 12 U.S.C. 1956 carried a criminal penalty of up to $1,000 and imprisonment for one year. 31 U.S.C. 5321(a) permits civil penalties of $25,000 or the amount of the instrument (not to exceed $100,000); 31 U.S.C. 5322 permits criminal penalties of up to $250,000 in fines and imprisonment of up to 5 years for a single offense and enhancement for offenses committed in conjunction with other offenses or as a pattern of criminal activity.

The section also extends the prohibitions on structuring transactions to avoid reporting requirements, 31 U.S.C. 5324, to cover structuring to avoid geographic targeting orders and record keeping requirements of the Bank Secrecy Act, found in Section 21 of the FDIA, 12 U.S.C. 1829(b) and 12 U.S.C. 1951-1959. It extends the permissible length of geographic targeting orders from 60 to 180 days.

Section 354. Anti-Money Laundering Strategy

Section 354 includes among the areas suggested for inclusion in the annual anti-money laundering strategy data regarding the funding of international terrorism acts.

Section 355. Authorization to Include Suspicions of Illegal Activity in Written Employment References

Section 355 authorizes depository institutions, "[n]otwithstanding any other provision of law," to disclose the possible involvement of institution-affiliated parties in potentially unlawful activity. Such disclosures may be made to other insured depository institutions requesting employment references, provided the disclosure is not made with malicious intent.

Section 356. Reporting of Suspicious Activities Reports by Securities Brokers and Dealers; Investment Company Study

Section 356 requires the Secretary of the Treasury, by January 1, 2002, to publish proposed regulations requiring registered brokers and dealers to file suspicious activity reports under 31 U.S.C. 5318(g). It also authorizes the Secretary to prescribe such regulations for futures commission merchants, commodity trading advisors, and commodity pool operators registered under the Commodity Exchange Act. It also requires a report, within one year of enactment, recommending effective regulations under the Currency and Foreign Transactions Reporting Act for investment companies, as defined in the Investment Company Act of 1940, and to evaluate the possibility of requiring trusts and personal holding companies to disclose their beneficial owners when opening accounts at depository institutions.

Section 357. Special Report on Administration of Bank Secrecy Provisions

Section 357 requires the Secretary of the Treasury to submit a report, within six months of enactment, on the role of the Internal Revenue Service in administering the Bank Secrecy Act's Currency and Foreign Transactions Reporting Act. The report is specifically to address such issues as whether processing of information is to be shifted from the Internal Revenue Service and whether the Internal Revenue Service is to retain authority for auditing money services and gaming businesses' compliance.

Section 358. Bank Secrecy Provisions and Activities of United States Intelligence Agencies to Fight International Terrorism

Section 358 authorizes the Secretary of the Treasury to refer suspicious activity reports to U.S. intelligence agencies for use in the conduct of intelligence or counterintelligence activities to protect against international terrorism. It authorizes the release of information under the Currency and Foreign Transactions Reporting Act and other provisions of the Bank Secrecy Act, the Right to Financial Privacy Act, and the Fair Credit Reporting Act, to U.S. intelligence agencies by amending 31 U.S.C. 5311, 5318(g)(4)(b), 5319; 12 U.S.C. 1829(b), 1953; 12 U.S.C. 3412(a); 15 U.S.C. 1681x.

Section 359. Reporting of Suspicious Activities by Underground Banking Systems

Section 359 specifically includes "a licensed sender of money or any other person who engages as a business in the transmission of funds, including any person who engages as a business in an informal money transfer system or any network of people who engage as a business in facilitating the transfer of money domestically or internationally outside of the conventional financial institutions system" as a "financial institution" subject to the requirements of the Currency and Foreign Transactions Reporting Act. It subjects them to any regulations promulgated under the authority of section 21 of the Federal Deposit Insurance Act, 12 U.S.C. 1829b. That section of the law provides authority for the regulations issued under 31 C.F.R. Part 103, requiring reports of currency and foreign transactions, including those requiring suspicious activity reports from money services businesses, 31 C.F.R. § 103.20. Section 359 also mandates a report by the Secretary, within a year of enactment, on whether further legislation is needed with respect to these underground banking systems, including whether the threshold for reporting suspicious activities ($2,000) should be lowered for them.

Section 360. Use of Authority of United States Executive Directors

Section 360 authorizes the President to direct the U. S. Executive Directors of international financial institutions to use their voice and vote to support countries or entities that have contributed to the U.S. anti-terrorism efforts and ensure that no funds of their institutions are paid to persons who threaten to commit or support terrorism. International financial institutions, as defined in 22 U.S.C. 262r(c)(2), include the International Monetary Fund, the International

Bank for Reconstruction, the European Bank for Reconstruction and Development, the International Development Association, the International Finance Corporation, the Multilateral Investment Guarantee Agency, the African Development Bank, the African Development Fund, the Asian Development Bank, the Bank for Economic Development and Cooperation in the Middle East and North Africa, and the InterAmerican Investment Corporation.

Section 361. Financial Crimes Enforcement Network (FinCEN)

Section 361, by enacting 31 U.S.C. 310, transforms FinCEN from a Treasury Department bureau established administratively to a statutory bureau in the Treasury Department. It specifies that it is to be headed by a Director to be appointed by the Secretary. It details its duties and powers, not all of which are summarized here. Subject to applicable legal requirements and guidance by Treasury, FinCEN is to maintain a government-wide data access service to information collected under the anti-money laundering reporting laws, information on currency flows, and other records maintained by other government offices as well as privately and publically available information. It is to analyze and disseminate data : (1) to federal, state, local, and foreign law enforcement officials to identify possible criminal activity; and (2) to regulatory officials to identify possible violations of the anti-money laundering reporting requirements. It is to determine emerging trends and methods in money laundering, and support intelligence activities against international terrorism.

FinCEN is to establish and maintain a financial crimes communications center to furnish law enforcement authorities with intelligence information relating to investigations and undercover operations. It is to furnish informational services to financial institutions, federal regulatory agencies, and law enforcement authorities, in the interest of countering terrorism, organized crime, money laundering, and other financial crimes. It is to assist law enforcement and regulatory authorities in combating the use of informal nonbank networks permitting transfer of funds or the equivalent of funds without records and in insuring compliance with criminal and tax laws. It is to provide computer and data support and data analysis to the Secretary of the Treasury for tracking and controlling foreign assets. It is to administer the anti-money laundering reporting requirements as delegated by the Secretary of the Treasury.

Section 361 further specifies that the Secretary is to proscribe procedures with respect to the government-wide data access service and the financial crimes communications center maintained by FinCEN to provide efficient entry, retrieval, and dissemination of information. This is to include a method for submitting reports by Internet, cataloguing of information, and prompt initial review of suspicious activity reports. Section 361 requires the Secretary to develop, in accordance with the Privacy Act, 5 U.S.C. 552a, and the Right to Financial Privacy Act, 12 U.S.C. 3401, et seq., procedures for determining access, limits on use, and "how information about activities or relationships which

involve or are closely associated with the exercise of constitutional rights are screened out."

Appropriations of such sums as are necessary are authorized for fiscal years through 2005.

The Secretary is to study methods for improving compliance with the reporting requirements under 31 U.S.C. 5314, relating to foreign currency transactions, and to submit an annual report to Congress on the subject, beginning six months after enactment.

Section 362. Establishment of Highly Secure Network

Section 362 requires the Secretary to establish as operational within nine months, a highly secure network in FinCEN to allow financial institutions to file electronically reports required under the Bank Secrecy Act and to provide financial institutions with alerts and other information regarding suspicious activities warranting immediate and enhanced scrutiny.

Section 363. Increase in Civil and Criminal Penalties for Money Laundering

Section 363 amends 31 U.S.C. 5321(a) and 5322 to permit the Secretary to impose a civil money penalty and a court to impose a criminal penalty equal to 2 times the amount of the transaction, but not more than $1,000,000 for violations of the suspicious activity reporting requirements, under 31 U.S.C. 5318(i) and (j) or any special measures imposed under 31 U.S.C. 5318A. Under pre-existing law, the Secretary had authority to impose a civil money penalty of the amount of the transaction, up to $100,000, or $25,000; and, a criminal fine for a violation of the suspicious activity reporting requirement was set at not more than $250,000.

Section 364. Uniform Protection Authority for Federal Reserve Facilities

Section 364 authorizes the Federal Reserve Board to issue regulations, subject to the approval of the Attorney General, to authorize personnel to act as law enforcement officers to protect the Board's personnel, property, and operations, including the Federal Reserve banks, and for such personnel to carry firearms and make arrests. Pre-existing law provided no such authority.

Section 365. Reports Relating to Coins and Currency Received in Non-Financial Trade of Business

Section 365 adds a new section to the anti-money laundering reporting requirements, 31 U.S.C. 5331. It requires anyone engaging in a trade or business, who receives $10,000 in coins or currency (including foreign currency and financial instruments) in a single transaction or in two related transactions to file a report on the transaction to FinCEN as prescribed by the Secretary in regulations. The form for such reports must include the name and address of the

person from whom the coins or currency are received, the date and nature of the transaction, and such other information as the Secretary may prescribe. Exemptions are made for reports filed by financial institutions under 31 U.S.C. 5313 and its implementing regulations, and for transactions occurring outside the United States–unless the Secretary so prescribes. The section also includes a provision that prohibits structuring transactions to cause such businesses to evade these reporting requirements or requirements under implementing regulations.[3326] "Nonfinancial trade or business" is defined to mean any trade or business other than a financial institution subject to reporting requirements under 31 U.S.C. 5313 and regulations thereunder.

Under pre-existing law, the Secretary had broad authority to apply the reporting requirements of 31 U.S.C. 5313 by regulation. Under 31 U.S.C. 5312 "financial institution" is defined explicitly to include many non-financial businesses including vehicle sales, real estate closings, the United States Postal Service, and casinos. 31 U.S.C. 5312(a)(2)(T), (U), (V), and (X). It also may include any business or agency determined by the Secretary to engage in an activity that is a substitute for any of the activities listed as "financial institutions," and "any other business designated by the Secretary whose cash transactions have a high degree of usefulness in criminal, tax, or regulatory matters." 31 U.S.C. 5312(a)(2)(Z) and (Y). The Secretary has, thus far, not chosen to exercise this power broadly. The new law provides even more comprehensive authority but does not require reports until regulations are issued.

Section 366. Efficient Use of Currency Transaction Report System

Section 366 requires the Secretary to study expanding the statutory exemption system to the currency transaction reporting requirements , under 31 U.S.C. 5313, authorizing exemptions for transactions with various entities and qualified business customers from the domestic currency and coin reporting requirements. The study is to address methods for improving financial institutions' use of these exemptions to reduce the submission of reports with little or no value for law enforcement purposes. A report on this is required within one year.

Subtitle C–Currency Crimes and Protection

Section 371. Bulk Cash Smuggling into or out of the United States

Section 371 creates a new criminal offense, knowingly concealing more than $10,000 and transporting it or attempting to transfer it out of or into the United States. Conviction under the statute is subject to imprisonment for up to 5 years and forfeiture of any property involved in the offense. Preexisting law, 31 U.S.C. 5316, requires a report by anyone transporting monetary instruments, defined to

[3326] There appears to be a typographical error in the text of the legislation. The prohibition on structuring refers to 31 U.S.C. 5333, rather than to 5331.

include currency, of more than $10,000 into or out of the U.S. In United States v. Bajakajian, 524 U.S. 324 (1998), the Supreme Court ruled it unconstitutional to require forfeiture of $357,144, in cash that the defendant possessed legitimately and was attempting to carry with him when leaving the United States. The Court found the penalty disproportional to the gravity of the offense and a violation of the Excessive Fines Clause of the Eighth Amendment to the U. S. Constitution. In reaching that decision, the Court considered the fact that the offense was merely a reporting offense since it was not illegal to transport the currency.

Section 372. Forfeiture in Currency Reporting Cases

Section 372 authorizes criminal forfeiture and civil forfeitures for violations of the reporting requirements relating to monetary instruments and makes the criminal forfeiture procedures of section 413 of the Controlled Substances Act and the civil forfeiture procedures of 18 U.S.C. 981(a)(1)(A) (money laundering) applicable to criminal and civil forfeiture, respectively, under 31 U.S.C. 5313 (reports on domestic coins and currency), 5316 (reports on exporting monetary instruments), and 5324 (structuring transactions to evade reporting requirements). Pre-existing law authorized forfeiture of any property involved in the transaction in violation of 31 U.S.C. 5324(b) (international monetary instruments) or property traceable to such property under customs procedures, as held by the court in United States v. Twenty Thousand Seven Hundred Fifty-Seven Dollars and Eight-Three Cents ($20,757.83) Canadian Currency, 769 F. 2d 479 (8th Cir. 1985).

Section 373. Illegal Money Transmitting Businesses

Section. 373 prohibits anyone from knowingly conducting, controlling, managing, supervising, directing, or owning a money transmitting business: (1) without a license in a state that requires such a license and subjects operating without a licence to state misdemeanor or felony penalties; (2) not registered with Treasury under 31 U.S.C. 5330; or (3) involves the transportation or transmission of funds that the defendants knows to have been derived from a criminal offense or are intended to be used to promote or support unlawful activity. The section prescribes a federal penalty of up to five years' imprisonment and criminal fines and authorizes civil forfeiture of property involved in transactions in connection with this offense.

Under the Money Laundering Suppression Act of 1994, 31 U.S.C. 5330(a), the Secretary of the Treasury is required to establish a system to register money transmitting businesses. FinCEN's regulations require registration by December 31, 2001. 31 C.F.R. §103.41.

Section 374. Counterfeiting Domestic Currency and Obligations

Section 374 extends the definition of counterfeiting obligations of the United States to cover analog, digital, or electronic images, as well as "any plate, stone, or

other thing or part thereof, used to counterfeit" such obligations or securities, as provided in pre-existing law, 18 U.S.C. 470(2). This section is also amended to provide similar penalties for offenses committed outside the U.S. as are applicable to those within the U.S. Other provisions increase the penalties under other counterfeiting statutes to 20 years' imprisonment: 18 U.S.C. 471 (obligations or securities of the U.S.); 472 (uttering counterfeit obligations or securities); 473 (dealing in counterfeit obligations or securities); and, 474 (using plates or stones for counterfeiting).

The section amends 18 U.S.C. 474 to cover counterfeiting involving an analog, digital or electronic image of U.S. obligations, unless authorized by Treasury. It amends 18 U.S.C. 476 (taking impressions of tools used for obligations or securities of the U.S.) to increase the penalty from 10 years to 25 years' imprisonment. It amends 18 U.S.C. 477 (possessing or selling impressions of tools used for obligations or securities) to cover an analog, digital, or electronic image. It raises the penalty for connecting parts of different notes, 18 U.S.C. 484, from five years' to ten years' imprisonment, and for offenses under 18 U.S.C. 493 (bonds and obligations of certain lending agencies), from five to ten years' imprisonment.

Section 375. Counterfeiting Foreign Currency and Obligations

Section 375 increases the penalties for violations of various offenses involving foreign currency and obligations as follows: 18 U.S.C. 478 (foreign obligations or securities, penalty raised from five to 20 years); 18 U.S.C. 479 (uttering counterfeit foreign obligations, penalty raised from three to 20 years); 18 U.S.C. 480 (possessing counter foreign obligations or securities, penalty raised from one to 20 years); 18 U.S.C. 481 (plates or stones for counterfeiting foreign obligations or securities, penalty raised from five to 20 years); 18 U.S.C. 482 (foreign bank notes, penalty raised from two to twenty years); and 18 U.S.C. 483 (foreign bank notes, penalty raised from two to 20 years). The section also criminalizes counterfeiting involving an analog, digital, or electronic image of foreign obligations and securities. It adds 18 U.S.C. 2339B, providing material support to designated foreign terrorist organizations as a predicate for a money laundering prosecution under 18 U.S.C. 1956.

Section 377. Extraterritorial Jurisdiction

Section 377 enhances the applicability of 18 U.S.C. 1029 (computer fraud) by covering offenses committed outside the U.S. that involve an access device issued by a U.S. entity, such as a credit card, provided the defendant transports, delivers, conveys, transfers to or through, or otherwise stores, secrets, or holds within the jurisdiction of the U.S., any article used to assist in the commission of the offense or the proceeds of such offense or property derived therefrom.

Title IV – Protecting the Border
Subtitle A – Protecting the Northern Border

Section 401. Ensuring Adequate Personnel on the Northern Border

Annual appropriation legislation ordinarily authorizes the number of work years ("full time equivalents") that an agency may devote to a particular mission. Section 401 authorizes the Attorney General to waive the limitation applicable to Immigration and Naturalization Service (INS) personnel assigned to the Northern Border.

Section 402. Northern Border Personnel

Section 402 authorizes appropriations in the amounts necessary to triple the number of Border Patrol, Custom Service, and the Immigration and Naturalization Service (INS) personnel in each state along the Northern Border of the United States. It authorizes appropriations of an additional $50 million each for INS and the Customs Service to improve and supplement their monitoring equipment at the Northern Border.

Section 403. Access by the Department of State and the INS to Certain Identifying Information in the Criminal History Records of Visa Applicants and Applicants for Admission to the United States

Section 403 authorizes the appropriations necessary to provide the State Department and INS with access to the Federal Bureau of Investigation's automated National Criminal Information Files and to permit the National Institute of Standards and Technology to development the standards necessary to accommodate the transfer of information. All United States consular officers responsible for issuing visas, border inspection officers, and law enforcement and intelligence officers with alien investigation and identification responsibilities will use access to ensure that applicants for entry into the United States have no criminal record here. The FBI will provide access without charge except, at least initially, for fingerprint processing. The Secretary of State will promulgate regulations to ensure the confidentiality and appropriate use of the FBI information. The Attorney General and Secretary of State, in consultation with the Secretary of the Treasury, must report within 18 months of enactment and every two years thereafter on development, implementation, efficacy and privacy implications of the process. Sections 405 and 1008, discussed below, call for studies and reports to Congress on the feasibility of related enhancements in the systems to which this section gives access.

Section 404. Limited Authority to Pay Overtime

In more normal times, Justice Department appropriations legislation placed a $30,000 cap on the amount of overtime that could paid individual INS officers. In light of the extraordinary circumstances at the end of the last fiscal year,

section 404 repeals the limitation contained in the INS appropriation for border services for fiscal year 2001, 114 Stat. 2762-58 to 2762A-59 (2000).

Section 405. Report on the Integrated Automated Fingerprint Identification System for Ports of Entry and Overseas Consular Posts

Section 405 directs the Attorney General, after consultation with the Secretaries of State, the Treasury, and Transportation, as well as other appropriate agency heads, to study and report upon the feasibility of enhancing the FBI's Integrated Automated Fingerprint Identification System (IAFIS) and other identification systems in order to better screen applications seeking to enter this country. The section authorizes appropriations of $2 million to the purpose.

Subtitle B – Enhanced Immigration Provisions

Section 411. Definitions Relating to Terrorism

Foreign nationals (aliens) are deportable from the United States if they were inadmissible at the time they entered the country or if they have subsequently engaged in terrorist activity, 8 U.S.C. 1227(a)(1)(A),(a)(4)(B), 1182(a)(3)(B)(iv). Aliens may be inadmissible for any number of terrorism-related reasons, 8 U.S.C. 1182(a)(3)(B). Section 411 adds to the terrorism-related grounds upon which an alien may be denied admission into the United States.

Prior law recognized five categories of terrorism-related factors which rendered an alien inadmissible. Section 411 redefines two of these, engaging in terrorist activity and representing a terrorist organization, 8 U.S.C. 1182(a)(3)(B)(iv), (a)(3)(B)(i)(IV), and it adds three more, espousing terrorist activity, being the spouse or child of an inadmissible alien, associating with a terrorist organization and intending to engage in activities that could endanger the welfare, safety or security of the United States, 8 U.S.C. 1182(a)(3)(B)(i)(VI), (a)(3)(B)(i)(VII), 1182(a)(3)(F).

Earlier law defined engaging in terrorist activity, which is grounds for both inadmissibility and deportation, to encompass soliciting on behalf of a terrorist organization or providing material support to a terrorist organization, 8 U.S.C. 1182(a)(3)(B)(iii)(2000 ed.). It did not explain in so many words, however, what constituted a "terrorist organization," although it presumably at the very least included groups designated a terrorist organizations under section 219 of the Immigration and Nationality Act (8 U.S.C. 1189). Although only effective after designation, §411(c), section 411 defines "terrorist organization" to include not only organizations designated under section 219 but also organizations which the Secretary has identified in the Federal Register as having provided material support for, committed, incited, planned, or gathered information on potential targets of, terrorist acts of violence, 8 U.S.C. 1182(a)(3)(B)(vi), (a)(3)(B)(iv). It then recasts the definition of engaging in terrorist activities to include solicitation on behalf of such organizations, or recruiting on their behalf, or providing them with material support, 8 U.S.C. 1182(a)(3)(B)(iv). Nevertheless, section 411

permits the Secretary of State or Attorney General to conclude that the material support prohibition does not apply to particular aliens, 8 U.S.C. 1182(a)(3)(B)(vi).

Prior law made representatives of terrorist organizations designated by the Secretary under section 219 (8 U.S.C. 1189) inadmissible, 8 U.S.C. 1182(a)(3)(B)(i) (IV)(2000 ed.). And so they remain. Section 411 makes representatives of political, social or similar groups, whose public endorsements of terrorist activities undermines our efforts to reduce or eliminate terrorism, inadmissible as well, 8 U.S.C. 1882(a)(3) (B)(i)(IV).

An individual who uses his or her place of prominence to endorse, espouse, or advocate support for terrorist activities or terrorist organizations in a manner which the Secretary of State concludes undermines our efforts to reduce or eliminate terrorism becomes inadmissible under section 411, 8 U.S.C. 1182(a)(3)(B)(i)(VI).

The spouse or child of an alien, who is inadmissible on terrorist grounds for activity occurring within the last 5 years, is likewise inadmissible, unless the child or spouse was reasonably unaware of the disqualify conduct or has repudiated the disqualify conduct, 8 U.S.C. 1182(a)(3)(B)(i)(VII), 1182(a)(3)(B)(ii).

Finally, any alien, whom the Secretary of State or the Attorney General conclude has associated with a terrorist organization and intends to engage in conduct dangerous to the welfare, safety, security of the United States while in their country, is inadmissible, 8 U.S.C. 1182(a)(3)(F).

Section 219 of the Immigration and Nationality Act (8 U.S.C. 1189) permits the Secretary to designate as terrorist organizations any foreign group which he finds to have engaged in terrorist activities. A second subsection 411(c) permits him to designate groups which as subnational groups or clandestine agents, engage in "premeditated, politically motivated violence perpetrated against noncombatant targets," or groups which retain the capacity and intent to engage in terrorism or terrorist activity, 8 U.S.C. 1189(a)(1)(B).

Section 412. Mandatory Detention of Suspected Terrorists; Habeas Corpus; Judicial Review

Section 412 permits the Attorney General to detain alien terrorist suspects for up to seven days, 8 U.S.C. 1226a. He must certify that he has reasonable grounds to believe that the suspects either are engaged in conduct which threatens the national security of the United States or are inadmissible or deportable on grounds of terrorism, espionage, sabotage, or sedition. Within seven days, the Attorney General must initiate removal or criminal proceedings or release the alien. If the alien is held, the determination must be reexamined every six months to confirm that the alien's release would threaten national security or endanger some individual or the general public. The Attorney General's determinations are

subject to review only under writs of habeas corpus issued out of any federal district court but appealable only to the United States Court of Appeals for the District Columbia. The Attorney General must report to the Judiciary Committee on the details of the operation of section 412.

Uncertain is the relationship between section 412 and the President's Military Order of November 13, 2001, which allows the Secretary of Defense to detain designated alien terrorist suspects, within the United States or elsewhere, without express limitation or condition except with regard to food, water, shelter, clothing, medical treatment, religious exercise, and a proscription on invidious discrimination, 66 Fed.Reg. 57833, 57834 (Nov. 16, 2001).

Section 413. Multilateral Cooperation Against Terrorists

State Department records concerning its processing of visa applications are confidential and generally available only for court and law enforcement purposes, 8 U.S.C. 1202(f). Section 413 authorizes the Secretary of State to share the information with other countries in order to combat terrorism, drug trafficking, gun running, smuggling of immigrants, or other criminal activity, either on a case by case basis or pursuant to a general agreement.

Section 414. Visa Integrity and Security

The Illegal Immigration Reform and Immigrant Responsibility Act of 1996, 8 U.S.C. 1365a, instructed the Attorney General to implement an integrated entry and exit data system for airports, seaports and land border ports of entry. Section 414 expresses the sense of Congress that he should do so expeditiously and authorizes such appropriations as are necessary.

The section also directs the Attorney General and the Secretary of State to focus particularly on the use of biometric technology and tamper-resistant documents readable at ports of entry and to see to the development of a system that can be used by federal law enforcement officers to identify and detain individuals who pose a threat to U.S. national security.

Finally, it calls for the Office of Home Land Security to report to the Congress within a year of the enactment on the information needed for federal authorities to identify those seeking to enter the United States who are associated with terrorists organizations or otherwise pose a threat to our national security.

Section 415. Participation of Office of Homeland Security on Entry-Exit Task Force

Section 415 adds the Office of Home Land Security to the Integrated Entry and Exit Data System Task Force, 8 U.S.C. 1365a note.

Section 416. Foreign Student Monitoring Program

Section 417 authorizes appropriations of $36.8 million for the period ending on January 1, 2003 to implement and expand the program for collection of information relating to nonimmigrant foreign students and other exchange program participants, 8 U.S.C. 1372. The section adds air flight schools, language training schools, and vocations schools to the list of institutions whose students are to be included in the reporting requirement.

Section 417. Machine Readable Passports

Section 217 of the Immigration and Nationality Act permits a visa waiver program with respect to foreign tourists from countries which among things issue machine-readable passports that comply with international standards (or anticipate being able to do so prior to October 1, 2003), 8 U.S.C. 1187(c). Section 417 directs the Secretary of State to report the results of annual audits of the progress of program countries towards full implementation of machine-readable passport capability, of the existence of programs to prevent passport theft and counterfeiting, and of the development of tamper-proof passports. Subject to a progress waiver by the Secretary of State, the section limits the countries eligible for visa waiver program participation to those who have machine-readable passports as of October 1, 2003 (rather than October 1, 2007 as was previously the case).

Section 418. Prevention of Consulate Shopping

Section 418 commands the Secretary of State to determine whether consular shopping is a problem, to take steps to remedy any such problem, and to report to Congress on the action taken.

Subtitle C – Preservation of Immigration Benefits for Victims of Terrorism

The House Committee on the Judiciary explained a similar subtitle by noting that, "It is certain that some aliens fell victim to the terrorist attacks on the U.S. on September 11. This subtitle endeavors to modify immigration law to provide humanitarian relief to these victims and their family members," H.Rept. 107-236, at 66. Since the subtitle in the USA PATRIOT Act is largely unchanged from the subtitle reported out by the House Committee on the Judiciary, the analysis that follows is largely that of the Committee.

Section 421. Special Immigration Status

"The [USA PATRIOT] Act provides permanent resident status through the special immigrant program to an alien who was the beneficiary of a petition filed (on or before September 11) to grant the alien permanent residence as an employer-sponsored immigrant or of an application for labor certification (filed on or before September 11), if the petition or application was rendered null because of the disability of the beneficiary or loss of employment of the beneficiary due to physical damage to, or destruction of, the business of the petitioner or applicant

as a direct result of the terrorist attacks on September 11, or because of the death of the petitioner or applicant as a direct result of the terrorist attacks. Permanent residence would be granted to an alien who was the spouse or child of an alien who was the beneficiary of a petition filed on or before September 11 to grant the beneficiary permanent residence as a family-sponsored immigrant (as long as the spouse or child follows to join not later than September 11, 2003). Permanent residence would be granted to the beneficiary of a petition for a nonimmigrant visa as the spouse or the fiancé (and their children) of a U.S. citizen where the petitioning citizen died as a direct result of the terrorist attack. The section also provides permanent resident status to the grandparents of a child both of whose parents died as a result of the terrorist attacks, if either of such deceased parents was a citizen of the U.S. or a permanent resident," H.Rept. 107-236, at 66-7 (2001).

Section 422. Extension of Filing or Reentry Deadlines

"The Act provides that an alien who was legally in a nonimmigrant status and was disabled as a direct result of the terrorist attacks on September 11 (and his or her spouse and children) may remain lawfully in the U.S. (and receive work authorization) until the later of the date that his or her status normally terminates or September 11, 2002. Such status is also provided to the nonimmigrant spouse and children of an alien who died as a direct result of the terrorist attacks.

Where an alien was prevented from taking timely action because of office closures, airline schedule disruptions or other similar impediments, the "Act provides that an alien who was lawfully present as a nonimmigrant at the time of the terrorist attacks will be granted 60 additional days to file an application for extension or change of status if the alien was prevented from so filing as a direct result of the terrorist attacks. Also, an alien who was lawfully present as a nonimmigrant at the time of the attacks but was then unable to timely depart the U.S. as a direct result of the attacks will be considered to have departed legally if doing so before November 11. An alien who was in lawful nonimmigrant status at the time of the attacks (and his or her spouse and children) but not in the U.S. at that time and was then prevented from returning to the U.S. in order to file a timely application for an extension of status as a direct result of the terrorist attacks will be given 60 additional days to file an application and will have his or her status extended 60 days beyond the original due date of the application.

"Under current law, winners of the fiscal year 2001 diversity visa lottery must enter the U.S. or adjust status by September 30, 2001. The Act provides that such an alien may enter the U.S. or adjust status until April 1, 2002, if the alien was prevented from doing so by September 30, 2001 as a direct result of the terrorist attacks. If the visa quota for the 2001 diversity visa program has already been exceeded, the alien shall be counted under the 2002 program. Also, if a winner of the 2001 lottery died as a direct result of the terrorist attacks, the spouse and children of the alien shall still be eligible for permanent residence under the

program. The ceiling placed on the number of diversity immigrants shall not be exceeded in any case.

"Under the Act, in the case of an alien who was issued an immigrant visa that expires before December 31, 2001, if the alien was unable to timely enter the U.S. as a direct result of the terrorist attacks, the validity shall be extended until December 31.

"Under the Act, in the case of an alien who was granted parole that expired on or after September 11, if the alien was unable to enter the U.S. prior to the expiration date as a direct result of the terrorist attacks, the parole is extended an additional 90 days.

"Under the Act, in the case of an alien granted voluntary departure that expired between September 11 and October 11, 2001, voluntary departure is extended an additional 30 days," H.Rept. 107-236, at 67-8 (2001).

Section 423. Humanitarian Relief or Certain Surviving Spouses and Children

"Current law provides that an alien who was the spouse of a U.S. citizen for at least 2 years before the citizen died shall remain eligible for immigrant status as an immediate relative. This also applies to the children of the alien. The Act provides that if the citizen died as a direct result of the terrorist attacks, the 2 year requirement is waived.

"The Act provides that if an alien spouse, child, or unmarried adult son or daughter had been the beneficiary of an immigrant visa petition filed by a permanent resident who died as a direct result of the terrorist attacks, the alien will still be eligible for permanent residence. In addition, if an alien spouse, child, or unmarried adult son or daughter of a permanent resident who died as a direct result of the terrorist attacks was present in the U.S. on September 11 but had not yet been petitioned for permanent residence, the alien can self-petition for permanent residence.

"The Act provides that an alien spouse or child of an alien who 1) died as a direct result of the terrorist attacks and 2) was a permanent resident (petitioned-for by an employer) or an applicant for adjustment of status for an employment-based immigrant visa, may have his or her application for adjustment adjudicated despite the death (if the application was filed prior to the death)," H.Rept. 107-236, at 68 (2001).

Section 424. "Age-out" Protection for Children

"Under current law, certain visas are only available to an alien until the alien's 21st birthday. The Act provides that an alien whose 21st birthday occurs this September and who is a beneficiary for a petition or application filed on or before September 11 shall be considered to remain a child for 90 days after the alien's

21st birthday. For an alien whose 21st birthday occurs after this September, (and who had a petition for application filed on his or her behalf on or before September 11) the alien shall be considered to remain a child for 45 days after the alien's 21st birthday," H.Rept. 107-236, at 68 (2001).

Section 425. Temporary Administrative Relief

"The Act provides that temporary administrative relief may be provided to an alien who was lawfully present on September 10, was on that date the spouse, parent or child of someone who died or was disabled as a direct result of the terrorist attacks, and is not otherwise entitled to relief under any other provision of Subtitle [C]," H.Rept. 107-236, at 68 (2001).

Section 426. Evidence of Death, Disability, or Loss of Employment

"The Attorney General shall establish appropriate standards for evidence demonstrating that a death, disability, or loss of employment due to physical damage to, or destruction of, a business, occurred as a direct result of the terrorist attacks on September 11. The Attorney General is not required to promulgate regulations prior to implementing Subtitle [C]," H.Rept. 107-326, at 68-9 (2001).

Section 427. No Benefits to Terrorists or Family Members of Terrorists

"No benefit under Subtitle B shall be provided to anyone culpable for the terrorist attacks on September 11 or to any family member of such an individual," H.Rept. 107-236, at 69 (2001).

Section 428. Definitions

"The term 'specified terrorist activity' means any terrorist activity conducted against the Government or the people of the U.S. on September 11, 2001," H.Rept. 107-236, at 69 (2001).

Title V – Removing Obstacles to Investigating Terrorism

Section 501. Attorney General's Authority to Pay Rewards to Combat Terrorism

The Attorney General enjoys the power to pay rewards in criminal cases, but his power under other authorities is often subject to caps on the amount he might pay. Thus as a general rule, he may award amounts up to $25,000 for the capture of federal offenders, 18 U.S.C. 3059, and may pay rewards in any amount in recognition of assistance to the Department of Justices as long as the Appropriations and Judiciary Committees are notified of any rewards in excess of $100,000, 18 U.S.C. 3059B. Although he has special reward authority in terrorism cases, individual awards are capped at $500,000, (the ceiling for the total amount paid in such rewards is $5 million), and rewards of $100,000 or more require his personal approval or that of the President, 18 U.S.C. 3071-3077.

Over the last several years, annual appropriation acts have raised the $500,000 cap to $2 million and the $5 million ceiling to $10 million, e.g., Public Law 106-553, 114 Stat. 2762-67 (2000); Public Law 106-113, 113 Stat. 1501A-19 (1999); Public Law105-277, 112 Stat. 2681-66 (1998).

The USA PATRIOT Act supplies the Attorney General with the power to pay rewards to combat terrorism in any amount and without an aggregate limitation, but for rewards of $250,000 or more it insists on personal approval of the Attorney General or the President and on notification of the Appropriations and Judiciary Committees, §501. The funds to pay the rewards may come from any federal department or agency. In addition, the counterterrorism fund of section 101 can be used "without limitation" to pay rewards to prevent, investigate, or prosecute terrorism.

Section 502. Secretary of State's Authority to Pay Rewards

The Secretary of State's reward authority was already somewhat more generous than that of the Attorney General. He may pay rewards of up to $5 million for information in international terrorism cases as long as he personally approves payments in excess of $100,000, 22 U.S.C. 2708. The Act removes the $5 million cap and allows rewards to be paid for information concerning the whereabouts of terrorist leaders and facilitating the dissolution of terrorist organizations, §502.

Section 503. DNA Identification of Terrorists and Other Violent Offenders.

Federal law allows the Attorney General to collect DNA samples from federal prisoners convicted of a variety of violent crimes, 42 U.S.C. 14135a(d)(2). Section 503 expands the range. It permits samples to be taken from any federal prisoner convicted of a federal crime of terrorism (as defined in 18 U.S.C. 2332b(g)(5)(B)), or a crime of violence (as defined by 18 U.S.C. 16), or attempt or conspiracy to commit a crime of terrorism or violence.

Section 504. Coordination With Law Enforcement

Federal intelligence officers who wish to conduct electronic surveillance or physical searches under a FISA court order must certify that the acquisition of foreign intelligence information constitutes a significant purpose for the surveillance or search, 50 U.S.C. 1805(a)(7)(B), 1823(a)(7)(B). Section 504 confirms that the certification requirement does not preclude intelligence officers operating under FISA orders from coordinating their investigations with law enforcement officers in cases involving a foreign attack or other grave hostile attack, sabotage or international terrorism by a foreign power or agent, or foreign clandestine intelligence activities.

Section 505. Miscellaneous National Security Authorities

Three statutes, the Electronic Privacy Act, the Right to Financial Privacy Act, and Fair Credit Reporting Act, authorize third parties to release confidential communication transaction records, financial reports, and credit information for intelligence purposes upon the written request of senior FBI officials. Prior to section 505, the FBI was required to assert that the information sought was related to a foreign power, foreign agent, an international terrorist, or an individual engaged in clandestine intelligence activities, 18 U.S.C. 2709(b)(2), 12 U.S.C. 3414(a)(5), 15 U.S.C. 1681u. In an explanation that applies to all three statutory provisions, the House Committee on the Judiciary described the change made in the Electronic Privacy Act section: "Section 2709 of title 18 permits the Director of the Federal Bureau of Investigation to request, through a National Security Letter (NSL), subscriber information and toll billing records of a wire or electronic communication service provider. The request must certify (1) that the information sought is relevant to an authorized foreign counterintelligence investigation; and (2) there are specific and articulable facts that the person or entity to whom the information sought pertains is a foreign power or an agent of a foreign power as defined in FISA. This requirement is more burdensome than the corresponding criminal authorities, which require only a certification of relevance. The additional requirement of documentation of specific and articulable facts showing the person or entity is a foreign power or an agent of a foreign power cause substantial delays in counterintelligence and counterterrorism investigations. Such delays are unacceptable as our law enforcement and intelligence community works to thwart additional terrorist attacks that threaten the national security of the United States and her citizens' lives and livelihoods.

"Section [505] amends title 18 U.S.C. 2709 to mirror criminal subpoenas and allow a NSL to be issued when the FBI certifies, the information sought is 'relevant to an authorized foreign counterintelligence investigation,'" H.Rept. 107-236, at 61-2 (2001).

Section 506. Extension of Secret Service Jurisdiction

The federal computer fraud and abuse section, 18 U.S.C. 1030, originally vested the Secret Service with investigative jurisdiction over violations other than those dealing with classified information under 18 U.S.C. 1030(a)(1). The Secret Service also enjoyed investigative authority over offenses involving credit and debit card frauds as well as offenses involving false identification documents or devices, 18 U.S.C.3056(b)(3)(2000 ed.).

Section 506 preserves the Service's jurisdiction with respect to section 1030. It explicitly notes the FBI's investigative jurisdiction over offenses under paragraph 1030(a)(1) and the FBI's concurrent jurisdiction over offenses under the remainder of 18 U.S.C. 1030. The section amends paragraph 3056(b)(3) to enlarge the Service's jurisdiction from offenses involving "credit and debit card frauds, and false identification documents and devices" to crimes involving "access device fraud, false identification documents or devices, and any fraud or

other criminal or unlawful activity in or against any federally insured financial institution."

Section 507. Disclosure of Educational Records

Section 507 calls for an ex parte court order procedure under which senior Justice Department officials may seek authorization to collect educational records relevant to an investigation or prosecution of a crime of terrorism (as an exception to the confidentiality requirements of the General Education Provisions Act, 20 U.S.C. 1232g). Educational institutions who comply receive immunity from liability for the disclosure.

Section 508. Disclosure of Information From NCES Surveys

Section 508 creates a similar ex parte court order procedure under which senior Justice Department officials may seek authorization to collect individually identifiable information from the National Center for Education (as an exception to the confidentiality requirements of the National Education Statistics Act, 20 U.S.C. 9007). Officers and employees of the Center who cooperate receive immunity from liability for the disclosure.

Title VI – Providing for Victims of Terrorism, Public Safety Officers, and Their Families
Subtitle A – Aid to Families of Public Safety Officers

Section 611. Expedited Payment for Public Safety Officers Involved in the Prevention, Investigation, Rescue, or Recovery Efforts Related to a Terrorist Attack

Federal law authorizes benefits for those victimized by the death or catastrophic injury resulting in permanent and total disability of a public safety officer in the line of duty, subject to certain limitation, 42 U.S.C. 3796 et seq. Gross negligence, substantial contributory negligence, and employment other than in a civilian capacity are among the disqualifying factors, 42 U.S.C. 3796a, and there is a $5 million cap on benefits awarded in any fiscal year, 42 U.S.C. 3796. In cases of death or catastrophic injury sustained in the line of duty in relation to a terrorist attack, section 611 waives the cap and these disqualifications and orders the Bureau of Justice Assistance, which administers the program, to make payments within 30 days of receipt of a public agency's certification of eligibility in a particular case.

Section 612. Technical Correction With Respect to Expedited Payments for Heroic Public Safety Officers

Public Law 107-37, 115 Stat. 219 (2001), makes the same adjustments as those of section 611 for death and catastrophic injuries sustained in the line of duty in the course of rescue or recovery efforts related to the terrorist attacks of September 11. Section 612 confirms certain technical corrections made by the clerk and that

the Public Law extends to death and catastrophic injuries producing permanent and total disability.

Section 613. Public Safety Officers Benefit Program Payment Increases

Section 613 raises the amount of the benefit from $100,000 to $250,000, effective January 1, 2001, 42 U.S.C. 3796.

Section 614. Office of Justice Programs

Title I of the Omnibus Crime Control and Safe Streets Act (Pubic Law 90-351), as amended, creates the Office of Justice Programs (OJP) and a series of federal criminal justice and related assistance programs administered under its auspices, 42 U.S.C. 3711 et seq. In 1998, while Congress was considering reauthorization of some of those programs, it authorized the Office of Justice Programs to exercise authority over and approve grants, contracts and the like with respect to it's programs during fiscal year 1999, Public Law 105-277, 112 Stat. 2681-67 (1998). The following year, it renewed that authority for fiscal year 2000, but denied OJP authority to approve grants under the National Institute of Justice, the Bureau of Justice Statistics, and a few Juvenile Justice and Delinquency Prevention programs, Public Law 106-113, 113 Stat. 1501A-20 (1999). The fiscal year 2001 appropriations act carried forward by cross reference the same provisions with the same limitations, Public Law 106-553, 114 Stat. 2762A-67 (2000). Section 614 removes the limitations.

Subtitle B – Amendments to the Victims of Crime Act of 1984

Section 621. Crime Victims Fund

The Crime Victims Fund receives most of the fines collected for violations of federal criminal law and distributes them for purposes of victim assistance and compensation, 42 U.S.C. 10601-10604. Section 621 authorizes the Fund to receive gifts from private individuals. It instructs the Department of Justice, which administers the Fund, to distribute every fiscal year between 90 and 110% of the amount distributed in the previous year (120% in any year when the amount on hand is twice the amount distributed the previous year).

Pre-existing law allocated 48.5% of the amounts available under the Fund to crime victim compensation grants, 48.5% to crime victim assistance grants, and 3% to discretionary grants, 42 U.S.C. 10601(d)(4)(2000 ed.). Section 621 reduces the amounts available for compensation and assistance grants by 1% and increases to 5% the amount available for discretionary grants.

The section allows the Department of Justice to establish a $50 million antiterrorism emergency reserve for supplemental grants to compensate and assist victims of terrorism or mass violence. It also removes the otherwise

applicable caps on the amounts transferred to the Fund in response to the terrorist acts of September 11.

Section 622. Crime Victim Compensation

Before passage of section 622, individual victim compensation program grants were capped at 40% of the amount awarded in the previous year. Section 622 lifts the cap to 60% beginning in fiscal year 2003.

It also (1) removes the requirement that an eligible state crime victim compensation program provide compensation to state residents for terrorist crimes committed overseas, 42 U.S.C. 10602(b)(6)(B); (2) drops crimes involving terrorism from the definition of "compensable crimes," 42 U.S.C. 10602(d)(3); (3) provides that unlike other victim compensation, victim compensation received under Title IV of the Air Transportation Safety and System Stabilization Act (September 11 Victim Compensation Fund), Public Law 107-42, 115 Stat. 237, 49 U.S.C. 40101 note, may be considered income, a resource, or an asset for purposes of qualifying as an indigent for any federal or federal supported grant or benefit program, 42 U.S.C. 10602(c); (4) adds Title IV victim compensation to the "double dipping" restriction that applies to victim compensation programs, 42 U.S.C. 10602(e); and (5) allows the Virgin Islands to participate as a state in the victim compensation grant program, 42 U.S.C. 10602(d)(4).

Section 623. Crime Victim Assistance

Section 623 expands the crime victim assistance grant program to permit grants to federal agencies who perform local law enforcement functions in or on behalf of the District of Columbia, the Virgin Islands, or any other U.S. territory or possessions. It prohibits program discrimination against crime victims based on their disagreement with the manner in which the state is prosecuting the underlying offense, 42 U.S.C.10603(b)(1)(F); allows grants to be used for program evaluation and compliance efforts, 42 U.S.C. 10603(c)(1)(A); for fellowships, clinical internships, and training programs, 42 U.S.C. 10603(c)(3)(E). Finally, it reverses the preference for victim service grants over demonstration projects and training grants, so that not more than 50% of the amounts available for crime victim assistance grants shall be used for victim service grants and not less than 50% for demonstration projects and training grants, 42 U.S.C. 10603(c)(2).

Section 624. Victims of Terrorism

Title VIII of the Omnibus Diplomatic Security and Antiterrorism Act of 1986, Public Law 99-399, 100 Stat. 879 (1986), provides victims' benefits for the Iranian hostages, 5 U.S.C. 5569. The Antiterrorism and Effective Death Penalty Act, Public Law 104-132, 110 Stat. 1243, 42 U.S.C. 10603b, and the Victims of Trafficking and Violence Protection Act of 2000, Public Law 106-386, 114 Stat.

1545, 42 U.S.C. 10603c, establish compensation programs for victims of terrorism or mass destruction and victims of international terrorism respectively.

Prior to the enactment of section 624 only the states were eligible for compensation and assistance grants on behalf of the victims of terrorism or mass destruction occurring within the United States, and victims eligible for benefits under the diplomatic security law were ineligible for compensation and assistance under the general provisions covering victims of terrorism or mass destruction occurring abroad, 42 U.S.C. 10603b(2000 ed.). Section 624 removes the diplomatic security law disqualification and permits grants to victim service organizations – federal, state, local and nongovernmental agencies – to provide emergency victim relief, 42 U.S.C. 10603b.

Further, the section reduces the amount of compensation available to victims of international terrorism generally by any amount a victim has received under the diplomatic security law, 42 U.S.C. 10603c.

Title VII – Increased Information Sharing for Critical Infrastructure Protection

Section 701. Expansion of Regional Information Sharing Systems to Facilitate Federal-State-Local Law Enforcement Response Related to Terrorist Attacks

The Office of Justice Programs is authorized to make grants and enter into contracts with state and local law enforcement agencies and with nonprofit organizations to identify and combat multi-jurisdictional criminal conspiracies, 42 U.S.C. 3796h. Section 701 amends section 3796h to authorize appropriations of $50 million for fiscal year 2002 and $100 million for fiscal year 2003 to be used to establish and operate a secure information sharing system to combat multi-jurisdictional terrorist conspiracies and activities.

Title VIII – Strengthening the Criminal Laws Against Terrorism

Section 801. Terrorist Attacks and Other Acts of Violence Against Mass Transportation Systems

Pre-existing federal law criminalized, among other things, wrecking trains, 18 U.S.C. 1992; damaging commercial motor vehicles or their facilities, 18 U.S.C. 33, or threatening to do so, 18 U.S.C. 35; destroying vessels within the navigable waters of the United States, 18 U.S.C. 2273; destruction of vehicles or other property used in activities affecting interstate or foreign commerce by fire or explosives, 18 U.S.C. 844(i); possession of a biological agent or toxin as a weapon or a threat, attempt, or conspiracy to do so, 18 U.S.C. 175; use of a weapon of mass destruction affecting interstate or foreign commerce or a threat, attempt, or conspiracy to do so, 18 U.S.C. 2332a; commission of a federal crime of violence while armed with a firearm, or of federal felony while in possession an explosive,

18 U.S.C. 924(c), 844(h); and conspiracy to commit a federal crime, 18 U.S.C. 371.

Section 801 fills in some of the gaps in these proscriptions. It makes terrorist attacks and other acts of violence against mass transportation systems federal crimes, punishable by imprisonment for any term of years or life if the conveyance is occupied at the time of the offense, and imprisonment for not more than twenty years in other cases. Under its provisions, it is a crime to willfully

- wreck, derail, burn, or disable mass transit;
- place a biological agent or destructive device on mass transit recklessly or with the intent to endanger;
- -burn or place a biological agent or destructive device in or near a mass transit facility knowing a conveyance is likely to be disabled;
- impair a mass transit signal system;
- -interfere with a mass transit dispatcher, operator, or maintenance personnel in the performance of their duties recklessly or with the intent to endanger;
- -act with the intent to kill or seriously injure someone on mass transit property;
- convey a false alarm concerning violations of the section;
- attempt to violate the section;
- threaten or conspire to violate the section

when the violation involves interstate travel, communication, or transportation of materials or that involves a carrier engaged in or affecting interstate or foreign commerce, 18 U.S.C. 1993.

Section 802. Definition of Domestic Terrorism

Section 802 adjusts the definition of international terrorism in 18 U.S.C. 2331 and borrows from it to define domestic terrorism. Section 2331 has for some time defined international terrorism as those criminal acts of violence, committed primarily overseas or internationally, that appear to be intended to intimidate or coerce a civilian population, or to influence a governmental policy by intimidation or coercion, or to affect the conduct of a government by assassination or kidnaping, 18 U.S.C. 2331(1). Section 802 simply modifies this last element to include acts that appear to be intended to affect the conduct of a government by mass destruction, assassination or kidnaping.

It defines domestic terrorism as those criminal acts dangerous to human life, committed primarily within the United States, that appear to be intended to intimidate or coerce a civilian population, or to influence a governmental policy by intimidation or coercion, or to affect the conduct of a government by mass destruction, assassination or kidnaping, 18 U.S.C. 2331(5).

Section 803. Prohibition Against Harboring Terrorists

It is a federal crime to harbor aliens, 8 U.S.C. 1324, or those engaged in espionage, 18 U.S.C. 792, or to commit misprision of a felony (which may take the form of harboring the felon), 18 U.S.C. 4, or to act as an accessory after the fact to a federal crime (including by harboring the offender), 18 U.S.C. 3. The Justice Department asked that a terrorist harboring offense be added to the espionage section, and that it be given extraterritorial effect and venue flexibility.

Section 803 instead establishes a separate offense which punishes harboring terrorists by imprisonment for not more than ten years and/or a fine of not more than $250,000, 18 U.S.C. 2339. The predicate offense list consists of:

- destruction of aircraft or their facilities, 18 U.S.C. 32;
- biological weapons offenses, 18 U.S.C. 175;
- chemical weapons offenses, 18 U.S.C. 229; ! nuclear weapons offenses, 18 U.S.C. 831;
- bombing federal buildings, 18 U.S.C. 844(f);
- destruction of an energy facility, 18 U.S.C. 1366;
- violence committed against maritime navigational facilities, 18 U.S.C. 2280;
- offenses involving weapons of mass destruction, 18 U.S.C. 2232a;
- international terrorism, 18 U.S.C. 2232b;
- sabotage of a nuclear facility, 42 U.S.C. 2284;
- air piracy, 49 U.S.C. 46502.

It permits prosecution either at the place the harboring occurred or where the underlying act of terrorism committed by the sheltered terrorist might be prosecuted. In order to enjoy the full benefits of section 803, the prosecution may have to establish a nexus between the act of terrorism and the site of concealment, U.S. Const. Art. III, §2, cl.3; Amend. IV; United States v. Cabrales, 524 U.S. 1 (1998). On the other hand, if the acts of terrorism occur in the United States or over which the United States has jurisdiction, the crime of harboring the terrorist even overseas can be prosecuted in the United States in all likelihood without amending existing law, cf., United States v. Felix-Gutierrez, 940 F.2d 1200, 1205 (9th Cir. 1991)("crime of accessory after the fact gives rise to extraterritorial jurisdiction to the same extent as the underlying offense").

Section 804. Jurisdiction Over Crimes Committed at U.S. Facilities Abroad

Crime is usually outlawed, prosecuted and punished where it is committed. In the case of the United States, this a matter of practical and diplomatic preference rather than constitutional necessity. Consequently, a surprising number of federal criminal laws have extraterritorial application. In some instances, the statute proscribing the misconduct expressly permits the exercise of extraterritorial jurisdiction, e.g., 18 U.S.C. 2332a (relating to use of weapons of mass destruction by an American overseas). In others, such as those banning

assassination of Members of Congress, 18 U.S.C. 351, or the attempted murder of federal law enforcement officers, 18 U.S.C. 1114, the court will assume Congress intended the prohibitions to have extraterritorial reach.[3327]

Section 804 touches upon extraterritoriality only to a limited extent and in somewhat unusual manner. The special maritime and territorial jurisdiction of the United States represent two variations of the extraterritorial jurisdiction. Congress has made most common law crimes – murder, sexual abuse, kidnaping, assault, robbery, theft and the like – federal crimes when committed within the special maritime and territorial jurisdiction of the United States.

The special maritime jurisdiction of the United States extends to the vessels of the United States. Historically, the territorial jurisdiction of the United States was thought to reach those areas over which Congress enjoyed state-like legislative jurisdiction. For some time, those territories were located exclusively within the confines of the United States, but over the years came to include at least temporarily, Hawaii, the Philippines, and other American overseas territories and possessions. Recently, the lower federal courts have become divided over the question of whether laws enacted to apply within federal enclaves within the United States and American territories overseas might also apply to areas overseas over which the United States has proprietary control, compare, United States v. Gatlin, 216 F.3d 207 (2d Cir. 2000); United States v. Laden, 92 F.Supp.2d 189 (S.D.N.Y. 2000); with, United States v. Corey, 232 F.3d 1166 (9th Cir. 2000); United States v. Erdos, 474 F.2d 157 (4th Cir. 1973). The section resolves the conflict by declaring within the territorial jurisdiction of the United States includes those overseas areas used by American governmental entities for their activities or residences for their personnel, at least to the extent that crimes are committed by or against an American. It is intended as a residual provision and therefore does not apply where it would conflict with a treaty obligation or where the offender is covered by the Military Extraterritorial Jurisdiction Act (18 U.S.C. 3261).

Section 805. Material Support of Terrorism

Sections 2339A and 2339B of title 18 of the United States Code ban providing material support to individuals and to organizations that commit various crimes of terrorism. Section 804 amends the sections in several ways, some at the behest of the Justice Department. Section 2339B (support of a terrorist organization) joins section 2339A (support of a terrorist) as a money laundering predicate offense, 18 U.S.C. 1956(c)(7)(D) The predicate offense list of 18 U.S.C. 2339A (support to terrorists) grows to include:

[3327] United Stats v. Layton, 855 F.2d 1388 (9th Cir. 1981); United States v. Benitez, 741 F.2d 1312 (11th Cir. 1984) United States v. Bowman, 260 U.S. 94 (1922); Ford v. United States, 273 U.S. 593 (1927).

- chemical weapons offenses, 18 U.S.C. 229;
- terrorist attacks on mass transportation, 18 U.S.C. 1993 ;
- sabotage of a nuclear facility, 42 U.S.C. 2284; and
- sabotage of interstate pipelines, 49 U.S.C. 60123(b).

Section 805 also adds expert advice or assistance of the types of assistance that may not be provided under section 2339A. Prosecutions grounded on providing material assistance in the form of expert advice may encounter the same First Amendment vagueness problems some courts have found in assistance which takes the form of "training"and "personnel," Humanitarian Law Project v. Reno, 205 F.3d 1130, 1137-136 (9th Cir. 2000).

Finally, the section declares that a prosecution for violation of section 2339A (support of terrorists) may be brought where the support is provided or where the predicate act of terrorism occurs. The full benefit of this amendment may have to await clarification in the law concerning venue, U.S.Const. Art.III, §2, cl.3; Amend. IV; United States v. Cabrales, 524 U.S. 1 (1998).

Section 806. Assets of Foreign Terrorist Organizations

Modern forfeiture law strips criminals of the proceeds and instruments of crime. Terrorism, however, neither produces profits of drug dealing nor requires the specialized equipment of the rum runner or the counterfeiter. Consequently, most forfeiture statutes do not reach the crimes of terrorism. Nevertheless terrorism, particularly international terrorism, requires financing; cash is the essential instrumentality of terrorism. The USA PATRIOT Act attacks terrorism at its most vulnerable spot, its need for financial support. The Act's invigorating of the International Economic Emergency Powers Act asset forfeiture and its money laundering measures are calculated to encumber and prevent terrorism by drying up its sources of financial support.

Section 806 supplies another tool for that effort. It subjects to civil forfeiture property wherever located: (1) which belongs to an individual or entity planning or engaging in domestic or international terrorism against the United States (as defined in 18 U.S.C. 2331) or which affords the individual a source of influence over a terrorist organization; (2) which is acquired or maintained for use in furtherance of acts of domestic or international terrorism committed against Americans; or (3) which is derived from or is useful for the commission of acts of domestic or international terrorism committed against the Americans, 18 U.S.C. 981(a)(1)(G). The section is something of a rarity in that it creates a forfeiture of estate (confiscation based solely on the property's relation to an offender rather than to the offense; discussed earlier with respect to section 106), traditionally thought to be at odds with the concept of civil in rem forfeiture and with the bans on corruption of the blood, U.S.Const. Art.III, §3, cl.2; Amend.V; United States v. Grande, 620 F.2d 1026 (4th Cir. 1980).

Section 807. Technical Clarification Relating to Provision of Material Support to Terrorism

The Trade Sanctions Reform and Export Enhancement Act of 2000, Title IX of Public Law 106-387, 114 Stat. 1549A-69, limits the power of the President to unilaterally impose export restrictions on agricultural and medical products, subject to certain exceptions. Section 807 builds on the pronouncement of section 221(b)(2) to confirm that the trade sanctions bill should not be construed to limit or otherwise amend the prohibitions on providing material support to terrorist or terrorist organizations found in 18 U.S.C. 2339A and 2339B.

Section 808. Definition of Federal Crime of Terrorism

Paragraph 2332b(g)(5)(b) lists a number of violent federal crimes within its definition of "federal crime[s] of terrorism" for purposes of the section's prohibition on acts of terrorism transcending national boundaries. Section 808 amends the definition for consistency with its use in various other sections of the USA PATRIOT Act. The Section drops a number of less serious crimes from the definition, such as simple assault (18 U.S.C. 351(e)), bomb scares (18 U.S.C. 844(e)), and malicious mischief (18 U.S.C. 1361), after reaffirming that the omitted offenses remain within the investigative jurisdiction of the Department of Justice. It places several more serious crimes within the definition, crimes like biological weapons offenses (18 U.S.C. 175b), cybercrime (18 U.S.C. 1030), terrorists attacks on mass transit (18 U.S.C. 1993), and various violent crimes committed aboard aircraft within U.S. jurisdiction (49 U.S.C. 46504, 46505(b)(3),(c), 46505).

Section 809. No Statute of Limitations for Certain Terrorism Offenses

Prosecution for murder may be initiated at any time; there is no statute of limitations, 18 U.S.C. 3281. With a few exceptions, there is a five year statute of limitations on the prosecution of other federal crimes. Among the relevant exceptions before the USA PATRIOT Act was enacted, were an eight year statute of limitations for several terrorist offenses, 18 U.S.C. 3286,[3328] and a ten year statute of limitations for arson in federal enclaves and explosives offenses involving federal property, property used in an activity affecting interstate

[3328] 18 U.S.C. 32 (destruction of aircraft or aircraft facilities), 37 (violence at international airports), 112 (assaults on foreign dignitaries), 351 (crimes of violence against Members of Congress), 1116 (killing foreign dignitaries), 1203 (hostage taking), 1361 (destruction of federal property), 1751 (crimes of violence against the President), 2280 (violence against maritime navigation), 2281 (violence on maritime platforms), 2332 (terrorist violence against Americans overseas), 2332a (use of weapons of mass destruction), 2332b (acts of terrorism transcending national boundaries), 2340A (torture); 49 U.S.C. 46502 (air piracy), 46504 (interference with a flight crew), 46505 (carrying a weapon aboard an aircraft), and 46506 (assault, theft, robbery, sexual abuse, murder, manslaughter or attempted murder or manslaughter in the special aircraft jurisdiction of the United States).

commerce, and use of an explosive during the commission of a federal offense, 18 U.S.C. 3295. The Administration recommended the elimination of a statute of limitations in terrorism cases.

Section 809 takes a less dramatic approach. It eliminates the statute of limitations for any federal crime of terrorism (as defined by 18 U.S.C. 2332b(g)(5)(B), with the amendments of §808) that risks or results in a death or serious bodily injury, 18 U.S.C. 3286. In the absence of such a risk or result, all other terrorism offenses become subject to the eight year statute of limitations unless already covered by the ten year statute for explosives and arson offenses, 18 U.S.C. 3286 (§809).

Section 810. Alternative Maximum Penalties for Terrorism Offenses

The Justice Department suggested an alternative term of imprisonment up to life imprisonment for anyone convicted of an offense designated a terrorist crime. It described the proposal as analogous to standard fine provisions of 18 U.S.C. 3571(b),(c), which in 1984 established a basic fine of $250,000 for any individual who committed a federal felony, notwithstanding the lower maximum fine described in the statute that outlawed the offense.

The proposal, however, failed to identify the critical elements that would trigger the alternative. Both practical and constitutional challenges might be thought to attend this failure to distinguish between those convicted of some "garden variety" crime of terrorism and the more serious offender meriting the alternative, supplementary penalty. Section 810 instead opts to simply increase the maximum penalties for various crimes of terrorism, particularly those which involve the taking of a human life and are not already capital offenses. It increases the maximum terms of imprisonment:

- for life-threatening arson or arson of a dwelling committed within a federal enclave, from 20 years to any term of years or life, 18 U.S.C. 81;
- for causing more than $100,000 in damage to, or significantly impairing the operation of an energy facility, from 10 to 20 years (or any term of years or life, if death results), 18 U.S.C. 1366;
- for providing material support to a terrorist or a terrorist organization, from 10 to 15 years (or any term of years or life, if death results), 18 U.S.C. 2339A, 2339B;
- for destruction of national defense materials, from 10 to 20 years (or any term of years or life, if death results), 18 U.S.C. 2155;
- for sabotage of a nuclear facility, from 10 to 20 years (or any term of years or life, if death results), 42 U.S.C. 2284;
- for carrying a weapon or explosive aboard an aircraft within U.S. special aircraft jurisdiction, from 15 to 20 years (or any term of years or life, if death results), 49 U.S.C. 46505; and
- for sabotage of interstate gas pipeline facilities, from 15 to 20 years (or any term of years or life, if death results), 49 U.S.C. 60123.

Section 811. Penalties for Terrorist Conspiracies

It is a separate federal offense punishable by imprisonment for not more than five years to conspire to commit any federal felony, 18 U.S.C. 371. Coconspirators are likewise subject to punishment for the underlying offense and for any other crimes committed in furtherance of the conspiracy. Nevertheless, some federal criminal statutes impose the same penalties for both the crimes they proscribe and for conspiracy to commit. Again, section 811, opts for a less sweeping approach than the Administration had proposed. It establishes equivalent sanctions for conspiracy and the underlying offense in cases of:

- arson committed within a federal enclave, 18 U.S.C. 81;
- killing committed while armed with a firearm in a federal building, 18
- U.S.C. 930(c);
- destruction of communications facilities, 18 U.S.C. 1362;
- destruction of property within a federal enclave, 18 U.S.C. 1363;
- causing a train wreck, 18 U.S.C. 1922;
- providing material support to a terrorist, 18 U.S.C. 2339A;
- torture committed overseas under color of law, 18 U.S.C. 2340A;
- sabotage of a nuclear facility, 42 U.S.C. 2284;
- interfering with a flight crew within U.S. special aircraft jurisdiction, 49 U.S.C. 46504;
- carrying a weapon or explosive abroad an aircraft with U.S. special aircraft jurisdiction, 49 U.S.C. 46505; and
- sabotage of interstate gas pipeline facilities, 49 U.S.C. 60123.

Section 812. Post-Release Supervision of Terrorists

When federal courts impose a sentence of a year or more upon a convicted defendant, they must also impose a term of supervised release, 18 U.S.C. 3583; U.S.S.G. §5D1.1. Supervised release is not unlike parole, except that it is ordinarily imposed in addition to rather than in lieu of a term, or portion of a term, of imprisonment. The term may be no longer than 5 years for most crimes and violations of the conditions of release may result in imprisonment for up to an additional 5 years, 18 U.S.C. 3583(e). There were proposals to create a maximum supervisory term of life for those convicted of acts of terrorism (subject to the calibrations of the Sentencing Commission). Section 812 amends section 3583 to provide for a supervisory release term of life or any term of years following conviction for a federal crime of terrorism as defined in 18 U.S.C. 2332b which resulted in death or involved a foreseeable risk of death or serious bodily injury, 18 U.S.C. 3583(j).

Section 813. Inclusion of Acts of Terrorism as Racketeering Activity

Section 813 accepts the Administration's recommendation that all federal crimes of terrorism be included on the predicate offense list for RICO (racketeer

influenced and corrupt organizations) which proscribes acquiring or operating, through the patterned commission of any of a series of predicate offenses, an enterprise whose activities affect interstate or foreign commerce, 18 U.S.C. 1961.

Section 814. Deterrence and Prevention of Cyberterrorism

Computer fraud and abuse is a federal crime when it involves a federally protected computer, i.e., a federal computer, a computer used by financial institutions, or a computer used in interstate or foreign commerce, 18 U.S.C. 1030. Section 814 increases the penalty for intentionally damaging a protected computer from imprisonment for not more than 5 years to imprisonment for not more than 10 years. It also raises the penalty for either intentionally or recklessly damaging a protected computer after having previously been convicted of computer abuse from imprisonment for not more than 10 years to imprisonment for not more than 20 years.

In order to trigger criminal or civil liability for causing damage to a federally protected computer, the damage must fall into one of several categories. It must involve losses of $5000 or more, or adversely affect certain medical data, or cause a physical injury, or threaten public health or safety. Section 814 supplies a fifth category – damage affecting a computer system used by or for the government for the administration of justice, national defense, or national security.

Section 814 supplies an explicit definition for the kinds of losses that may be considered in order to determine whether the $5000 threshold has been met. They consist of any reasonable cost including but not limited to those incurred to take corrective action, make damage assessments, and effect recuperation, as well as the consequential costs of interrupted service.

Section 815. Additional Defense to Civil Actions Relating to Preserving Records in Response to Government Requests

Section 2707(e) of title 18 of the United States Code affords communications service providers with a good faith defense to civil or criminal liability for their cooperation in response to a warrant, subpoena or court order. Section 2703(f) requires them to return over records and other evidence at government request. Section 815 extends the good faith defense of section 2707(e) to cover civil and criminal liability for service provider cooperation with a request under section 2703(f).

Section 816. Development and Support of Cybersecurity Forensic Capabilities

Section 816 authorizes annual appropriations of $50 million to establish regional computer forensic laboratories.

Section 817. Expansion of the Biological Weapons Statute

Prior to enactment of the USA PATRIOT Act, federal law proscribed the use of biological agents or toxins as weapons, 18 U.S.C. 175. Section 817 supplements existing law with two federal crimes. First, it outlaws possession of a type or quantity of biological agents or toxins that cannot be justified for peaceful purposes, 18 U.S.C. 175(b). Second, consistent with federal prohibitions on the possession of firearms, 18 U.S.C. 922(g), and explosives, 18 U.S.C. 842(i), it makes it a federal offense for certain individuals – convicted felons, illegal aliens, and fugitives and the like – to possess biological toxins or agents, 18 U.S.C. 175b. Both offenses are punishable by imprisonment for not more than ten years and/or a fine of not more than $250,000.

Title IX – Improved Intelligence

Section 901. Responsibilities of Director of Central Intelligence Regarding Foreign Intelligence Collected Under Foreign Intelligence Surveillance Act of 1978

Only the President or the Attorney General may authorize application for a FISA surveillance or physical search order, 50 U.S.C. 1802, 1804, 1822, 1823. Information acquired by means of a FISA order may be shared with other federal officials, including members of the intelligence community, as long as minimization procedures are observed, 50 U.S.C. 1806, 1825. FISA minimization procedures are crafted "consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information," 50 U.S.C. 1801(h), 1821(4).

Section 901 amends the National Security Act of 1947, 50 U.S.C. 403-3(c), instructing the Director of the Central Intelligence[3329] to establish priorities and requirements concerning the use of the Foreign Intelligence Surveillance Act (FISA) and to assist the Attorney General to ensure that information generated by the execution of FISA surveillance and physical search orders is disseminated so as to be used efficiently and effectively for foreign intelligence purposes. The intelligence community, however, must work through the good offices of the Attorney General to use FISA orders in the performance of its responsibilities, since in the absence of specific statutory or executive order authority, the Director is not permitted to direct, manage, or undertake execution of a FISA order.

Section 902. Inclusion of International Terrorist Activities Within the Scope of Foreign Intelligence Under the National Security Act of 1947

[3329] The Director of Central Intelligence is simultaneously Director of the Central Intelligence Agency (CIA), the President's principal advisor on national security intelligence matters, and coordinating head of the intelligence community, 50 U.S.C. 403(a).

Section 3 of the National Security Act defines the kind of information that constitutes "foreign intelligence" for purposes of the Act, 50 U.S.C. 5401a(2). Section 902 adds information relating to the activities of international terrorists to the definition.

Section 903. Sense of Congress on the Establishment and Maintenance of Intelligence Relationships to Acquire Information on Terrorists and Terrorist Organizations

Section 903 expresses the sense of Congress that members of the intelligence community should be outgoing in their efforts to acquire information about terrorists and terrorist organizations.

Section 904. Temporary Authority to Defer Submittal to Congress of Reports on Intelligence and Intelligence-Related Matters

Section 904 permits intelligence community agencies to defer submission of required intelligence reports to Congress (other than the reports on covert actions required under 50 U.S.C. 413a, 413b) until February 1, 2002. They may delay submission further, if compliance would impede counterintelligence activities.

Section 905. Disclosure to Director of Central Intelligence of Foreign Intelligence-Related Information With Respect to Criminal Investigations

The Attorney General in consultation with the Director of Central Intelligence has been directed in section 905 to develop guidelines to ensure the dissemination to the intelligence community of foreign intelligence information unearthed during the course of a criminal investigation. The guidelines may embody exceptions necessary to prevent jeopardizing an ongoing criminal investigation or other significant law enforcement interests. They should contain a means for reporting back to the intelligence community on the action taken or to be taken on the basis of information which elements of the intelligence community have passed to the Justice Department.

Section 906. Foreign Terrorist Asset Tracking Center

Following the attacks of September 11, the Treasury Department announced the creation of an inter-agency foreign terrorist asset tracking center, which reportedly consists of agents from the Customs Service, Office of Foreign Asset Control (OFAC), Internal Revenue Service, FBI, and CIA.

Section 906 asks for a joint report from the Secretary of the Treasury, the Attorney General, and the Director of Central Intelligence on the feasibility of reconfiguring the Center and OFAC into an entity able to analyze the financial capabilities and resources of international terrorists organizations, on the extent to which the Financial Crimes Enforcement Center (FinCEN) should be included,

and on a legislative proposal detailing the specifics of any such entity found whose creation they find feasible and desirable.

Section 907. National Virtual Translation Center

Section 907 instructs the Director of Central Intelligence, in consultation with the Director of the FBI to report on the establishment of a national virtual translation center for the purpose providing timely and accurate translations of foreign intelligence.

Section 908. Training of Government Officials Regarding Identification and Use of Foreign Intelligence

Section 908 authorizes the necessary appropriations to train federal officials who do not ordinarily deal with foreign intelligence matters and state and local government officials who may encounter foreign intelligence in the course of a terrorist attack. The training would assist the officials to identify and use foreign intelligence information in the performance of their duties.

Title X – Miscellaneous

Section 1001. Review of the Department of Justice

As the House Judiciary Committee, from which this proposal first emerged, explained, "In the wake of several significant incidents of security lapses and breach of regulations, there has arisen the need for independent oversight of the Federal Bureau of Investigation. Oversight of the Federal Bureau of Investigation is currently under the jurisdiction of the Department of Justice Office of Professional Responsibility. This section directs the Inspector General of the Department of Justice to appoint a Deputy Inspector General for Civil Rights, Civil Liberties, and the Federal Bureau of Investigation who shall be responsible for supervising independent oversight of the FBI until September 30, 2004. This section also directs the Deputy Inspector to review all information alleging abuses of civil rights, civil liberties, and racial and ethnic profiling by employees of the Department of Justice, which could include allegations of inappropriate profiling at the border," H.Rept. 107-236, at 78. (2001).

Section 1002. Sense of Congress

Section 1002 expresses the sense of Congress that the rights of all Americans include those of Sikh-Americans should be protected in the quest to apprehend those responsible for the attacks of September 11; that violence or discrimination against any Americans including Sikh-Americans should be condemned; law enforcement authorities should work to prevent all Americans including Sikh-Americans from becoming crime victims; and that federal authorities should prosecute those responsible to the fullest extent of the law.

Section 1003. Definition of "Electronic Surveillance"

The Foreign Intelligence Surveillance Act (FISA) allows federal authorities to conduct "electronic surveillance" under certain limited foreign intelligence gathering purposes. Section 217 allows federal law enforcement officers to intercept the communications of computer trespassers within the system in which they are intruders, 18 U.S.C. 2511(2)(i). Section 1003 amends FISA to make it clear that the computer trespasser exception does not apply to FISA surveillance orders. FISA surveillance orders may be issued to acquire the communications of a computer trespasser, 50 U.S.C. 1801(f)(2).

Section 1004. Venue in Money Laundering Cases

The Constitution provides that, the "Trial of all Crimes . . . shall be held in the State where the said Crimes shall have been committed; but when not committed within any State, the Trial shall be at such Place or Places as the Congress may by Law have directed," U.S.Const. Art.III, §2, 3, and that "[i]n all criminal prosecutions, the accused shall enjoy the right to a speedy and public trial, by an impartial jury of the State and district wherein the crime shall have been committed, which district shall have been previously ascertained by law," U.S.Const. Amend. VI. When a crime begins in one district and continues on to another, trial may be constitutionally held in either district, United States v. Anderson, 328 U.S. 699, 704-5 (1946). Thus, the federal crime of conspiracy, which consists of the agreement to commit a federal crime plus an overt act committed in furtherance of the conspiracy, may be tried wherever the agreement occurred or wherever an overt act in its furtherance was committed, Hyde v. United States, 225 U.S. 347, 363 (1912).

This doctrine of continuing offenses, however, is not boundless. In United States v. Cabrales, 524 U.S. 1 (1998), a unanimous Supreme Court held that a charge of laundering of the proceeds of a Missouri drug trafficking operation in Florida could not tried in Missouri. In the course of its opinion, the Court observed, that "[m]oney laundering. . . arguably might rank as a continuing offense, triable in more that one place, if the launderer acquired the funds in one district and transported them into another," 524 U.S. at 8.

Section 1004 relies on this language when it permits a prosecution for money laundering in violation of either 18 U.S.C. 1956 or 1957 in the place where the predicate offense occurred "if the defendant participated in the transfer of the proceeds" of the predicate offense from the district in which the predicate offense occurred into the district in which the laundering occurred, 18 U.S.C. 1956(i)(1). The section also permits prosecution where an overt act in furtherance of conspiracy to violation the money laundering sections occurs, 18 U.S.C. 1956(i)(2).

Section 1005. First Responders Assistance Act

Section 1005 authorizes appropriations of $25 million for each fiscal year from 2003 through 2007 to permit the Attorney General to make grants to state and

local governments for terrorism prevention and antiterrorism training of fire fighters and other first responders. Each state from which a qualified grant application is submitted is entitled to no less than 0.5% of the total amount appropriated under section 1005 for that year.

Section 1006. Inadmissibility of Aliens Engaged in Money Laundering

Section 1006 makes aliens who have participated in money laundering inadmissible for admission into the United States. The Secretary of State is instructed to maintain a watchlist to be consulted to ensure that aliens involved in money laundering are not allowed to enter this country.

Section 1007. Authorization of Funds for DEA Police Training in South and Central Asia

The Taliban and al Qaeda reportedly fund their activities in part by trafficking in heroin. The material used to process the heroin flow into Afghanistan from South and Central Asia and the processed heroin is transported into world commerce through Turkey. Section 1007 authorizes appropriations of $5 million for Drug Enforcement Administration training for the police of Turkey and of the countries of South and Central Asia in order to disrupt heroin production in Afghanistan.

Section 1008. Feasibility Study on Use of Biometric Identifier Scanning System With Access to the FBI Integrated Automated Fingerprint Identification System at Overseas Consular Posts and Points of Entry to the United States

"Section 1008 requires the Attorney General to conduct a study of the feasibility of utilizing a biometric identifier (fingerprint) scanning system at consular offices and points of entry into the United States to identify aliens who may be wanted in connection with criminal or terrorist investigations in the United States or abroad. A biometric fingerprint scanning system is a sophisticated computer scanning technology that analyzes a person's fingerprint and compares the measurement with a verified sample digitally stored in the system. The accuracy of these systems is claimed to be above 99.9%. The biometric identifier system contemplated by this section would have access to the database of the Federal Bureau of Investigation Integrated Automated Fingerprint Identification System. The section requires that the Attorney General shall submit a summary of the findings of the study to Congress within 90 days.

Section 1009. Study of Access

Section 1009 authorizes $250,000 for the Federal Bureau of Investigation to study the feasibility of providing airlines with computer access to the names of those the federal government suspects of terrorism.

Section 1010. Temporary Authority to Contract With Local and State Governments for Performance of Security Functions at United States Military Installations

Subject to limited exceptions, the Department of Defense may not contract for fire fighting or security-guard functions to be performed on military installations, 10 U.S.C. 2465. Section 1010 creates another exception and allows neighboring state and local authorities to perform security functions for military installations and facilities pursuant to contracts with the Defense Department for a period up to 180 days after the completion of Operation Enduring Freedom.

Section 1011. Crimes Against Charitable Americans

The Telemarketing and Consumer Fraud and Abuse Prevention Act, 15 U.S.C. 6101 et seq. empowers the Federal Trade Commission (FTC) to promulgate regulations to prevent telemarketing deception. It is a federal crime to impersonate members or agents of the Red Cross for fraudulent purposes, 18 U.S.C. 917. And the federal criminal code imposes special penalties for telemarketing fraud, 18 U.S.C. 2325-2327.

Section 1011 brings telephone charitable solicitations under the FTC's regulatory umbrella, 15 U.S.C. 6102, 6106. It increases the penalty for impersonating Red Cross members or agents in order make fraudulent charitable solicitations from imprisonment for not more than 1 year to imprisonment for not more than 5 years, 18 U.S.C. 917. It also amends 18 U.S.C. 2325 in order make the enhanced telemarketing fraud penalties applicable to fraudulent charitable telephone solicitations, 18 U.S.C. 2325.

Section 1012. Limitation on Issuance of Hazmat Licenses

The Secretary of Transportation exercises regulatory authority over the safe interstate transportation of hazardous materials (hazmat), 49 U.S.C. 5101 et seq., and over commercial motor vehicle operators, 49 U.S.C. 31301 et seq. Section 1012 enacts 49 U.S.C. 5103a, which limits the issuance of hazmat licenses to instances where the Secretary of Transportation has certified that the applicant is not a security risk. It allows the states to request a background check from the Attorney General for a criminal record, for illegal alien status, and with Interpol. It expands the definition of hazardous materials to include chemical and biological materials and agents, and authorizes the Secretary of the Transportation to require the states to report relevant related information. Section 1012 also amends 49 U.S.C. 31305 with respect to the minimum standards for commercial motor vehicle operator fitness to include a determination that the applicant has been determined under section 5103a not to pose a security risk.

Section 1013. Expressing the Sense of the Senate Concerning the Provision of Funding for Bioterrorism Preparedness and Response

Section 1013 expresses the sense of the Senate that there should be an expanded level of public expenditures to prepare and respond to threats of bioterrorism.

Section 1014. Grant Program for State and Local Domestic Preparedness Support

Section 1014 authorizes appropriations in whatever sums are necessary for fiscal years 2002 through 2007 to make OJP grants to the state and local units of government to enhance their capacity to respond to terrorist attacks including those involving use of weapons of mass destruction, biological, chemical, nuclear, radiological, incendiary, chemical and explosive devises. The grants may be used to train and equip first responders. The Department of Justice may use no more than 3% of the appropriations for salaries and administrative expenses and each state is entitled to not less than 0.75% of the amount appropriated in any given fiscal year (not less than 0.25% for each of Guam, the Virgin Islands, American Samoa and the Northern Mariana Islands).

Section 1015. Expansion and Reauthorization of the Crime Identification Technology Act for Antiterrorism Grants to States and Localities

The Crime Identification Technology Act, Public Law 105-251, 112 Stat. 1871 (1998), 42 U.S.C. 14601, authorizes the OJP to issue state and local grants for the development of various integrated information and identification systems and for that purpose authorizes appropriations of $250 million for each fiscal year through 2003. Section 1015 amends section 14601 to permit grants for related terrorism purposes and extends the authorization of appropriations in the amount of $250 million per year through fiscal year 2007.

Section 1016. Critical Infrastructures Protection

Section 1016 authorizes appropriations of $20 million for fiscal year 2002 to be used by the Department of Defense's Defense Threat Reduction Agency for activities of National Infrastructure Simulation and Analysis Center.

The USA PATRIOT Act: A Legal Analysis, RL31377 (April 15, 2002).

CHARLES DOYLE, CONG. RESEARCH SERV., THE USA PATRIOT ACT: A LEGAL ANALYSIS (2002), *available at* http://www.intelligencelaw.com/library/secondary/crs/pdf/RL31377_4-15-2002.pdf.

Order Code RL31377
CRS Report for Congress

Received through the CRS Web

April 15, 2002

Charles Doyle
Senior Specialist American Law Division
Congressional Research Service ˜
The Library of Congress

SUMMARY

The USA PATRIOT Act passed in the wake of the September 11 terrorist attacks. It flows from a consultation draft circulated by the Department of Justice, to which Congress made substantial modifications and additions. The stated purpose of the Act is to enable law enforcement officials to track down and punish those responsible for the attacks and to protect against any similar attacks.

The Act grants federal officials greater powers to trace and intercept terrorists' communications both for law enforcement and foreign intelligence purposes. It reenforces federal anti-money laundering laws and regulations in an effort to deny terrorists the resources necessary for future attacks. It tightens our immigration laws to close our borders to foreign terrorists and to expel those among us. Finally, it creates a few new federal crimes, such as the one outlawing terrorists' attacks on mass transit; increases the penalties for many others; and institutes several procedural changes, such as a longer statute of limitations for crimes of terrorism.

Critics have suggested that it may go too far. The authority to monitor e-mail traffic, to share grand jury information with intelligence and immigration officers, to confiscate property, and to impose new book-keeping requirements on financial institutions, are among the features troubling to some.

The Act itself responds to some of these reservations. Many of the wiretapping and foreign intelligence amendments sunset on December 31, 2005. The Act

creates judicial safeguards for e-mail monitoring and grand jury disclosures; recognizes innocent owner defenses to forfeiture; and entrusts enhanced anti-money laundering powers to those regulatory authorities whose concerns include the wellbeing of our financial institutions.

This report, stripped of its citations and footnotes, is available in an abbreviated form as The USA PATRIOT Act: A Sketch, CRS REP.NO. RS21203. In addition, much of the information contained here may also be found under a different arrangement in a report entitled, Terrorism: Section by Section Analysis of the USA PATRIOT Act, CRS REP.NO. RL31200 (Dec. 10, 2001). A wider array of terrorism-related analysis appears on the CRS terrorism electronic briefing book page.

INTRODUCTION

Congress passed the USA PATRIOT Act (the Act) in response to the terrorists' attacks of September 11, 2001.[3330] The Act gives federal officials greater authority to track and intercept communications, both for law enforcement and foreign intelligence gathering purposes. It vests the Secretary of the Treasury with regulatory powers to combat corruption of U.S. financial institutions for foreign money laundering purposes. It seeks to further close our borders to foreign terrorists and to detain and remove those within our borders. It creates new crimes, new penalties, and new procedural efficiencies for use against domestic and international terrorists. Although it is not without safeguards, critics contend some of its provisions go too far. Although it grants many of the enhancements sought by the Department of Justice, others are concerned that it does not go far enough.

The Act originated as H.R.2975 (the PATRIOT Act) in the House and S.1510 in the Senate (the USA Act).[3331] S.1510 passed the Senate on October 11, 2001, 147 Cong.Rec. S10604 (daily ed.). The House Judiciary Committee reported out an amended version of H.R. 2975 on the same day, H.R.Rep.No. 107-236. The House passed H.R. 2975 the following day after substituting the text of H.R. 3108, 147 Cong.Rec. H6775-776 (daily ed. Oct. 12, 2001). The House-passed version incorporated most of the money laundering provisions found in an earlier House bill, H.R. 3004, many of which had counterparts in S.1510 as approved by

---

[3330] P.L. 107-56, 115 Stat. 272 (2001); its full title is the "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT)."

[3331] H.R. 2975 was introduced by Representative Sensenbrenner for himself and Representatives Conyers, Hyde, Coble, Goodlatte, Jenkins, Jackson-Lee, Cannon, Meehan, Graham, Bachus, Wexler, Hostettler, Keller, Issa, Hart, Flake, Schiff, Thomas, Goss, Rangel, Berman and Lofgren; S.1510 by Senator Daschle for himself and Senators Lott, Leahy, Hatch, Graham, Shelby and Sarbanes.

the Senate.[3332] The House subsequently passed a clean bill, H.R. 3162 (under suspension of the rules), which resolved the differences between H.R. 2975 and S.1510, 147 Cong. Rec. H7224 (daily ed. Oct. 24, 2001). The Senate agreed, 147 Cong. Rec. S10969 (daily ed. Oct. 24, 2001), and H.R. 3162 was sent to the President who signed it on October 26, 2001.

CRIMINAL INVESTIGATIONS: TRACKING AND GATHERING COMMUNICATIONS

A portion of the Act addresses issues suggested originally in a Department of Justice proposal circulated in mid-September.[3333] The first of its suggestions called for amendments to federal surveillance laws, laws which govern the capture and tracking of suspected terrorists' communications within the United States. Federal law features a three tiered system, erected for the dual purpose of protecting the confidentiality of private telephone, face-to-face, and computer communications while enabling authorities to identify and intercept criminal communications.[3334]

The tiers reflected the Supreme Court's interpretation of the Fourth Amendment's ban on unreasonable searches and seizures.[3335] The Amendment protects private conversations, Berger v. New York, 388 U.S. 41 (1967); Katz v. United States, 389 U.S. 347 (1967). It does not cloak information, even highly personal information, for which there is no individual justifiable expectation of privacy, such as telephone company records of calls made to and from an individual's home, Smith v. Maryland, 442 U.S. 735 (1979), or bank records of an individual's financial dealings, United States v. Miller, 425 U.S. 435 (1976).

[3332] H.R. 3004 was introduced by Representative Oxley for himself and Represenatives LaFalce, Leach, Maloney, Roukema, Bentsen, Hooley, Bereuter, Baker, Bachus, King, Kelly, Gillmore, Cantor, Riley, Latourette, Green (of Wisconsin), and Grucci; and reported out of the House Financial Services Committee with amendments on October 15, 2001, H.R.Rep.No. 107-250. H.R. 3004, as reported out, included Internet gambling amendments that were not included in H.R. 2975/H.R.3108.

[3333] The Department's proposal, dated September 20, 2001, came with a brief section by section analysis. Both the proposal (Draft) and analysis (DoJ) were printed as an appendix in Administration's Draft Anti-Terrorism Act of 2001, Hearing Before the House Comm. on the Judiciary, 107th Cong., 1st Sess. 54 (2001).

[3334] For a general discussion of federal law in the area prior to enactment of the Act, see, Stevens & Doyle, Privacy: An Overview of Federal Statutes Governing Wiretappping and Electronic Eavesdropping, CRS REP.NO. 98-327A (Aug. 8, 2001); Fishman & McKenna, WIRETAPPING AND EAVESDROPPING (2d ed. 1995 & 2001 Supp.).

[3335] "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized," U.S. Const. Amend. IV.

Congress responded to Berger and Katz, with Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. 2510-2522 (Title III). Title III, as amended, generally prohibits electronic eavesdropping on telephone conversations, face-to-face conversations, or computer and other forms of electronic communications, 18 U.S.C. 2511.[3336] At the same time, it gives authorities a narrowly defined process for electronic surveillance to be used as a last resort in serious criminal cases. When approved by senior Justice Department officials,[3337] law enforcement officers may seek a court order authorizing them to secretly capture conversations concerning any of a statutory list of offenses (predicate offenses), 18 U.S.C. 2516.[3338]

[3336] Although there are technical differences, the interception processes are popularly known as wiretapping, electronic eavesdropping, or electronic surveillance. The terms are used interchangeable here for purposes of convenience, but strictly speaking, wiretapping is limited to the mechanical or electronic interception of telephone conversations, while electronic eavesdropping or electronic surveillance refers to mechanical or electronic interception of communications generally.

[3337] "The Attorney General, Deputy Attorney General, Associate Attorney General, or any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General or acting Deputy Assistant Attorney General in the Criminal Division specially designated by the Attorney General, may authorize an application to a Federal judge of competent jurisdiction for, and such judge may grant in conformity with section 2518 of this chapter an order authorizing or approving the interception of wire or oral communications by the Federal Bureau of Investigation, or a Federal agency having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of" one or more predicate offense, 18 U.S.C. 2516.

[3338] The predicate offense list includes (a) felony violations of 42 U.S.C. 2274 through 2277 (enforcement of the Atomic Energy Act of 1954), 42 U.S.C. 2284 (sabotage of nuclear facilities or fuel), or of 18 U.S.C. ch. 37 (espionage), ch. 90 (protection of trade secrets), ch. 105 (sabotage), ch. 115 (treason), ch. 102 (riots), ch. 65 (malicious mischief), ch. 111 (destruction of vessels), or ch. 81 (piracy); (b) a violation of 29 U.S.C. 186 or 501(c) (restrictions on payments and loans to labor organizations), or any offense which involves murder, kidnapping, robbery, or extortion, and which is punishable under title 18 of the United States Code; (c) any offense which is punishable under 18 U.S.C. 201 (bribery of public officials and witnesses), 215 (bribery of bank officials), 224 (bribery in sporting contests), 844 (d), (e), (f), (g), (h), or (i) (unlawful use of explosives), 1032 (concealment of assets), 1084 (transmission of wagering information), 751 (escape), 1014 (loans and credit applications generally; renewals and discounts), 1503, 1512, and 1513 (influencing or injuring an officer, juror, or witness generally), 1510 (obstruction of criminal investigations), 1511 (obstruction of State or local law enforcement), 1751 (presidential and presidential staff assassination, kidnaping, or assault), 1951 (interference with commerce by threats or violence), 1952 (interstate and foreign travel or transportation in aid of racketeering enterprises), 1958 (use of interstate commerce facilities in the commission of murder for hire), 1959 (violent crimes in aid of racketeering activity), 1954 (offer, acceptance, or solicitation to influence operations of employee benefit plan), 1955 (prohibition of business enterprises of gambling), 1956 (laundering of monetary instruments), 1957 (engaging in monetary transactions in property derived from specified unlawful activity), 659 (theft from interstate shipment), 664 (embezzlement from pension and welfare funds), 1030 (computer abuse felonies), 1343 (fraud by wire, radio, or television), 1344 (bank fraud), 2251 and 2252 (sexual exploitation of children), 2312, 2313, 2314, and 2315 (interstate transportation of stolen property), 2321 (trafficking in certain motor vehicles or motor vehicle parts), 1203 (hostage taking), 1029 (fraud and related activity in connection with

Title III court orders come replete with instructions describing the permissible duration and scope of the surveillance as well as the conversations which may be seized and the efforts to be taken to minimize the seizure of innocent conversations, 18 U.S.C. 2518. The court notifies the parties to any conversations seized under the order after the order expires, 18 U.S.C. 2518(8).

Below Title III, the next tier of privacy protection covers some of those matters which the Supreme Court has described as beyond the reach of the Fourth Amendment protection – telephone records, e-mail held in third party storage, and the like, 18 U.S.C. 2701-2709 (Chapter 121). Here, the law permits law enforcement access, ordinarily pursuant to a warrant or court order or under a subpoena in some cases, but in connection with any criminal investigation and without the extraordinary levels of approval or constraint that mark a Title III interception, 18 U.S.C. 2703.

---

access devices), 3146 (penalty for failure to appear), 3521(b)(3) (witness relocation and assistance), 32 (destruction of aircraft or aircraft facilities), 38 (aircraft parts fraud), 1963 (violations with respect to racketeer influenced and corrupt organizations), 115 (threatening or retaliating against a Federal official), 1341 (mail fraud), 351 (violations with respect to congressional, Cabinet, or Supreme Court assassinations, kidnaping, or assault), 831 (prohibited transactions involving nuclear materials), 33 (destruction of motor vehicles or motor vehicle facilities), 175 (biological weapons), 1992 (wrecking trains), a felony violation of 1028 (production of false identification documentation), 1425 (procurement of citizenship or nationalization unlawfully), 1426 (reproduction of naturalization or citizenship papers), 1427 (sale of naturalization or citizenship papers), 1541 (passport issuance without authority), 1542 (false statements in passport applications), 1543 (forgery or false use of passports), 1544 (misuse of passports), or 1546 (fraud and misuse of visas, permits, and other documents); (d) any offense involving counterfeiting punishable under 18 U.S.C. 471, 472, or 473; (e) any offense involving fraud connected with a case under title 11 or the manufacture, importation, receiving, concealment, buying, selling, or otherwise dealing in narcotic drugs, marihuana, or other dangerous drugs, punishable under any law of the United States; (f) any offense including extortionate credit transactions under 18 U.S.C. 892, 893, or 894; (g) a violation of 31 U.S.C. 5322 (dealing with the reporting of currency transactions); (h) any felony violation of 18 U.S.C. 2511 and 2512 (interception and disclosure of certain communications and to certain intercepting devices); (i) any felony violation of 18 U.S.C. ch. 71 (obscenity); (j) 49 U.S.C. 60123(b) (destruction of a natural gas pipeline), 46502 (aircraft piracy); (k) 22 U.S.C. 2778 (Arms Export Control Act); (l) the location of any fugitive from justice from an offense described in this section; (m) a violation of 8 U.S.C. 1324, 1327, or 1328; (n) any felony violation of 18 U.S.C. 922, 924 (firearms); (o) any violation of 26 U.S.C. 5861 (firearms); (p) a felony violation of 18 U.S.C. 1028 (production of false identification documents), 1542 (false statements in passport applications), 1546 (fraud and misuse of visas, permits, and other documents) or a violation of 8 U.S.C. 1324, 1327, or 1328 (smuggling of aliens); (p) 229 (chemical weapons), 2332 (terrorist violence against Americans overseas), 2332a (weapons of mass destruction), 2332b (multinational terrorism), 2332d (financial transactions with countries supporting terrorism), 2339A (support of terrorist), 2332B (support of terrorist organizations); (r) any conspiracy to commit any of these, 18 U.S.C. 2516(1)(crimes added by the Act in italics). Other than telephone face to face conversations (i.e., electronic communications), the approval of senior Justice Department officials is not required and an order may be sought in any felony investigation, 18 U.S.C. 2516(3).

Least demanding and perhaps least intrusive of all is the procedure that governs court orders approving the government's use of trap and trace devices and pen registers, a kind of secret "caller id", which identify the source and destination of calls made to and from a particular telephone, 18 U.S.C. 3121-3127 (Chapter 206). The orders are available based on the government's certification, rather than a finding of the court, that the use of the device is likely to produce information relevant to the investigation of a crime, any crime, 18 U.S.C. 3123. The devices record no more than the identity of the participants in a telephone conversation,[3339] but neither the orders nor the results they produce need ever be revealed to the participants.

The Act modifies the procedures at each of the three levels. It:

- permits pen register and trap and trace orders for electronic communications (e.g., e-mail)
- authorizes nationwide execution of court orders for pen registers, trap and trace devices, and access to stored e-mail or communication records
- treats stored voice mail like stored e-mail (rather than like telephone conversations)
- permits authorities to intercept communications to and from a trespasser within a computer system (with the permission of the system's owner)
- adds terrorist and computer crimes to Title III's predicate offense list
- reenforces protection for those who help execute Title III, ch. 121, and ch. 206 orders
- encourages cooperation between law enforcement and foreign intelligence investigators
- establishes a claim against the U.S. for certain communications privacy violations by government personnel
- terminates the authority found in many of the these provisions and several of the foreign intelligence amendments with a sunset provision (Dec. 31, 2005).

Pen Registers and Trap and Trace Devices

In section 216, the Act allows court orders authorizing trap and trace devices and pen registers to be used to capture source and addressee information for computer conversations (e.g., e-mail) as well as telephone conversations, 18 U.S.C. 3121, 3123. In answer to objections that e-mail header information can be more revealing than a telephone number, it creates a detailed report to the court, 18 U.S.C. 3123(a)(3).[3340]

[3339] Or more precisely, they reveal no more than the identity of the numbers assigned to the telephone lines activated for a particular communication.

[3340] "Where the law enforcement agency implementing an ex parte order under this subsection seeks to do so by installing and using its own pen register or trap and trace device on a packet-switched data network of a provider of electronic communication service to the public the agency shall ensure that a record will be maintained which will identify – (i) any officer or officers who

The use of pen registers or trap and trace devices was limited at one time to the judicial district in which the order was issued, 18 U.S.C. 3123 (2000 ed.). Under section 216, a court with jurisdiction over the crime under investigation may issue an order to be executed anywhere in the United States, 18 U.S.C. 3123(b)(1)(C), 3127(2).[3341]

Communications Records and Stored E-Mail

With respect to chapter 126, relating among other things to the content of stored e-mail and to communications records held by third parties, the law permits criminal investigators to retrieve the content of electronic communications in storage, like e-mail, with a search warrant, and if the communication has been in remote storage for more than 180 days without notifying the subscriber, 18 U.S.C. 2703(a),(b). A warrant will also suffice to seize records describing telephone and other communications transactions without customer notice, 18 U.S.C. 2703(c). In the absence of the probable cause necessary for a warrant but with a showing of reasonable grounds to believe that the information sought is relevant to a criminal investigation, officers are entitled to a court order mandating access to electronic communications in remote storage for more than 180 days or to communications records, 18 U.S.C. 2703(b),(c). They can obtain a limited amount of record information (subscribers' names and addresses, telephone numbers, billing records and the like) using an administrative, grand jury, or trial court subpoena, 18 U.S.C. 2703(c)(1)(C). There is no subscriber notification in record cases. Elsewhere, the court may delay customer notification in the face of exigent circumstances or if notice is likely to seriously jeopardize the investigation or unduly delay the trial, 18 U.S.C. 2705.

In order to streamline the investigation process, the Act, in section 210, adds credit card and bank account numbers to the information law enforcement

---

installed the device and any officer or officers who accessed the device to obtain information from the network; (ii) the date and time the device was installed, the date and time the device was uninstalled, and the date, time, and duration of each time the device is accessed to obtain information; (iii) the configuration of the device at the time of its installation and any subsequent modification thereof; and (iv) any information which has been collected by the device. To the extent that the pen register or trap and trace device can be set automatically to record this information electronically, the record shall be maintained electronically throughout the installation and use of the such device. "(B) The record maintained under subparagraph (A) shall be provided ex parte and under seal to the court which entered the ex parte order authorizing the installation and use of the device within 30 days after termination of the order (including any extensions thereof)," section 216(b)(1).

[3341] The Justice Department urged the change in the name of expediency, "At present, the government must apply for new pen trap orders in every jurisdiction where an investigation is being pursued. Hence, law enforcement officers tracking a suspected terrorist in multiple jurisdictions must waste valuable time and resources by obtaining a duplicative order in each jurisdiction," DoJ at §101. Here and throughout citations to the United States Code (U.S.C.) without reference to an edition refer to the current Code; references to the 2000 edition of the Code refer to the law prior to amendment by the Act.

officials maysubpoena from a communications service provider's customer records, 18 U.S.C. 2703(c)(1)(C).[3342]

Another streamlining amendment, section 220, eliminates the jurisdictional restrictions on access to the content of stored e-mail pursuant to a court order. Previously, only a federal court in the district in which the e-mail was stored could issue the order. Under section 220, federal courts in the district where an offense under investigation occurred may issue orders applicable "without geographic limitation," 18 U.S.C. 2703.[3343]

The Act, in section 209, treats voice mail like e-mail, that is, subject to the warrant or court order procedure, rather than to the more demanding coverage of Title III once required, United States v. Smith, 155 F.3d 1050, 1055-56 (9th Cir. 1998).

Finally, the Act resolves a conflict between chapter 121 and the federal law governing cable companies. Government entities may have access to cable company customer records only under a court order following an adversary hearing if they can show that the records will evidence that the customer is or has engaged in criminal activity, 47 U.S.C. 511(h). When cable companies began offering telephone and other communications services the question arose whether the more demanding cable rules applied or whether law enforcement

---

[3342] Prior to the amendment, "investigators [could] not use a subpoena to obtain such records as credit card number or other form of payment. In many cases, users register with Internet service providers using false names, making the form of payment critical to determining the user's true identity. . . . this information [could] only be obtained by the slower and more cumbersome process of a court order. In fast-moving investigation[s] such as terrorist bombings – in which Internet communications are a critical method of identifying conspirators and in determining the source of the attacks – the delay necessitated by the use of court orders can often be important. Obtaining billing and other information can identify not only the perpetrator but also give valuable information about the financial accounts of those responsible and their conspirators," DoJ at §107.

[3343] Speaking of the law before amendment, DoJ explained, "Current law requires the government to use a search warrant to compel a provider to disclose unopened e-mail. 18 U.S.C. §2703(a). Because Federal Rule of Criminal Procedure 41 requires that the 'property' to be obtained 'be within the district' of the issuing court, however, the rule may not allow the issuance of §2703(a) warrants for e-mail located in other districts. Thus, for example, where an investigator in Boston is seeking electronic e-mail in the Yahoo! account of a suspected terrorist, he may need to coordinate with agents, prosecutors, and judges in the Northern District of California, none of whom have any other involvement in the investigation. This electronic communications information can be critical in establishing relationships, motives, means, and plans of terrorists. Moreover, it is equally relevant to cyber-incidents in which a terrorist motive has not (but may well be) identified. Finally, even cases that require the quickest response (kidnappings, threats, or other dangers to public safety or the economy) may rest on evidence gathered under §2703(a). To further public safety, this section accordingly authorizes courts with jurisdiction over investigations to compel evidence directly, without requiring the intervention of their counterparts in other districts where major Internet service providers are located," DoJ at §108.

agencies were entitled to ex parte court orders under the no-notice procedures applicable to communications providers.[3344] The Act makes it clear that the cable rules apply when cable television viewing services are involved and that the communications rules of chapter 121 apply when a cable company or anyone else provides communications services, section 211.

Electronic Surveillance

To Title III's predicate offense list, the Act adds cybercrime (18 U.S.C. 1030) and several terrorists crimes, sections 201, 202.[3345] A second cybercrime initiative, section 217, permits law enforcement officials to intercept the communications of an intruder within a protected computer system (i.e., a system used by the federal government, a financial institution, or one used in interstate or foreign commerce or communication), without the necessity of a warrant or court order, 18 U.S.C. 2511(2)(i). Yet only the interloper's intruding communications, those to or from the invaded system, are exposed under the section. The Justice Department originally sought the change because the law then did not clearly allow victims of computer trespassing to request law enforcement assistance in monitoring unauthorized attacks as they occur.[3346]

[3344] See e.g., DoJ at §109 ("Law enforcement must have the capability to trace, intercept, and obtain records of the communications of terrorists and other criminals with great speed, even if they choose to use a cable provider for their telephone and Internet service. This section amends the Cable Communications Policy Act ('Cable Act') to clarify that when a cable company acts as a telephone company or an Internet service provider, it must comply with the same laws governing the interception and disclosure of wire and electronic communications that apply to any other telephone company or Internet service provider. The Cable Act, passed in 1984 to regulate various aspects of the cable television industry, could not take into account the changes in technology that have occurred over the last seventeen years. Cable television companies now often provide Internet access and telephone service in addition to television programming. Because of perceived conflicts between the Cable Act and laws that govern law enforcement's access to communications and records of communications carried by cable companies, cable providers have refused to comply with lawful court orders, thereby slowing or ending critical investigations").

[3345] 18 U.S.C. 229 (chemical weapons), 2332(terrorist acts of violence committed against Americans overseas), 2332a(use of weapons of mass destruction), 2332b(acts of terrorism transcending national boundaries), 2332d(financial transactions with countries which support terrorists), 2339A(providing material support to terrorists), and 2339B(providing material support to terrorist organizations).

[3346] "Because service providers often lack the expertise, equipment, or financial resources required to monitor attacks themselves as permitted under current law, they often have no way to exercise their rights to protect themselves from unauthorized attackers. Moreover, such attackers can target critical infrastructures and engage in cyberterrorism," DoJ at §106. Elsewhere the Act defines "electronic surveillance" for purposes of the Foreign Intelligence Surveillance Act (FISA) to emphasize that the law enforcement authority for this intruder surveillance does not confer similar authority for purposes of foreign intelligence gathering, section 1003 (50 U.S.C. 1801(f)(2)).

Criminal Investigators' Access to Foreign Intelligence Information

The Act clearly contemplates closer working relations between criminal investigators and foreign intelligence investigators, particular in cases of international terrorism.[3347] It amends the Foreign Intelligence Surveillance Act (FISA) to that end. As originally enacted, the application for a surveillance order under FISA required certification of the fact that "the purpose for the surveillance is to obtain foreign intelligence information," 50 U.S.C. 1804(a)(7)(B)(2000 ed.) (emphasis added), although it anticipated that any evidence divulged as a result might be turned over to law enforcement officials. Defendants often questioned whether authorities had used a FISA surveillance order against them in order to avoid the predicate crime threshold for a Title III order. Out of these challenges arose the notion that perhaps "the purpose" might not always mean the sole purpose. The case law indicated that, while an expectation that evidence of a crime might be discovered did not preclude a FISA order, at such time as a criminal prosecution became the focus of the investigation officials were required to either end surveillance or secure an order under Title III.[3348]

[3347] For a general discussion of federal intelligence and law enforcement cooperation, see, Best, Intelligence and Law Enforcement: Countering Transnational Threats to the U.S., CRS REP.NO. RL30252 (Dec. 3, 2001).

[3348] Before FISA, several lower federal courts recognized a foreign intelligence exception to the Fourth Amendment's warrant clause. It is here that the "primary purpose" notion originated. In United States v. Truong Dinh Hung, 629 F.2d 908, 915 (4th Cir. 1980), decided after FISA on the basis of pre-existing law, the court declared, "as the district court ruled, the executive should be excused from securing a warrant only when the surveillance is conducted 'primarily' for foreign intelligence reasons. We think that the district court adopted the proper test, because once surveillance becomes primarily a criminal investigation, the courts are entirely competent to make the usual probable cause determination, and because, importantly, individual privacy interests come to the fore and government foreign policy concerns recede when the government is primarily attempting to form the basis for a criminal prosecution." Subsequent case law, however, is not as clear as it might be: see e.g., United States v. Duggan, 743 F.2d 59, 77 (2d Cir. 1984)("FISA permits federal officials to obtain orders authorizing electronic surveillance 'for the purpose of obtaining foreign intelligence information.' The requirement that foreign intelligence information be the primary objective of the surveillance is plain not only from the language of Sec. 1802(b) but also from the requirements in Sec. 1804 as to what the application must contain. The application must contain a certification by a designated official of the executive branch that the purpose of the surveillance is to acquire foreign intelligence information, and the certification must set forth the basis for the certifying officials's belief that the information sought is the type of foreign intelligence information described"); United States v. Pelton, 835 F.2d 1067, 1075-76 (4th Cir. 1987)("We also reject Pelton's claim that the 1985 FISA surveillance was conducted primarily for the purpose of his criminal prosecution, and not primarily for the purpose of obtaining foreign intelligence information. . . . We agree with the district court that the primary purpose of the surveillance, both initially and throughout was to gather foreign intelligence information. It is clear that otherwise valid FISA surveillance is not tainted simply because the government can anticipate that the fruits of the surveillance may later be used . . . as evidence in a criminal trial"); United States v. Sarkissian, 841 F.2d 959, 907-8 (9th Cir. 1988)("Defendants rely on the primary purpose test articulated in United States v. Truong Dinh Hung. . . . One other court has applied the primary purpose test. Another court has rejected it . . . distinguishing

The Justice Department sought FISA surveillance and physical search authority on the basis of "a" foreign intelligence purpose.[3349] Section 218 of the Act insists that foreign intelligence gathering be a "significant purpose" for the request for the FISA surveillance or physical search order, 50 U.S.C. 1804(a)(7)(B), 1823(a)(7)(B), a more demanding standard than the "a purpose" threshold proposed by the Justice Department, but a clear departure from the original "the purpose" entry point. FISA once described a singular foreign intelligence focus prerequisite for any FISA surveillance application. Section 504 of the Act further encourages coordination between intelligence and law enforcement officials, and states that such coordination is no impediment to a "significant purpose" certification, 50 U.S.C. 1806(k), 1825(k).[3350]

Protective Measures

The Act reenforces two kinds of safeguards, one set designed to prevent abuse and the other to protect those who assist the government. The sunset clause is perhaps the best known of the Act's safeguards. Under the direction of section 224, many of the law enforcement and foreign intelligence authorities granted by the Act expire as of December 31, 2005.[3351] The Act also fills some of the gaps in

---

Truong. A third court has declined to decide the issue. We also decline to decide the issue"); United States v. Johnson, 952 F.2d 565, 572 (1st Cir. 1991)("Appellants attack the government's surveillance on the ground that it was undertaken not for foreign intelligence purposes, but to gather evidence for a criminal prosecution. FISA applications must contain, among other things, a certification that the purpose of the requested surveillance is the gathering of foreign intelligence information. . . . Although the evidence obtained under FISA subsequently may be used in criminal prosecutions, the investigation of criminal activity cannot be the primary purpose of the surveillance").

[3349] "Current law requires that FISA be used only where foreign intelligence gathering is the sole or primary purpose of the investigation. This section will clarify that the certification of a FISA request is supportable where foreign intelligence gathering is 'a' purpose of the investigation. This change would eliminate the current need continually to evaluate the relative weight of criminal and intelligence purposes, and would facilitate information sharing between law enforcement and foreign intelligence authorities which is critical to the success of anti-terrorism efforts," DoJ at §153.

[3350] "(k)(1) Federal officers who conduct electronic surveillance to acquire foreign intelligence information under this title may consult with Federal law enforcement officers to coordinate efforts to investigate or protect against – (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power; (B) sabotage or international terrorism by a foreign power or an agent of a foreign power; or (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power. (2) Coordination authorized under paragraph (1) shall not preclude the certification required by section 104(a)(7)(B) or the entry of an order under section 105." FISA defines "foreign power" and "agent of a foreign power" broadly, see note 33, infra, quoting, 50 U.S.C. 1801.

[3351] "(a) Except as provided in subsection (b), this title and the amendments made by this title (other than sections 203(a)[sharing grand jury information], 203(c)[procedures for sharing grand jury information], 205 [FBI translators], 208 [seizure of stored voice-mail], 210[subpoenas for communications provider customer records], 211[access to cable company communication service

earlier sanctions available for official, abusive invasions of privacy. Prior law made it a federal crime to violate Title III (wiretapping), chapter 121 (e-mail and communications records), or chapter 206 (pen registers and trap and trace devices).[3352] Victims of offenses under Title III and chapter 121 (but not chapter 206) were entitled to damages (punitive damages in some cases) and reasonable attorneys' fees,[3353] but could not recover against the United States.[3354] Chapter 121 alone insisted upon an investigation into whether disciplinary action ought to be taken when federal officers or employees were found to have intentionally violated its proscriptions, 18 U.S.C. 2707.

The Act augments these sanctions by authorizing a claim against the United States for not less than $10,000 and costs for violations of Title III, chapter 121, or the Foreign Intelligence Surveillance Act (FISA), by federal officials, and emphasizing the prospect of administrative discipline for offending federal officials, section 223.

Finally, the Act instructs the Department of Justice's Inspector General to designate an official to receive and review complaints of civil liberties violations by DoJ officers and employees, section 1001.

The second category of protective measures applies to service providers and others who help authorities track and gather communications information. For

---

records], 213[sneak and peek], 216[pen register and trap and trace device amendments], 221[trade sanctions], and 222[assistance to law enforcement], and the amendments made by those sections) shall cease to have effect on December 31, 2005. "(b) With respect to any particular foreign intelligence investigation that began before the date on which the provisions referred to in subsection (a) cease to have effect, or with respect to any particular offense or potential offense that began or occurred before the date on which such provisions cease to have effect, such provisions shall continue in effect," section 224. The sections which expire are: 201 and 202 (adding certain terrorism crimes to the predicate list for Title III), 293(b)(sharing Title III information with foreign intelligence officers), 204 (clarifying the foreign intelligence exception to the law enforcement pen register and trap and trace device provisions), 206 (roving foreign intelligence surveillance), 207 (duration of foreign intelligence surveillance orders and extensions), 209 (treatment of voice mail as e-mail rather than as telephone conversation), 212 (service provider disclosures in emergency cases), 214 (authority for pen registers and trap and trace devices in foreign intelligence cases), 215 (production of tangible items in foreign intelligence investigations), 217 (intercepting computer trespassers' communications), 218 (foreign intelligence surveillance when foreign intelligence gathering is "a significant" reason rather than "the" reason for the surveillance), 219 (nationwide terrorism search warrants), 220 (nationwide communication records and stored e-mail search warrants), 223 (civil liability and administrative discipline for violations of Title III, chapter 121, and certain foreign intelligence prohibitions), and 225 (immunity for foreign intelligence surveillance assistance).

[3352] 18 U.S.C. 2511, 2701, and 3121 (2000 ed.), respectively.

[3353] 18 U.S.C. 2520 and 2707 (2000 ed.).

[3354] Spock v. United States, 464 F.Supp. 510, 514 n.2 (S.D.N.Y. 1978); Asmar v. IRS, 680 F.Supp. 248, 250 (E.D.Mich. 1987).

example, section 815 immunizes service providers who in good faith preserve customer records at the government's request until a court order authorizing access can be obtained.[3355] Another allows providers to disclose customer records to protect the provider's rights and property and to disclose stored customer communications and records in emergency circumstances, section 212. Under pre-existing law providers could disclose the content of stored communications but not customer records. The Justice Department recommended the changes in the interests of greater protection against cybercrimes committed by terrorists and others.[3356] A third section, section 222 promises reasonable compensation for service providers and anyone else who help law enforcement install or apply pen registers or trap and trace devices,[3357] but makes it clear that nothing in the Act is intended to expand communications providers' obligation to make modifications in their systems in order to accommodate law enforcement needs.[3358]

[3355] Prior law already granted service providers immunity for disclosure of customer records in compliance with a court access order, 18 U.S.C. 2703(f).

[3356] "Existing law contains no provision that allows providers of electronic communications service to disclose the communications (or records relating to such communications) of their customers or subscribers in emergencies that threaten death or serious bodily injury. This section amends 18 U.S.C. §2702 to authorize such disclosures if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person requires disclosure of the information without delay. "Current law also contains an odd disconnect: a provider may disclose the contents of the customer's communications in order to protect its rights or property but the current statute does not expressly permit a provider to voluntarily disclose non-content records (such as a subscriber's login records). 18 U.S.C. 2702(b)(5). This problem substantially hinders the ability of providers to protect themselves from cyber-terrorists and criminals. Yet the right to disclose the contents of communications necessarily implies the less intrusive ability to disclose non-content records. In order to promote the protection of our nation's critical infrastructures, this section's amendments allow communications providers to voluntarily disclose both content and non-content records to protect their computer systems," DoJ at § 110.

[3357] Chapter 206 had long guaranteed providers and others reasonable compensation, 18 U.S.C. 3124(c), but section 216 of the Act expands the circumstances under which the authorities may request assistance including requests for the help of those not specifically mentioned in the court order. Section 222 makes it clear the expanded obligation to provide assistance is matched by a corresponding right to compensation.

[3358] Thus in the name of assisting in the execution of Title III, chapter 121, or chapter 206 order, the courts may not cite the Act as the basis for an order compelling a service provider to make system modifications or provide any other technical assistance not already required under 18 U.S.C. 2518(4), 2706, or 3124(c), see, H.R.Rep.No. 107-236, at 62-3 (2001) (emphasis added) ("This Act is not intended to affect obligations under Communications Assistance for Law Enforcement Act [which addresses law enforcement-beneficial system modifications and the compensation to be paid for the changes], nor does the act impose any additional technical obligation or requirement on a provider of wire or electronic communication service or other person to furnish facilities or technical assistance").

Although both criminal investigations and foreign intelligence investigations are conducted in the United States, criminal investigations seek information about unlawful activity; foreign intelligence investigations seek information about other countries and their citizens. Foreign intelligence is not limited to criminal, hostile, or even governmental activity. Simply being foreign is enough.[3359]

Restrictions on intelligence gathering within the United States mirror American abhorrence of the creation of a secret police, coupled with memories of intelligence gathering practices during the Vietnam conflict which some felt threatened to chill robust public debate. Yet there is no absolute ban on foreign intelligence gathering in the United States. Congress enacted the Foreign Intelligence Surveillance Act (FISA),[3360] something of a Title III for foreign intelligence wiretapping conducted in this country, after the Supreme Court made it clear that the President's authority to see to national security was insufficient to excuse warrantless wiretapping of suspected terrorists who had no identifiable foreign connections, United States v. United States District Court, 407 U.S. 297 (1972). FISA later grew to include procedures for physical searches in foreign intelligence cases, 50 U.S.C. 1821-1829, for pen register and trap and trace orders, 50 U.S.C. 1841-1846, and for access to records from businesses engaged in car rentals, motel accommodations, and storage lockers, 50 U.S.C. 1861-1863 (2000 ed.). Intelligence authorities gained narrow passages through other privacy barriers as well.[3361]

In many instances, access was limited to information related to the activities of foreign governments or their agents in this country, not simply relating to something foreign here. FISA, for example, is directed at foreign governments, international terrorists, and their agents, spies and saboteurs.[3362] There were and

---

[3359] E.g., As amended by section 902 of the Act, "'foreign intelligence' means information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities," 50 U.S.C. 401a(2)(language added by the Act in italics).

[3360] 50 U.S.C. 1801 et seq.

[3361] E.g., 18 U.S.C. 2709 (counterintelligence access to telephone toll and transaction records), 12 U.S.C. 3414 (right to financial privacy), 15 U.S.C. 1681u(fair credit reporting).

[3362] "As used in this subchapter: (a) 'Foreign power' means – (1) a foreign government or any component thereof, whether or not recognized by the United States; (2) a faction of a foreign nation or nations, not substantially composed of United States persons; (3) an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments; (4) a group engaged in international terrorism or activities in preparation therefor; (5) a foreign-based political organization, not substantially composed of United States persons; or (6) an entity that is directed and controlled by a foreign government or governments. "(b) 'Agent of a foreign power' means – (1) any person other than a United States person, who – (A) acts in the United States as an officer or employee of a foreign

still are extra safeguards if it appears that an intelligence investigation may generate information about Americans ("United States persons," i.e., citizens or permanent resident aliens).[3363] The procedures tend to operate under judicial supervision and tend to be confidential as a matter of law, prudence, and practice.

The Act eases some of the restrictions on foreign intelligence gathering within the United States, and affords the U.S. intelligence community greater access to

---

power, or as a member of a foreign power as defined in subsection (a)(4) of this section; (B) acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of the United States, when the circumstances of such person's presence in the United States indicate that such person may engage in such activities in the United States, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities; or (2) any person who – (A) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States; (B) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States;(C) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, or on behalf of a foreign power; (D) knowingly enters the United States under a false or fraudulent identity for or on behalf of a foreign power or, while in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power; or (E) knowingly aids or abets any person in the conduct of activities described in subparagraph (A), (B), or (C) or knowingly conspires with any person to engage in activities described in subparagraph (A), (B), or (C). "(c) 'International terrorism' means activities that – (1) involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or any State; (2) appear to be intended – (A) to intimidate or coerce a civilian population; (B) to influence the policy of a government by intimidation or coercion; or (C) to affect the conduct of a government by assassination or kidnaping; and (3) occur totally outside the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum. "(d) 'Sabotage' means activities that involve a violation of chapter 105 of Title 18, or that would involve such a violation if committed against the United States. "(e) 'foreign intelligence information' means – (1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against – (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power; (B) sabotage or international terrorism by a foreign power or an agent of a foreign power; or (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or (2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to – (A) the national defense or the security of the United States; or (B) the conduct of the foreign affairs of the United States," 50 U.S.C. 1801.

[3363] Strictly speaking for FISA purposes, a United States person "means a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 1101(a)(20) of Title 8), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in subsection (a)(1), (2), or (3) of this section," 50 U.S.C. 1801(i).

information unearthed during a criminal investigation, but it also establishes and expands safeguards against official abuse. More specifically, it:

- permits "roving" surveillance (court orders omitting the identification of the particular instrument, facilities, or place where the surveillance is to occur when the court finds the target is likely to thwart identification with particularity)
- increases the number of judges on the FISA court from 7 to 11
- allows application for a FISA surveillance or search order when gathering foreign intelligence is a significant reason for the application rather than the reason
- authorizes pen register and trap & trace device orders for e-mail as well as telephone conversations
- sanctions court ordered access to any tangible item rather than only business records held by lodging, car rental, and locker rental businesses
- carries a sunset provision
- establishes a claim against the U.S. for certain communications privacy violations by government personnel
- expands the prohibition against FISA orders based solely on an American's exercise of his or her First Amendment rights.

FISA

FISA is in essence a series of procedures available to secure court orders in certain foreign intelligence cases.[3364] It operates through the judges of a special court which prior to the Act consisted of seven judges, scattered throughout the country, two of whom were from the Washington, D.C. area. The Act, in section 208, authorizes the appointment of four additional judges and requires that three members of the court reside within twenty miles of the District of Columbia, 50 U.S.C. 1803(a).

Search and Surveillance for Intelligence Purposes

Unless directed at a foreign power, the maximum duration for FISA surveillance orders and extensions was once ninety days and forty-five days for physical search orders and extensions, 50 U.S.C. 1805(e), 1824(d)(2000 ed.). The Act, in section 207, extends the maximum tenure of physical search orders to ninety days and in the case of both surveillance orders and physical search orders extends the maximum life of an order involving an agent of a foreign power to 120 days, with extensions for up to a year, 50 U.S.C. 1805(e), 1824(d). This represents a compromise over the Justice Department's original proposal which

---

[3364] For a general discussion of FISA prior to enactment of the Act, see, Bazan, The Foreign Intelligence Surveillance Act: An Overview of the Statutory Framework for Electronic Surveillance, CRS REP.NO. RL30465 (Sept. 18, 2001).

would have set the required expiration date for orders at one year instead of 120 days, Draft at §151.[3365]

Section 901 of the Act address a concern raised during the 106th Congress relating to the availability of the FISA orders and the effective use of information gleaned from the execution of a FISA order.[3366] It vests the Director of Central Intelligence with the responsibility to formulate requirements and priorities for the use of FISA to collect foreign intelligence information. He is also charged

---

[3365] See also, DoJ at §151, "This section reforms a critical aspect of the Foreign Intelligence Surveillance Act (FISA). It will enable the Foreign Intelligence Surveillance Court (FISC), which presides over applications made by the U.S. government under FISA, to authorize the search and surveillance in the U.S. of officers and employees of foreign powers and foreign members of international terrorist groups for up to a year. Currently, the FISC may only authorize such searches and surveillance for up to 45 days and 90 days, respectively. The proposed change would bring the authorization period in line with that allowed for search and surveillance of the foreign establishments for which the foreign officers and employees work. The proposed change would have no effect on electronic surveillance of U.S. citizens or permanent resident aliens." Section 314 of the Intelligence Authorization Act for Fiscal Year 2002 (Intelligence Authorization Act), P.L. 107-108, 115 Stat. 1394, 1402 (2001), further amended some of the time limits relating to FISA surveillance and physical searches, extending from 24 hours to 72 hours: (a) the time period during which agents might disseminate or use information secured pursuant to a FISA surveillance or search order but otherwise protected from dissemination or use by the order's minimization requirements; and (b) the permissible duration of emergency surveillance or searches after which surveillance or the search must stop or a FISA order application filed (50 U.S.C. 1801(h)(4), 1821(4)(D), 1805(f), 1824(e)).

[3366] See e.g., S.Rep.No. 106-352, at 3, 6, 7 (2000)("The Office of Intelligence Policy and Review (OIPR) in the Department of Justice is responsible for advising the Attorney General on matters relating to the national security of the United States. As part of its responsibilities, the OIPR prepares and presents to the Foreign Intelligence Surveillance Court (FISC) all applications for electronic surveillance and physical searches under the Foreign Intelligence Surveillance Act . . . . Agencies have informed the Committee that the FISA application process, as interpreted by the OIPR is administratively burdensome and, at times, extremely slow. Many applications undergo months of scrutiny before submission to the court because the OIPR prescribes standards and restrictions not imposed by the statute. . . . In particular, the OIPR has been criticized for an overly restrictive interpretation of the FISA 'currency' requirement. This is the issue of how recent a subject's activities must be to support a finding of probable cause that the subject is engaged in clandestine intelligence gathering activities. . . .While existing law does not specifically address ``past activities,'' it does not preclude, and legislative history supports, the conclusion that past activities may be part of the totality of circumstances considered by the FISC in making a probable cause determination. . . . By definition, information collected pursuant to a court order issued under the Foreign Intelligence Surveillance Act is foreign intelligence not law enforcement information. Accordingly, the Committee wants to clarify that the FISA `take' can and must be shared by the Federal Bureau of Investigation with appropriate intelligence agencies. For the intelligence mission of the United States to be successful, there must be a cooperative and concerted effort among intelligence agencies. Any information collected by one agency under foreign intelligence authorities that could assist another agency in executing its lawful mission should be shared fully and promptly. Only then can the United States Government pursue aggressively important national security targets including, for example, counterterrorist and counternarcotics targets"); see also, 147 Cong. Rec. S799-803 (daily ed. Feb. 24, 2000)(remarks of Sens. Specter, Torricelli and Biden).

with the responsibility of assisting the Attorney General in the efficient and effective dissemination of FISA generated information (50 U.S.C. 403-3(c)).

Pen Registers and Trap and Trace Devices for Intelligence Gathering

Section 214 grants the request of the Department of Justice by dropping requirements which limited FISA pen register and trap and trace device orders to facilities used by foreign agents or those engaged in international terrorist or clandestine intelligence activities, 50 U.S.C. 1842(c)(3)(2000 ed.).[3367] It is enough that the order is sought as part of an investigation to protect against international terrorism or clandestine intelligence activities and is not motivated solely by an American's exercise of his or her First Amendment rights. Elsewhere (section 505), the Act drops a similar limitation for intelligence officials' access to telephone records, 18 U.S.C. 2709(b), and under the Right to Financial Privacy Act, 12 U.S.C. 3414(a)(5)(A), as well as the Fair Credit Reporting Act, 15 U.S.C. 1681u.[3368]

[3367] "When added to FISA two years ago, the pen register/trap and trace section was intended to mirror the criminal pen/trap authority defined in 18 U.S.C. §3123. The FISA authority differs from the criminal authority in that it requires, in addition to a showing of relevance, an additional factual showing that the communications device has been used to contact an 'agent of a foreign power' engaged in international terrorism or clandestine intelligence activities. This has the effect of making the FISA pen/trap authority much more difficult to obtain. In fact, the process of obtaining FISA pen/trap authority is only slightly less burdensome than the process for obtaining full electronic surveillance authority under FISA. This stands in stark contrast to the criminal pen/trap authority, which can be obtained quickly from a local court, on the basis of a certification that the information to be obtained is relevant to an ongoing investigation. The amendment simply eliminates the 'agent of a foreign power' prong from the predication, and thus makes the FISA authority more closely track the criminal authority," DoJ at §155.

[3368] Except in the case of certain credit information, these are not court procedures, but written requests for third party records which would otherwise to be entitled to confidentiality. Section 505, in response to the Justice Department's suggestion, allows FBI field offices to make the requests, see DoJ at §157 ("At the present time, National Security Letter (NSL) authority exists in three separate statutes: the Electronic Communications Privacy Act (for telephone and electronic communications records), the Financial Right to Privacy Act (for financial records), and the Fair Credit Reporting Act (for credit records). Like the FISA pen register/trap and trace authority described above, NSL authority requires both a showing of relevance and a showing of links to an 'agent of a foreign power.' In this respect, they are substantially more demanding than the analogous criminal authorities, which require only a certification of relevance. Because the NSLs require documentation of the facts supporting the 'agent of a foreign power' predicate and because they require the signature of a high-ranking official at FBI headquarters, they often take months to be issued. This is in stark contrast to criminal subpoenas, which can be used to obtain the same information, and are issued rapidly at the local level. In many cases, counterintelligence and counterterrorism investigations suffer substantial delays while waiting for NSLs to be prepared, returned from headquarters, and served. The section would streamline the process of obtaining NSL authority, and also clarify the FISA Court can issue orders compelling production of consumer reports").

Section 214 adjusts the language of the FISA pen register-trap and trace authority to permit its use to capture source and destination information relating to electronic communications (e.g., e-mail) as well as telephone communications, 50 U.S.C. 1842(d). The section makes it clear that requests for a FISA pen register-trap and trace order, like requests for other FISA orders, directed against Americans (U.S. persons) may not be based solely on activities protected by the First Amendment, 50 U.S.C. 1842, 1843.

Third Party Cooperation and Tangible Evidence

As in the case of criminal investigations, the Act has several sections designed to encourage third party cooperation and to immunize third parties from civil liability for their assistance. FISA orders may include instructions directing specifically identified third parties to assist in the execution of the order, 50 U.S.C. 1805(c)(2)(B). The Act permits inclusion of a general directive for assistance when the target's activities are designed to prevent more specific identification, section 206, and immunizes in 50 U.S.C. 1805(h), those who provide such assistance, section 225.[3369]

Prior to the Act, FISA allowed federal intelligence officers to seek a court order for access to certain car rental, storage, and hotel accommodation records, 50 U.S.C. 1861 to 1863 (2000 ed.). The Justice Department asked that the authority be replaced with permission to issue administrative subpoenas for any tangible item regardless of the business (if any) of the custodian.[3370] The Act amends the

---

[3369] When it requested the amendment, the Department of Justice explained that the "provision expands the obligations of third parties to furnish assistance to the government under FISA. Under current FISA provisions, the government can seek information and assistance from common carriers, landlords, custodians and other persons specified in court-ordered surveillance. Section 152 would amend FISA to expand existing authority to allow, 'in circumstances where the Court finds that the actions of the target of the application may have the effect of thwarting the identification of a specified person that a common carrier, landlord, custodian or other persons not specified in the Court's order be required to furnish the applicant information and technical assistance necessary to accomplish electronic surveillance in a manner that will protect its secrecy and produce a minimum of interference with the services that such person is providing to the target of electronic surveillance.' This would enhance the FBI's ability to monitor international terrorists and intelligence officers who are trained to thwart surveillance by rapidly changing hotel accommodations, cell phones, Internet accounts, etc., just prior to important meetings or communications. Under the current law, the government would have to return to the FISA Court for an order that named the new carrier, landlord, etc., before effecting surveillance. Under the proposed amendment, the FBI could simply present the newly discovered carrier, landlord, custodian or other person with a generic order issued by the Court and could then effect FISA coverage as soon as technically feasible," DoJ at 152. Section 314 of the Intelligence Authorization Act immunizes those who assist in the execution of either a FISA surveillance or physical search order (50 U.S.C. 1805(i)), 115 Stat. 1402.

[3370] "The 'business records' section of FISA (50 U.S.C. §§ 1861 and 1862) requires a formal pleading to the Court and the signature of a FISA judge (or magistrate). In practice, this makes the authority unavailable for most investigative contexts. The time and difficulty involved in getting such pleadings before the Court usually outweighs the importance of the business records

provisions, preserving the court order requirement. Yet it allows the procedure to be used in foreign intelligence investigations, conducted to protect against international terrorism or clandestine intelligence activities,[3371] in order to seize any tangible item regardless of who is in possession of the item, and continues in place the immunity for good faith compliance by third party custodians, section 215.

In a related provision, Section 358 amends the –

- purposes section of the Currency and Foreign Transaction Reporting Act (31 U.S.C. 5311);
- suspicious activities reporting requirements section of that Act (31 U.S.C. 5318(g)(4)(B);
- availability of records section of that Act (31 U.S.C. 5319);
- purposes section of the Bank Secrecy Act (12 U.S.C. 1829b(a);
- the Secretary of the Treasury's authority over uninsured banks and other financial institutions under that Act (12 U.S.C. 1953(a);
- access provisions of the Right to Financial Privacy Act (12 U.S.C. 3412(2)(a), 3414(a)(1), 3420(a)(2); and
- access provisions of the Fair Credit Reporting Act (15 U.S.C. 1681u, 1681v; to clarify and authorize access of federal intelligence authorities to the reports and information gathered and protected under those Acts.[3372]

---

sought. Since its enactment, the authority has been sought less than five times. This section would delete the old authority and replace it with a general 'administrative subpoena' authority for documents and records. This authority, modeled on the administrative subpoena authority available to drug investigators pursuant to Title 21, allows the Attorney General to compel production of such records upon a finding that the information is relevant," DoJ at §156.

[3371] Section 314 of the Intelligence Authorization Act further amended the section to permit orders relating to investigations "to obtain foreign intelligence information not concerning a United States person" in addition to those conducted to protect against terrorism and clandestine activities, 50 U.S.C. 1861(a)(1).

[3372] H.R. Rep. No. 107-205, at 60-1 (2001)("This section clarifies the authority of the Secretary of the Treasury to share Bank Secrecy Act information with the intelligence community for intelligence or counterintelligence activities related to domestic or international terrorism. Under current law, the Secretary may share BSA information with the intelligence community for the purpose of investigating and prosecuting terrorism. This section would make clear that the intelligence community may use this information for purposes unrelated to law enforcement. "The provision would also expand a Right to Financial Privacy Act (RFPA) exemption, currently applicable to law enforcement inquiries, to allow an agency or department to share relevant financial records with another agency or department involved in intelligence or counterintelligence activities, investigations, or analyses related to domestic or international terrorism. The section would also exempt from most provisions of the RFPA a government authority engaged in investigations of or analyses related to domestic or international terrorism. This section would also authorize the sharing of financial records obtained through a Federal grand jury subpoena when relevant to intelligence or counterintelligence activities, investigations, or analyses related to domestic or international terrorism. In each case, the transferring governmental entity must certify that there is reason to believe that the financial records are relevant to such an activity, investigation, or analysis. "Finally, this section facilitates government

Access to Law Enforcement Information

Shortly after September 11, sources within both Congress and the Administration stressed the need for law enforcement and intelligence agencies to more effectively share information about terrorists and their activities. On September 14, the Senate Select Committee on Intelligence observed that, "effective sharing of information between and among the various components of the government-wide effort to combat terrorists is also essential, and is presently hindered by cultural, bureaucratic, resource, training and, in some cases, legal obstacles," H.R. Rep. No. 107-63, at 10 (2001). The Justice Department's consultation draft of September 20 offered three sections which would have greatly expanded the intelligence community's access to information collected as part of a criminal investigation. First, it suggested that information generated through the execution of a Title III order might be shared in connection with the duties of any executive branch official, Draft at §103.[3373]

Second, it recommended a change in Rule 6(e) of the Federal Rules of Criminal Procedure that would allow disclosure of grand jury material to intelligence officials, Draft at §354.[3374]

---

access to information contained in suspected terrorists' credit reports when the governmental inquiry relates to an investigation of, or intelligence activity or analysis relating to, domestic or international terrorism. Even though private entities such as lenders and insurers can access an individual's credit history, the government is strictly limited in its ability under current law to obtain the information. This section would permit those investigating suspected terrorists prompt access to credit histories that may reveal key information about the terrorist's plan or source of funding--without notifying the target. To obtain the information, the governmental authority must certify to the credit bureau that the information is necessary to conduct a terrorism investigation or analysis. The amendment would also create a safe harbor from liability for credit bureaus acting in good faith that comply with a government agency's request for information").

[3373] See also, DoJ at §103, "This section facilities the disclosure of Title III information to other components of the intelligence community in terrorism investigations. At present, 18 U.S.C. §2517(1) generally allows information obtained via wiretap to be disclosed only to the extent that it will assist a criminal investigation. One must obtain a court order to disclose Title III information in non-criminal proceedings. Section 109 [103] would modify the wiretap statutes to permit the disclosure of Title III-generated information to a non-law enforcement officer for such purposes as furthering an intelligence investigation. This will harmonize Title III standards with those of the Foreign Intelligence Surveillance Act (FISA), which allows such information-sharing. Allowing disclosure under Title III is particularly appropriate given that the requirements for obtaining a Title III surveillance order in general are more stringent than for a FISA order, and because the attendant privacy concerns in either situation are similar and are adequately protected by existing statutory provisions."

[3374] See also, DoJ at §354, "This section makes changes in Rule 6(e) of the Federal Rules of Criminal Procedure, relating to grand jury secrecy, to facilitate the sharing of information with federal law enforcement, intelligence, protective, national defense, and immigration personnel in terrorism and national security cases. The section is in part complimentary to section 154 of the bill, relating to sharing of foreign intelligence information, and reflects a similar purpose of promoting a coordinated governmental response to terrorist and national security threats."

Third, it proposed elimination of all constraints on sharing foreign intelligence information uncovered during a law enforcement investigation, mentioning by name the constraints in Rule 6(e) and Title III, Draft at §154.[3375]

The Act combines versions of all three in section 203. Perhaps because of the nature of the federal grand jury, resolution of the grand jury provision proved especially difficult. The federal grand jury is an exceptional institution. Its purpose is to determine if a crime has been committed, and if so by whom; to indict the guilty; and to refuse to indict the innocent. Its probes may begin without probable cause or any other threshold of suspicion.[3376] It examines witnesses and evidence ordinarily secured in its name and questioned before it by Justice Department prosecutors. Its affairs are conducted in private and outside the presence of the court. Only the attorney for the government, witnesses under examination, and a court reporter may attend its proceedings, F.R. Crim. P. 6(d). Matters occurring before the grand jury are secret and may be disclosed by the attending attorney for the government and those assisting the grand jury only in the performance of their duties; in presentation to a successor grand jury; or under court order for judicial proceedings, for inquiry into misconduct before the grand jury, or for state criminal proceedings, F.R.Crim.P. 6(e).

The Act, in section 203(a), allows disclosure of matters occurring before the grand jury to "any federal law enforcement, intelligence, protective, immigration,

---

Contrary to the implication here section 154 deals with sharing information gathered by law enforcement officials not with information gathered by intelligence officers

[3375] See also, DoJ at §154, "This section provides that foreign intelligence information obtained in criminal investigations, including grand jury and electronic surveillance information, may be shared with other federal government personnel having responsibilities relating to the defense of the nation and its interests. With limited exceptions, it is presently impossible for criminal investigators to share information obtained through a grand jury (including through the use of grand jury subpoenas) and information obtained from electronic surveillance authorized under Title III with the intelligence community. This limitation will be very significant in some criminal investigations. For example, grand jury subpoenas often are used to obtain telephone, computer, financial and other business records in organized crime investigations. Thus, these relatively basic investigative materials are inaccessible for examination by intelligence community analysts working on related transnational organized crime groups. A similar problem occurs in computer intrusion investigations: grand jury subpoenas and Title III intercepts are used to collect transactional data and to monitor the unknown intruders. The intelligence community will have an equal interest in such information, because the intruder may be acting on behalf of a foreign power."

[3376] Blair v. United States, 250 U.S. 273, 281 (1919)(the grand jury "is a grand inquest, a body with powers of investigation and inquisition, the scope of whose inquiries is not to be limited narrowly by questions of propriety or forecasts of whether any particular individual will be found properly subject to an accusation of crime").

national defense, or national security" officer to assist in the performance of his official duties, F.R.Crim.P. 6(e)(3)(C)(i)(V).[3377]

Critics may protest that the change could lead to the use of the grand jury for intelligence gathering purposes, or less euphemistically, to spy on Americans.[3378] The proposal was never among those scheduled to sunset, but earlier versions of the section followed the path used for most other disclosures of grand jury material: prior court approval, H.R.Rep.No. 107-236, at 73 (2001). The Act, in section 203(a), instead calls for confidential notification of the court that a disclosure has occurred and the entity to whom it was made, F.R. Crim. P. 6(e)(3)(C)(iii). It also insists that the Attorney General establish implementing procedures for instances when the disclosure "identifies" Americans (U.S. persons), section 203(c).

[3377] These officers may receive: (1) "foreign intelligence information" that is, information regardless whether it involves Americans or foreign nationals that "[a] relates to the ability of the United States to protect against – (aa) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power; (bb) sabotage or international terrorism by a foreign power or an agent of a foreign power; (cc) clandestine intelligence activities by an intelligence service or network of a foreign power;" or [b] "with respect to a foreign power or foreign territory that relates to – (aa) the national defense or security of the United States; or (bb) the conduct of the foreign affairs of the United States," F.R.Crim.P. 6(e)(3)(C)(iv); (2) when the matters involve foreign intelligence or counterintelligence, that is, [a] "information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities" or [b] "information gathered and activities conducted, to protect against espionage, other intelligence activities, sabotage, or assassinations conducted on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities," 50 U.S.C. 401a(2),(3)(language added by section 902 of the Act in italics).

[3378] Beale & Felman, The Consequences of Enlisting Federal Grand Juries in the War on Terrorism: Assessing the USA PATRIOT Act's Changes to Grand Jury Secrecy, 25 HARVARD JOURNAL OF LAW & PUBLIC POLICY 699, 719-20 (2002)("There is a significant danger that the rule permitting disclosure will be treated as the de facto authorization of an expansion of the grand jury's investigative role to encompass seeking material relevant only to matters of national security, national defense, immigration, and so forth. The grand jury's awesome powers should not be unwittingly extended to a much wider range of issues. . . Since the grand jury operates in secret, there are no public checks on the scope of its investigations, and witnesses are not permitted to challenge its jurisdiction. Only the supervising court is in a position to keep the grand jury's investigation within proper bounds. Requiring judicial approval of foreign intelligence and counterintelligence information disclosures would provide a natural check against the temptation to manipulate the grand jury to develop information for unauthorized purposes"); but see, Scheidegger et al., Federalist Society White Paper on The USA PATRIOT Act of 2001: Criminal Procedure Sections 6 (Nov. 2001)("The grand jury secrecy rule is a rule of policy which has always had exceptions, and it has been frequently modified. The secrecy rule has no credible claim to constitutional stature").

Law enforcement officials may share Title III information with the intelligence community under the same conditions, section 203(b),[3379] although the grand jury and Title III sharing provisions differ in at least three important respects. The court need not be notified of Title III disclosures. On the other hand, the authority for sharing Title III information expires on December 31, 2005, section 224, and agencies and their personnel guilty of intentional improper disclosures may be subject to a claim for damages and disciplinary action, 18 U.S.C. 2520.

The third subsection of section 203 remains something of an enigma. It speaks in much the same language as its counterparts. It allows law enforcement officials to share information with the intelligence community, "notwithstanding any other provisions of law," section 203(d).[3380] It either swallows the other subsections, or supplements them. Several factors argue for its classification as a supplement. Congress is unlikely to have crafted subsections (a), (b) and (c) only to completely nullify them in subsection (d). Without a clear indication to the contrary, the courts are unlikely to find that Congress intended nullification.[3381] By gathering

---

[3379] Information derived from a Title III interception may be shared with any other federal law enforcement, intelligence, protective, immigration, national defense, or national security officer if it regards: (1) "foreign intelligence information" that is, information irrespective of whether it involves Americans or foreign nationals that "[A] relates to the ability of the United States to protect against – (i) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power; (ii) sabotage or international terrorism by a foreign power or an agent of a foreign power; (iii) clandestine intelligence activities by an intelligence service or network of a foreign power;" or [B] "with respect to a foreign power or foreign territory that relates to – (i) the national defense or security of the United States; or (ii) the conduct of the foreign affairs of the United States;" (2) when the matters involve foreign intelligence or counterintelligence as defined by 50 U.S.C. 401a (as amended by section 902 of the Act), i.e., "As used in this Act: (1) The term 'intelligence' includes foreign intelligence and counterintelligence. (2) The term 'foreign intelligence' means information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities. (3) The term 'counterintelligence' means information gathered and activities conducted, to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities" (language added by section 902 in italics).

[3380] "Notwithstanding any other provision of law, it shall be lawful for foreign intelligence or counterintelligence (as defined in section 3 of the National Security Act of 1947 (50 U.S.C.) or foreign intelligence information obtained as part of a criminal investigation to be disclosed to any federal law enforcement, intelligence, protective, immigration, national defense, or national security official in order to assist the official receiving that information in the performance of his official duties. Any federal official who receives information pursuant to this provision may use that information only as necessary in the conduct of that person's official duties subject to any limitations on the unauthorized disclosure of such information," §203(d)(1). The subsection goes to define "foreign intelligence information" in the same terms used to define that phrase in Title III (18 U.S.C. 2510(19)) and in Rule 6(e)(F.R.Crim.P.6(e)(3)(C)(iv)), §203(d)(2).

[3381] Duncan v. Walker, 121 S.Ct. 2120, 2125 (2001)(internal quotation marks and parallel citations omitted)("It is our duty to give effect, if possible, to every clause and word of a statute. United States v. Menasche, 348 U.S. 528, 538-539 (1955) (quoting Montclair v. Ramsdell, 107 U.S. 147,

the three into a single section Congress avoided the suggestion that the phrase "notwithstanding any other provision of law" constitutes surplusage. The Title III and grand jury sharing procedures are not in other provisions of law, they are now subsections of the same provision of law. Moreover, Congress seemed to signal an intent for the subsections to operate in tandem when it dropped the language of the original Justice Department proposal which expressly identified Title III and Rule 6(e) as examples of the restrictions to be overcome by the universal sharing language.[3382]

Section 203 deals with earlier legal impediments to sharing foreign intelligence information unearthed during the course of a criminal investigation. Section 905 looks to dissolve the barriers may be more cultural than legal. Under it, the Attorney General is to issue guidelines governing the transmittal to the Director of Central Intelligence of foreign intelligence information that surfaces in the course of a criminal investigation. The section also instructs the Attorney General to promulgate guidelines covering reports to the Director of Central Intelligence on whether a criminal investigation has been initiated or declined based on an intelligence community referral, 50 U.S.C. 403-5b. To ensure effective use of increased information sharing, section 908 calls for training of federal, state and local officials to enable them to recognize foreign intelligence information which they encounter in their work and how to use it in the performance of their duties, 28 U.S.C. 509 note.

Increasing Institutional Capacity

As noted elsewhere, the Act liberalizes authority for the FBI to hire translators, section 203, which enhances its capacity to conduct both criminal and foreign intelligence investigations. The Act also reflects sentiments expressed earlier concerning coordinated efforts to develop a computerized translation capability

---

152 (1883)); see also Williams v. Taylor, 529 U.S. 362, 404 (2000) (describing this rule as a cardinal principle of statutory construction); Market Co. v. Hoffman, 101 U.S. 112, 115 (1879)(As early as in Bacon's Abridgment, sect. 2, it was said that a statute ought, upon the whole, to be so construed that, if it can be prevented, no clause, sentence, or word shall be superfluous, void, or insignificant). We are thus reluctant to treat statutory terms as surplusage in any setting. Babbitt v. Sweet Home Chapter, Communities for Great Ore., 515 U.S. 687, 698 (1995); see also Ratzlaf v. United States, 510 U.S. 135, 140 (1994)"). It is not possible to conclude that Congress intended the universal subsection (d) to apply until sunset and the grand jury and Title III subsections (a), (b), and (c) to operate thereafter, because the Title III subsection expires at the same time as the universal subsection.

[3382] Draft at §154, "Notwithstanding any other provision of law, it shall be lawful for foreign intelligence information obtained as part of a criminal investigation (including, without limitation, information subject to Rule 6(e) of the Federal Rules of Criminal Procedure and information obtained pursuant to chapter 119 of title 18, United States Code [i.e. Title III]) to be provided to any federal law enforcement, intelligence, protective, or national defense personnel, or any federal personnel responsible for administering the immigration laws of the United States, or to the President and the Vice President of the United States."

to be used in foreign intelligence gathering.[3383] Section 907 instructs the Director of the Central Intelligence, in consultation with the Director of the FBI, to report on the creation of a National Virtual Translation Center. The report is to include information concerning staffing, allocation of resources, compatibility with comparable systems to be used for law enforcement purposes, and features which permit its efficient and secure use by all of the intelligence agencies.

MONEY LAUNDERING

In federal law, money laundering is the flow of cash or other valuables derived from, or intended to facilitate, the commission of a criminal offense. It is the movement of the fruits and instruments of crime. Federal authorities attack money laundering through regulations, international cooperation, criminal sanctions, and forfeiture.[3384] The Act bolsters federal efforts in each area.

Regulation

Prior to passage of the Act, the Treasury Department already enjoyed considerable authority to impose reporting and record-keeping standards on financial institutions generally and with respect to anti-money laundering matters in particular.[3385]

[3383] "The Committee is concerned that intelligence in general, and intelligence related to terrorism in particular, is increasingly reliant on the ability of the Intelligence Community to quickly, accurately and efficiently translate information in a large number of languages. Many of the languages for which translation capabilities are limited within the United States Government are the languages that are of critical importance in our counterterrorism efforts. The Committee believes that this problem can be alleviated by applying cutting-edge, internet-like technology to create a 'National Virtual Translation Center.' Such a center would link secure locations maintained by the Intelligence Community throughout the country and would apply digital technology to network, store, retrieve, and catalogue the audio and textual information. Foreign intelligence could be collected technically in one location, translated in a second location, and provided to an Intelligence Community analyst in a third location. "The Committee notes that the CIA, FBI NSA and other intelligence agencies have applied new technology to this problem. The Committee believes that these efforts should be coordinated so that the solution can be applied on a Community-wide basis. Accordingly, the Committee directs the Director of Central Intelligence, in consultation with the Director of the FBI, and other heads of departments and agencies within the Intelligence Community, to prepare and submit to the intelligence committees by June 1, 2002, a report concerning the feasibility and structure of a National Virtual Translation Center, including recommendations regarding the establishment of such a center and the funding necessary to do so," S. Rep. No. 107-63, at 11 (2001).

[3384] For a brief overview, see, Murphy, Money Laundering: Current Law and Proposals, CRS REP.NO. RS21032 (DEC. 21, 2001).

[3385] See e.g,, 12 U.S.C. 1829b (retention or records by insured depository institutions), 1951-1959 (record-keeping by financial institutions); 31 U.S.C. 5311 ("It is the purpose of this subchapter [31 U.S.C. 5311 et seq.] (except section 5315 [relating to foreign current transaction reports]) to require certain reports or records where they have a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings").

For instance, under the Currency and Financial Transaction Reporting Act, a component of the Bank Secrecy Act, anyone who transports more than $10,000 into or out of the United States must report that fact to the Treasury Department, 31 U.S.C. 5316. Banks, credit unions, and certain other financial institutions must likewise report identifying information relating to cash transactions in excess of $10,000 to the Treasury Department (CTRs), 31 U.S.C. 5313, 31 C.F.R. §103.22. Other businesses are required to report to the Internal Revenue Service the particulars relating to any transaction involving more than $10,000 in cash, 26 U.S.C. 6050I. Banks must file suspicious activity reports (SARs) with the Treasury Department's Financial Crimes Enforcement Network (FinCEN) for any transactions involving more than $5,000 which they suspect may be derived from illegal activity, 31 U.S.C. 5318(g), 31 C.F.R. §103.18. Money transmission businesses and those that deal in traveler's checks or money orders are under a similar obligation for suspicious activities involving more than $2,000, 31 U.S.C. 5318(g), 31 C.F.R. §103.18.

Among other things, the Act expands the authority of the Secretary of the Treasury over these reporting requirements. He is to promulgate regulations, pursuant to sections 356 and 321, under which securities brokers and dealers as well as commodity merchants, advisors and pool operators must file suspicious activity reports, 31 U.S.C. 5318 note; 31 U.S.C. 5312(2)(c)(1). Businesses which were only to report cash transactions involving more than $10,000 to the IRS are now required to files SARs as well,[3386] reflecting Congress' view that the information provided the IRS may be valuable for other law enforcement purposes.[3387] This concern is likewise reflected in section 357 which asks the

---

[3386] Section 365, 31 U.S.C. 5331; Sec. 321, 31 U.S.C. 5312.

[3387] H.R.Rep.No. 107-250, at 38-9 (2001)("Most importantly, the Committee found significant shortcomings in the use of information already in possession of the government. Section 6050I of the Internal Revenue Code requires that any person engaged in a trade or business (other than financial institutions required to report under the Bank Secrecy Act) file a report with the Federal government on cash transactions in excess of $10,000. Reports filed pursuant to this requirement provide law enforcement authorities with a paper trail that can, among other things, lead to the detection and prosecution of money laundering activity. "Under current law, non-financial institutions are required to report cash transactions exceeding $10,000 to the Internal Revenue Service (IRS) on IRS Form 8300. Because the requirement that such reports be filed is contained in the Internal Revenue Code, Form 8300 information is considered tax return information, and is subject to the procedural and record-keeping requirements of section 6103 of the Internal Revenue Code. For example, section 6103(p)(4)(E) requires agencies seeking Form 8300 information to file a report with the Secretary of the Treasury that describes the procedures established and utilized by the agency for ensuring the confidentiality of the information. IRS requires that agencies requesting Form 8300 information file a 'Safeguard Procedures Report' which must be approved by the IRS before any such information can be released. For that reason, Federal, State and local law enforcement agencies are not given access to the Form 8300s as Congress anticipated when it last amended this statute. See 26 U.S.C. 6103(l)(15). "While the IRS uses Form 8300 to identify individuals who may be engaged in tax evasion, Form 8300

Secretary of the Treasury to report on the Internal Revenue Service's role in the administration of the Currency and Foreign Transaction Reporting Act (31 U.S.C. 5311 et seq.), and what transfers of authority, if any, are appropriate.

Sections 351 and 355 address the liability for disclosure of suspicious activity reports (SARs). Prior to the Act, federal law prohibited financial institutions and their officers and employees from tipping off any of the participants in a suspicious transaction, 31 U.S.C. 5318(g)(2)(2000 ed.). Federal law, however, immunized the institutions and their officers and employees from liability for filing the reports and for failing to disclose that they had done so, 31 U.S.C. 5318(g)(3)(2000 ed.). Section 351 makes changes in both the immunity and the proscription. It adds government officials who have access to the reports to the anti-tip ban, 31 U.S.C. 5318(g)(2)(A). It allows, but does not require, institutions to reveal SAR information in the context of employment references to other financial institutions, 31 U.S.C. 5318(g)(2)(B). Finally, it makes clear that the immunity does not extend to immunity from governmental action.[3388] Section

---

information can also be instrumental in helping law enforcement authorities trace cash payments by drug traffickers and other criminals for luxury cars, jewelry, and other expensive merchandise. Because of the restrictions on their dissemination outlined above, however, Form 8300s are not nearly as accessible to law enforcement authorities as the various reports mandated by the Bank Secrecy Act, which can typically be retrieved electronically from a database maintained by the Treasury Department. The differential access to the two kinds of reports is made anomalous by the fact that Form 8300 elicits much the same information that is required to be disclosed by the Bank Secrecy Act. For example, just as Form 8300 seeks the name, address, and social security number of a customer who engages in a cash transaction exceeding $10,000 with a trade or business, Currency Transaction Reports (CTRs) mandated by the Bank Secrecy Act require the same information to be reported on a cash transaction exceeding $10,000 between a financial institution and its customer").

[3388] "Subsection (a) of section [351] makes certain technical and clarifying amendments to 31 U.S.C. 5318(g)(3), the Bank Secrecy Act's 'safe harbor' provision that protects financial institutions that disclose possible violations of law or regulation from civil liability for reporting their suspicions and for not alerting those identified in the reports. The safe harbor is directed at Suspicious Activity Reports and similar reports to the government and regulatory authorities under the Bank Secrecy Act. "First, section [351](a) amends section 5318(g)(3) to make clear that the safe harbor from civil liability applies in arbitration, as well as judicial, proceedings. Second, it amends section 5318(g)(3) to clarify the safe harbor's coverage of voluntary disclosures (that is, those not covered by the SAR regulatory reporting requirement). The language in section 5318(g)(3)(A) providing that 'any financial institution that * * * makes a disclosure pursuant to * * * any other authority * * * shall not be liable to any person' is not intended to avoid the application of the reporting and disclosure provisions of the Federal securities laws to any person, or to insulate any issuers from private rights of actions for disclosures made under the Federal securities laws. "Subsection [351](b) amends section 5318(g)(2) of title 31--which currently prohibits notification of any person involved in a transaction reported in a SAR that a SAR has been filed--to clarify (1) that any government officer or employee who learns that a SAR has been filed may not disclose that fact to any person identified in the SAR, except as necessary to fulfill the officer or employee's official duties, and (2) that disclosure by a financial institution of potential wrongdoing in a written employment reference provided in response to a request from another financial institution pursuant to section 18(v) of the Federal Deposit Insurance Act, or in a written termination notice or employment reference provided in accordance with the rules of a

355 expands the immunity to cover disclosures in employment references to other insured depository financial institutions provided disclosure is not done with malicious intent.[3389]

The Financial Crimes Enforcement Network (FinCEN), a component within the Treasury Department long responsible for these anti-money laundering reporting and record-keeping requirements, 31 C.F.R. pt. 103, was administratively created in 1990 to provide other government agencies with an "intelligence and analytical network in support of the detection, investigation, and prosecution of domestic and international money laundering and other financial crimes," 55 Fed.Reg. 18433 (May 2, 1990).

The Act, in section 361, makes FinCEN a creature of statute, a bureau within the Treasury Department, 31 U.S.C. 310. Section 362 charges it with the responsibility of establishing a highly secure network to allow financial institutions to file required reports electronically and to permit FinCEN to provide those institutions with alerts and other information concerning money laundering protective measures, 31 U.S.C. 310 note.

Special Measures

In extraordinary circumstances involving international financial matters, the Act grants the Secretary of the Treasury, in consultation with other appropriate regulatory authorities, the power to issue regulations and orders involving additional required "special measures" and additional "due diligence" requirements to combat money laundering. The special measure authority, available under section 311, comes to life with the determination that particular institutions, jurisdictions, types of accounts, or types of transactions pose a primary money laundering concern.[3390] These special measures may require U.S. financial institutions to:

---

securities self-regulatory organization, is not prohibited simply because the potential wrongdoing was also reported in a SAR," H.R.Rep.No. 107-250, at 66 (2001).

[3389] 31 U.S.C. 1828(w). "This section deals with the same employment reference issue addressed in section [351] but with respect to title 12. Occasionally banks develop suspicions that a bank officer or employee has engaged in potentially unlawful activity. These suspicions typically result in the bank filing a SAR. Under present law, however, the ability of banks to share these suspicions in written employment references with other banks when such an officer or employee seeks new employment is unclear. Section 208 would amend 12 U.S.C. 1828 to permit a bank, upon request by another bank, to share information in a written employment reference concerning the possible involvement of a current or former officer or employee in potentially unlawful activity without fear of civil liability for sharing the information, but only to the extent that the disclosure does not contain information which the bank knows to be false, and the bank has not acted with malice or with reckless disregard for the truth in making the disclosure," H.R.Rep.No. 107-250, at 67 (2001).

[3390] 31 U.S.C. 5318A. The circumstances considered in the case of a suspect jurisdiction are: evidence of organized crime or terrorist transactions there; the extent to which the jurisdiction's bank secrecy or other regulatory practices encourage foreign use; the extent and effectiveness of

- maintain more extensive records and submit additional reports relating to participants in foreign financial transactions with which they are involved
- secure beneficial ownership information with respect to accounts maintained for foreign customers
- adhere to "know-your-customer" requirements concerning foreign customers who use "payable-through accounts" held by the U.S. entity for foreign financial institutions
- keep identification records on foreign financial institutions' customers whose transactions are routed through the foreign financial institution's correspondent accounts with the U.S. financial institution
- honor limitations on correspondent or payable-through accounts maintained for foreign financial institutions.[3391]

---

the jurisdiction's banking regulation; the volume of financial transactions in relation to the size of the jurisdiction's economy; whether international watch dog groups (such as the Financial Action Task Force) have identified the jurisdiction as an offshore banking or secrecy haven; the existence or absence of a mutual legal assistance treaty between the U.S. and the jurisdiction; and the extent of official corruption within the jurisdiction. The institutional circumstances weighed before imposing special measures with respect to particular institutions or types of accounts or transactions include the intent to which the suspect institution or types of accounts or transactions are particularly attractive to money launderers, the extent to which they can be used by legitimate businesses, and the extent to which focused measures are likely to be successful.

[3391] The House report describes these measures in greater detail: "Section [311] adds a new section 5318A to the Bank Secrecy Act, authorizing the Secretary of the Treasury to require domestic financial institutions and agencies to take one or more of five 'special measures' if the Secretary finds that reasonable grounds exist to conclude that a foreign jurisdiction, a financial institution operating outside the United States, a class of international transactions, or one or more types of accounts is a 'primary money laundering concern.' Prior to invoking any of the special measures contained in section 5318A(b), the Secretary is required to consult with the Chairman of the Board of Governors of the Federal Reserve System, any other appropriate Federal banking agency, the Securities and Exchange Commission, the National Credit Union Administration Board, and, in the sole discretion of the Secretary, such other agencies and interested parties as the Secretary may find to be appropriate. Among other things, this consultation is designed to ensure that the Secretary possesses information on the effect that any particular special measure may have on the domestic and international banking system. In addition, the Committee encourages the Secretary to consult with non-governmental 'interested parties,' including, for example, the Bank Secrecy Act Advisory Group, to obtain input from those who may be subject to a regulation or order under this section. "Prior to invoking any of the special measures contained in section 5318A, the Secretary must consider three discrete factors, namely (1) whether other countries or multilateral groups have taken similar action; (2) whether the imposition of the measure would create a significant competitive disadvantage, including any significant cost or burden associated with compliance, for firms organized or licensed in the United States; and (3) the extent to which the action would have an adverse systemic impact on the payment system or legitimate business transactions. "Finally, subsection (a) makes clear that this new authority is not to be construed as superseding or restricting any other authority of the Secretary or any other agency. "Subsection (b) of the new section 5318A outlines the five 'special measures' the Secretary may invoke against a foreign jurisdiction, financial institution operating outside the U.S., class of transaction within, or involving, a jurisdiction outside the U.S., or one or more types of accounts, that he finds to be of primary money laundering concern. "The first such measure would require domestic financial institutions to maintain records and/or file reports on certain transactions

Due Diligence

Section 312 demands that all U.S. financial institutions have policies, procedures, and controls in place to identify instances where their correspondent and private banking accounts with foreign individuals and entities might be used for money laundering purposes, 31 U.S.C. 5318(i). They must establish enhanced due diligence standards for correspondent accounts held for offshore banking institutions (whose licenses prohibit them from conducting financial activities in

---

involving the primary money laundering concern, to include any information the Secretary requires, such as the identity and address of participants in a transaction, the legal capacity in which the participant is acting, the beneficial ownership of the funds (in accordance with steps that the Secretary determines to be reasonable and practicable to obtain such information), and a description of the transaction. The records and/or reports authorized by this section must involve transactions from a foreign jurisdiction, a financial institution operating outside the United States, or class of international transactions within, or involving, a foreign jurisdiction, and are not to include transactions that both originate and terminate in, and only involve, domestic financial institutions. "The second special measure would require domestic financial institutions to take such steps as the Secretary determines to be reasonable and practicable to ascertain beneficial ownership of accounts opened or maintained in the U.S. by a foreign person (excluding publicly traded foreign corporations) associated with what has been determined to be a primary money laundering concern. "The third special measure the Secretary could impose in the case of a primary money laundering concern would require domestic financial institutions, as a condition of opening or maintaining a 'payable-through account' for a foreign financial institution, to identify each customer (and representative of the customer) who is permitted to use or whose transactions flow through such an account, and to obtain for each customer (and representative) information that is substantially comparable to the information it would obtain with respect to its own customers. A 'payable-through account' is defined for purposes of the legislation as an account, including a transaction account (as defined in section 19(b)(1)(C) of the Federal Reserve Act), opened at a depository institution by a foreign financial institution by means of which the foreign financial institution permits its customers to engage, either directly or through a sub-account, in banking activities usual in connection with the business of banking in the United States. "The fourth special measure the Secretary could impose in the case of a primary money laundering concern would require domestic financial institutions, as a condition of opening or maintaining a 'correspondent' account for a foreign financial institution, to identify each customer (and representative of the customer) who is permitted to use or whose transactions flow through such an account, and to obtain for each customer (and representative) information that is substantially comparable to the information that it would obtain with respect to its own customers. With respect to a bank, the term 'correspondent account' means an account established to receive deposits from and make payments on behalf of a foreign financial institution. "The fifth measure the Secretary could impose in the case of a primary money laundering concern would prohibit or impose conditions (beyond those already provided for in the third and fourth measures) on domestic financial institutions' correspondent or payable-through accounts with foreign banking institutions. In addition to the required consultation with the Chairman of the Board of Governors of the Federal Reserve, prior to imposing this measure the Secretary is also directed to consult with the Secretary of State and the Attorney General. "The five special measures authorized by this section may be imposed in any sequence or combination as the Secretary determines. The first four special measures may be imposed by regulation, order, or otherwise as permitted by law. However, if the Secretary proceeds by issuing an order, the order must be accompanied by a notice of proposed rulemaking relating to the imposition of the special measure, and may not remain in effect for more than 120 days, except pursuant to a regulation prescribed on or before the end of the 120-day period. The fifth special measure may be imposed only by regulation," H.R. Rep. No. 107-250, at 68-9.

---

the jurisdiction in which they are licensed) or institutions in money laundering jurisdictions designated by the Secretary of the Treasury or by international watch dog groups such as the Financial Action Task Force. The standards must at least involve reasonable efforts to identify the ownership of foreign institutions which are not publicly held; closely monitor the accounts for money laundering activity; and to hold any foreign bank, for whom the U.S. institution has a correspondent account, to the same standards with respect to other correspondent accounts maintained by the foreign bank. In the case of private banking accounts of $1 million or more, U.S. financial institutions must keep records of the owners of the accounts and the source of funds deposited in the accounts. They must report suspicious transactions and, when the accounts are held for foreign officials, guard against transactions involving foreign official corruption.[3392]

[3392] See generally, H.R. Rep. No. 107-250, at 71-2 ("Section [312] amends 31 U.S.C. 5318 to require financial institutions that establish, maintain, administer, or manage private banking or correspondent accounts for non-U.S. persons to establish appropriate, specific, and, where necessary, enhanced due diligence policies, procedures, and controls to detect and report instances of money laundering through those accounts. "The section requires financial institutions to apply enhanced due diligence procedures when opening or maintaining a correspondent account for a foreign bank operating (1) under a license to conduct banking activities which, as a condition of the license, prohibits the licensed entity from conducting banking activities with the citizens of, or with the local currency of, the country which issued the license; or (2) under a license issued by a foreign country that has been designated (a) as non-cooperative with international anti-money laundering principles by an intergovernmental group or organization of which the United States is a member, with which designation the Secretary of the Treasury concurs, or (b) by the Secretary as warranting special measures due to money laundering concerns. "The enhanced due diligence procedures include (1) ascertaining the identity of each of the owners of the foreign bank (except for banks that are publicly traded); (2) conducting enhanced scrutiny of the correspondent account to guard against money laundering and report any suspicious activity; and (3) ascertaining whether the foreign bank provides correspondent accounts to other foreign banks and, if so, the identity of those foreign banks and related due diligence information. "For private banking accounts requested or maintained by a non-United States person, a financial institution is required to implement procedures for (1) ascertaining the identity of the nominal and beneficial owners of, and the source of funds deposited into, the account as needed to guard against money laundering and report suspicious activity; and (2) conducting enhanced scrutiny of any such account requested or maintained by, or on behalf of, a senior foreign political figure, or his immediate family members or close associates, to prevent, detect and report transactions that may involve the proceeds of foreign corruption. A private bank account is defined as an account (or any combination of accounts) that requires a minimum aggregate deposit of funds or other assets of not less than $1 million; is established on behalf of one or more individuals who have a direct or beneficial ownership in the account; and is assigned to, or administered or managed by, an officer, employee or agent of a financial institution acting as a liaison between the institution and the direct or beneficial owner of the account. "This section directs the Secretary of the Treasury, within 6 months of enactment of this bill and in consultation with appropriate Federal functional regulators, to further define and clarify, by regulation, the requirements imposed by this section").

The Act establishes several other regulatory mechanisms directed at the activities involving U.S. financial institutions and foreign individuals or institutions. Section 313, for instance, in another restriction on correspondent accounts for foreign financial institutions, prohibits U.S. financial institutions from maintaining correspondent accounts either directly or indirectly for foreign shell banks (banks with no physical place of business[3393]) which have no affiliation with any financial institution through which their banking activities are subject to regulatory supervision.[3394]

The Act, in section 325, empowers the Secretary of the Treasury to promulgate regulations to prevent financial institutions from allowing their customers to conceal their financial activities by taking advantage of the institutions' concentration account practices.[3395]

The Secretary of the Treasury is instructed in section 326 to issue regulations for financial institutions' minimum new customer identification standards and record-keeping and to recommend a means to effectively verify the identification of foreign customers.[3396]

[3393] Or more exactly, a bank which has no physical presence in any country; a "physical presence" for a foreign bank is defined as "a place of business that – (i) is maintained by a foreign bank; (ii) is located at a fixed address (other than solely an electronic address) in a country in which the foreign bank is authorized to conduct banking activities, at which location the foreign bank – (I) employs 1 or more individuals on a full-time basis; and (II) maintains operating records relating to its banking activities; and (iii) is subject to inspection by the banking authority which licensed the foreign bank to conduct banking activities," 31 U.S.C. 5318(j)(4).

[3394] 31 U.S.C. 5318(j); H.R.Rep.No. 107-250, at 72 (2001).

[3395] The Act does not define "concentration accounts," although the House Financial Services Committee report provides some incite into the section's intent, H.R.Rep.No. 107-250, at 72-3 (2001)("This section gives the Secretary of the Treasury discretionary authority to prescribe regulations governing the maintenance of concentration accounts by financial institutions, to ensure that these accounts are not used to prevent association of the identity of an individual customer with the movement of funds of which the customer is the direct or beneficial owner. If promulgated, the regulations are required to prohibit financial institutions from allowing clients to direct transactions into, out of, or through the concentration accounts of the institution; prohibit financial institutions and their employees from informing customers of the existence of, or means of identifying, the concentration accounts of the institution; and to establish written procedures governing the documentation of all transactions involving a concentration account.")

[3396] 31 U.S.C. 5318(l); H.R.Rep.No. 107-250, at 62-3 (2001)("Section [326](a) amends 31 U.S.C. 5318 by adding a new subsection governing the identification of account holders. Paragraph (1) directs Treasury to prescribe regulations setting forth minimum standards for customer identification by financial institutions in connection with the opening of an account. By referencing 'customers' in this section, the Committee intends that the regulations prescribed by Treasury take an approach similar to that of regulations promulgated under title V of the Gramm-Leach-Bliley Act of 1999, where the functional regulators defined 'customers' and 'customer

Federal regulatory authorities must approve the merger of various financial institutions under the Bank Holding Company Act, 12 U.S.C. 1842, and the Federal Deposit Insurance Act, 12 U.S.C. 1828. Section 327 requires consideration of an institution's anti-money laundering record when such mergers are proposed, 12 U.S.C. 1842(c)(6), 1828(c)(11).

Section 314 directs the Secretary of the Treasury to promulgate regulations in order to encourage financial institutions and law enforcement agencies to share information concerning suspected money laundering and terrorist activities, 31 U.S.C. 5311 note.

---

relationship' for purposes of the financial privacy rules. Under this approach, for example, where a mutual fund sells its shares to the public through a broker-dealer and maintains a 'street name' or omnibus account in the broker-dealer's name, the individual purchasers of the fund shares are customers of the broker-dealer, rather than the mutual fund. The mutual fund would not be required to 'look through' the broker-dealer to identify and verify the identities of those customers. Similarly, where a mutual fund sells its shares to a qualified retirement plan, the plan, and not its participants, would be the fund's customers. Thus, the fund would not be required to 'look through' the plan to identify its participants. "Paragraph (2) requires that the regulations must, at a minimum, require financial institutions to implement procedures to verify (to the extent reasonable and practicable) the identity of any person seeking to open an account, maintain records of the information used to do so, and consult applicable lists of known or suspected terrorists or terrorist organizations. The lists of known or suspected terrorists that the Committee intends financial institutions to consult are those already supplied to financial institutions by the Office of Foreign Asset Control (OFAC), and occasionally by law enforcement and regulatory authorities, as in the days immediately following the September 11, 2001, attacks on the World Trade Center and the Pentagon. It is the Committee's intent that the verification procedures prescribed by Treasury make use of information currently obtained by most financial institutions in the account opening process. It is not the Committee's intent for the regulations to require verification procedures that are prohibitively expensive or impractical. "Paragraph (3) requires that Treasury consider the various types of accounts maintained by various financial institutions, the various methods of opening accounts, and the various types of identifying information available in promulgating its regulations. This would require Treasury to consider, for example, the feasibility of obtaining particular types of information for accounts opened through the mail, electronically, or in other situations where the accountholder is not physically present at the financial institution. Millions of Americans open accounts at mutual funds, broker-dealers, and other financial institutions in this manner; it is not the Committee's intent that the regulations adopted pursuant to this legislation impose burdens that would make this prohibitively expensive or impractical. This provision allows Treasury to adopt regulations that are appropriately tailored to these types of accounts. "Current regulatory guidance instructs depository institutions to make reasonable efforts to determine the true identity of all customers requesting an institution's services. (See, e.g., FDIC Division of Supervision Manual of Exam Policies, section 9.4 VI.) The Committee intends that the regulations prescribed under this section adopt a similar approach, and impose requirements appropriate to the size, location, and type of business of an institution. "Paragraph (4) requires that Treasury consult with the appropriate functional regulator in developing the regulations. This will help ensure that the regulations are appropriately tailored to the business practices of various types of financial institutions, and the risks that such practices may pose. "Paragraph (5) gives each functional regulator the authority to exempt, by regulation or order, any financial institution or type of account from the regulations prescribed under paragraph (1). "Paragraph (6) requires that Treasury's regulations prescribed under paragraph (1) become effective within one year after enactment of this bill").

Section 319(b) requires U.S. financial institutions to respond to bank regulatory authorities' requests for anti-money laundering records (within 120 hours) and to Justice or Treasury Department subpoenas or summons for records concerning foreign deposits (within 7 days), 31 U.S.C. 5318(k). Section 319 also calls for civil penalties of up to $10,000 a day for financial institutions who have failed to terminate correspondent accounts with foreign institutions that have ignored Treasury or Justice Department subpoenas or summons, 31 U.S.C. 5318(k)(3).

Section 352 directs the Secretary of the Treasury to promulgate regulations, in consultation with other appropriate regulatory authorities, requiring financial institutions to maintain anti-money laundering programs which must include at least a compliance officer; an employee training program; the development of internal policies, procedures and controls; and an independent audit feature.[3397]

Section 359 subjects money transmitters to the regulations and requirements of the Currency and Foreign Transactions Reporting Act (31 U.S.C. 5311 et seq.) and directs the Secretary of the Treasury to report on the need for additional legislation relating to domestic and international underground banking systems.

Federal law obligates the Administration to develop a national strategy for combating money laundering and related financial crimes, 31 U.S.C. 5341. Section 354 insists that the strategy contain data relating to the funding of international terrorism and efforts to prevent, detect, and prosecute such funding, 31 U.S.C. 5341(b)(12).

Section 364 authorizes the Board of Governors of the Federal Reserve to hire guards to protect members of the Board, as well as the Board's property and personnel and that of any Federal Reserve bank. The guards may carry firearms and make arrests, 12 U.S.C. 248(q).

Reports to Congress

Section 366 instructs the Secretary of the Treasury to report on methods of improving the compliance of financial institutions with the currency transaction reporting requirements and on the possibility of expanding exemptions to the requirements with an eye to improving the quality of data available for law enforcement purposes and reducing the number of unnecessary filings.[3398]

Section 324 instructs the Secretary of the Treasury to report on the execution of authority granted under the International Counter Money Laundering and

---

[3397] 31 U.S.C. 5318(h); H.R.Rep.No. 107-250, at 72 (2001).

[3398] 31 U.S.C. 5313 note; H.R.Rep.No. 107-205, at 65 (2001).

Related Measures subtitle (III-A) of the Act and to recommend any appropriate related legislation, 31 U.S.C. 5311 note.

International Cooperation

Reflecting concern about the ability of law enforcement officials to trace money transfers to this country from overseas, section 328 instructs the Secretary of the Treasury, Secretary of State and Attorney General to make every effort to encourage other governments to require identification of the originator of international wire transfers.[3399]

Section 330 expresses the sense of the Congress that the Administration should seek to negotiate international agreements to enable U.S. law enforcement officials to track the financial activities of foreign terrorist organizations, money launderers and other criminals.

Section 360 authorizes the Secretary of the Treasury to direct the U.S. Executive Directors of the various international financial institutions (i.e., the International Monetary Fund, the International Bank for Reconstruction and Development, the European Bank for Reconstruction and Development, the International Development Association, the International Finance Corporation, the Multilateral Investment Guarantee Agency, the African Development Bank, the African Development Fund, the Asian Development Bank, the Bank for Economic Development and Cooperation in the Middle East and North Africa, and the InterAmerican Investment Corporation): (1) to support the loan and other benefit efforts on behalf of countries that the President determines have supported our anti-terrorism efforts, and (2) to vote to ensure that funds from those institutions are not used to support terrorism.

[3399] H.R. Rep. No. 107-250, at 67 (2001)("This section directs the Secretary of the Treasury, in consultation with the Attorney General and the Secretary of State, to (1) take all reasonable steps to encourage foreign governments to require the inclusion of the name of the originator in wire transfer instructions sent to the U.S. and other countries; and (2) report annually to Congress on Treasury's progress in achieving this objective, and on impediments to instituting a regime in which all appropriate identification about wire transfer recipients is included with wire transfers from their point of origination until disbursement. "The Committee is concerned that inadequate information on the originator of wire transfers from a number of foreign jurisdictions makes it difficult for both law enforcement and financial institutions to properly understand the source of funds entering the United States in wire transfers. Such a lack of clarity could aid money launderers or terrorists in moving their funds into the United States financial system. Additionally, while arguments have been made that there are technical impediments to requiring that complete addressee information appear on all wire transfers terminating in or passing through the United States, the Committee believes that having such information is technically feasible and would aid both financial institutions in performing due diligence and law enforcement in tracking or seizing money that is the derivative of or would be used in the commission of a crime").

Crimes

Federal criminal money laundering statutes punish both concealing the fruits of old offenses and financing new ones. They proscribe financial transactions which:

- involve more than $10,000 derived from one of a list of specified underlying crimes, 18 U.S.C. 1957, or
- are intended to promote any of the designated predicate offenses, or
- are intended to evade taxes, or
- are designed to conceal the proceeds generated by any of the predicate offenses, or
- are crafted to avoid transaction reporting requirements, 18 U.S.C. 1956.

They also condemn transporting funds into, out of, or through the United States with the intent to further a predicate offense, conceal its proceeds, or evade reporting requirements, 18 U.S.C. 1956. Offenders face imprisonment for up to twenty years, fines of up to $500,000, civil penalties, 18 U.S.C. 1956, 1957, and confiscation of the illicit funds involved in a violation or in any of the predicate offenses, 18 U.S.C. 981, 982.

The Act contains a number of new money laundering crimes, as well as amendments and increased penalties for existing crimes. Section 315, for example, adds several crimes to the federal money laundering predicate offense list of 18 U.S.C. 1956. The newly added predicate offenses include crimes in violation of the laws of the other nations when the proceeds are involved in financial transactions in this country: crimes of violence, public corruption, smuggling, and offenses condemned in treaties to which we are a party, 18 U.S.C. 1956(c)(7)(B). Additional federal crimes also join the predicate list:

- 18 U.S.C. 541 (goods falsely classified)
- 18 U.S.C. 922(1) (unlawful importation of firearms)
- 18 U.S.C. 924(n) (firearms trafficking)
- 18 U.S.C. 1030 (computer fraud and abuse)
- felony violations of the Foreign Agents Registration Act, 22 U.S.C. 618.

As the report accompanying H.R. 3004 explains:

> *This amendment enlarges the list of foreign crimes that can lead to money laundering prosecutions in this country when the proceeds of additional foreign crimes are laundered in the United States. The additional crimes include all crimes of violence, public corruption, and offenses covered by existing bilateral extradition treaties. The Committee intends this provision to send a strong signal that the United States will not tolerate the use of its financial institutions for the purpose of laundering the proceeds of such activities. H.R. Rep. No. 107-250, at 55 (2000).*

In this same vein, section 376 adds the crime of providing material support to a terrorist organization (18 U.S.C. 2339B) to the predicate offense list and section 318 expands 18 U.S.C. 1956 to cover financial transactions conducted in foreign financial institutions.[3400]

Section 329 makes it a federal crime to corruptly administer the money laundering regulatory scheme. Offenders are punishable by imprisonment for not more than 15 years and a fine of not more than three times the amount of the bribe.

Section 5326 of title 31 authorizes the Secretary of the Treasury to impose temporary, enhanced reporting requirements upon financial institutions in areas victimized by substantial money laundering activity (geographic targeting regulations and orders). Section 353 makes it clear that the civil sanctions, criminal penalties, and prohibitions on smurfing (structuring transactions to evade reporting requirements) apply to violations of the regulations and orders issued under 31 U.S.C. 5326.[3401] It also extends the permissible length of the temporary geographical orders from 60 to 180 days.

Violations of the special measures and special due diligence requirements of sections 311 and 312 are subject to both civil and criminal penalties by virtue of section 363's amendments to 31 U.S.C. 5321(a) and 5322. The amendments authorize civil penalties and criminal fines of twice the amount of the transaction

---

[3400] "[S]ection 1956 of title 18, United States Code, makes it an offense to conduct a transaction involving a financial institution if the transaction involves criminally derived property. Similarly, 18 U.S.C. 1957 creates an offense relating to the deposit, withdrawal, transfer or exchange of criminally derived funds 'by, to or through a financial institution.' For the purposes of both statutes, the term 'financial institution' is defined in 31 U.S.C. 5312. See 18 U.S.C. 1956(c)(6); 18 U.S.C. 1957(f). "The definition of 'financial institution' in 5312 does not explicitly include foreign banks. Such banks may well be covered because they fall within the meaning of 'commercial bank' or other terms in the statute, but as presently drafted, there is some confusion over whether the government can rely on section 5312 to prosecute an offense under either 1956 or 1957 involving a transaction through a foreign bank, even if the offense occurs in part in the United States. For example, if a person in the United States sends criminal proceeds abroad--say to a Mexican bank--and launders them through a series of financial transactions, the government conceivably could not rely on the definition of a 'financial institution' in 1956(c)(6) to establish that the transaction was a 'financial transaction' within the meaning of 1956(c)(4)(B) (defining a 'financial transaction' as a transaction involving the use of a 'financial institution'), or that it was a 'monetary transaction' within the meaning of 1957(f) (defining 'monetary transaction' as, inter alia, a transaction that would be a 'financial transaction' under 1956(c)(4)(B)). "Similarly, the money laundering laws in effect in most countries simply make it an offense to launder the proceeds of any crime, foreign or domestic. In the United States, however, the money laundering statute is violated only when a person launders the proceeds of one of the crimes set forth on a list of 'specified unlawful activities.' 18 U.S.C. 1956(c)(7). Currently only a handful of foreign crimes appear on that list. See 1956(c)(7)(B)," H.R.Rep.No. 107-250, at 38 (2000).

[3401] Cf., H.R.Rep.No. 107-250, at 57.

but not more than $1 million. Criminal offenders would be subject to a fine in the same amount.

Earlier federal law prohibited the operation of illegal money transmitting businesses, 18 U.S.C. 1960. Section 373 amends the proscription to make it clear that the prohibition must be breached "knowingly" and to cover businesses which are otherwise lawful but which transmit funds they know are derived from or intended for illegal activities. It also amends 18 U.S.C. 981(a)(1)(A) to permit civil forfeiture of property involved in a transaction in violation of 18 U.S.C. 1960.[3402]

Sections 374 and 375 of the Act seek to curtail economic terrorism by increasing and making more uniform the penalties for counterfeiting U.S. or foreign currency and by making it clear that the prohibitions against possession of counterfeiting paraphernalia extend to their electronic equivalents.[3403] They increase the maximum terms of imprisonment for violation of:

- 18 U.S.C. 471 (obligations or securities of the U.S.) from 15 to 20 years;

[3402] "The operation of an unlicensed money transmitting business is a violation of Federal law under 18 U.S.C. 1960. First, section 104 clarifies the scienter requirement in 1960 to avoid the problems that occurred when the Supreme Court interpreted the currency transaction reporting statutes to require proof that the defendant knew that structuring a cash transaction to avoid the reporting requirements had been made a criminal offense. See Ratzlaf v. United States, 114 S. Ct. 655 (1994). The proposal makes clear that an offense under 1960 is a general intent crime for which a defendant is liable if he knowingly operates an unlicensed money transmitting business. For purposes of a criminal prosecution, the Government would not have to show that the defendant knew that a State license was required or that the Federal registration requirements promulgated pursuant to 31 U.S.C. 5330 applied to the business. "Second, section 104 expands the definition of an unlicensed money transmitting business to include a business engaged in the transportation or transmission of funds that the defendant knows are derived from a criminal offense, or are intended to be used for an unlawful purpose. Thus, a person who agrees to transmit or to transport drug proceeds for a drug dealer, or funds from any source for a terrorist, knowing such funds are to be used to commit a terrorist act, would be engaged in the operation of an unlicensed money transmitting business. It would not be necessary for the Government to show that the business was a storefront or other formal business open to walk-in trade. To the contrary, it would be sufficient to show that the defendant offered his services as a money transmitter to another. "Finally, when Congress enacted 1960 in 1992, it provided for criminal but not civil forfeiture. The proposal corrects this oversight, and allows the government to obtain forfeiture of property involved in the operation of an illegal money transmitting business even if the perpetrator is a fugitive," H.R.Rep.No. 107-250, at 54 (2001).

[3403] "This section makes it a criminal offense to possess an electronic image of an obligation or security document of the United States with intent to defraud. The provision harmonizes counterfeiting language to clarify that possessing either analog or digital copies with intent to defraud constitutes an offense. This section mimics existing language that makes it a felony to possess the plates from which currency can be printed, and takes into account the fact that most counterfeit currency seized today is generated by computers or computer-based equipment. The section also increases maximum sentences for a series of counterfeiting offenses," H.R.Rep.No. 107-250, at 75-6 (2001).

- 18 U.S.C. 472 (uttering counterfeit obligations and securities) from 15 to 20 years;
- 18 U.S.C. 473 (dealing in counterfeit obligations and securities) from 10 to 20 years;
- 18 U.S.C. 476 (taking impressions of tools used for obligations and securities) from 10 to 25 years;
- 18 U.S.C. 477 (possessing or selling impressions of tools used for obligations or securities) from 10 to 25 years;
- 18 U.S.C. 484 (connecting parts of different notes) from 5 to 10 years;
- 18 U.S.C. 493 (bonds and obligations of certain lending agencies) from 5 to 10 years;
- 18 U.S.C. 478 (foreign obligations or securities) from 5 to 20 years;
- 18 U.S.C. 479 (uttering counterfeit foreign obligations or securities) from 3 to 20 years;
- 18 U.S.C. 480 (possessing counterfeit foreign obligations or securities) from 1 to 20 years;
- 18 U.S.C. 481 (plates, stones, or analog, digital, or electronic images for counterfeiting foreign obligations or securities) from 5 to 25 years;
- 18 U.S.C. 482 (foreign bank notes) from 2 to 20 years; and
- 18 U.S.C. 483 (uttering counterfeit foreign bank notes) from 1 to 20 years.

Aliens believed to have engaged in money laundering may not enter the United States, section 1006 (8 U.S.C. 1182(a)(2)(I)). The same section directs the Secretary of State to maintain a watchlist to ensure that they are not admitted, 8 U.S.C. 1182 note.

Bulk Cash

Customs officials ask travelers leaving the United States whether they are taking $10,000 or more in cash with them. Section 1001 of title 18 of the United States Code makes a false response punishable by imprisonment for not more than 5 years. Section 5322 of title 31 makes failure to report taking $10,000 or more to or from the United States punishable by the same penalties. The Act's bulk cash smuggling offense, section 371, augments these proscriptions with a somewhat unique feature, 31 U.S.C. 5332 – a criminal forfeiture of the smuggled cash in lieu of a criminal fine. The basic offense outlaws smuggling cash into or out of the United States. The concealment element of the offense seems to cover everything but in-sight possession as long as an amount $10,000 or more is carried in manner to evade reporting.[3404]

The section appears to be the product of reactions to the Supreme Court's decision in United States v. Bajakian, 524 U.S. 321 (1998). There officials had

---

[3404] "For purposes of this section, the concealment of currency on the person of any individual includes concealment in any article of clothing worn by the individual or in any luggage, backpack, or other container worn or carried by such individual," 31 U.S.C. 5332(a)(2).

confiscation $350,000 because Bajakian attempted to leave the country without declaring it, a violation of 31 U.S.C. 5322. In the view of the Court, the confiscation was grossly disproportionate to the gravity of the offense and consequently contrary to the Constitution's excessive fines clause, 524 U.S. at 337. The Committee Report accompanying H.R. 3004 explains the Justice Department's assurance that casting surreptitious removal of cash from the United States as a smuggling rather than a false reporting offense will avoid the adverse consequences of the Supreme Court's examination of forfeiture in false reporting cases under the Constitution's Excessive Fines Clause.[3405]

Section 5317 of title 31 once called for civil forfeiture of property traceable to a violation of 31 U.S.C. 5316 (reports on exporting or importing money instruments worth $10,000 or more). Section 372 of the Act recasts section 5317 to provide for civil and criminal forfeitures for violations of 31 U.S.C. 5316, of 31 U.S.C. 5313 (reports on domestic coins and currency transactions involving $10,000 or more) and of 31 U.S.C. 5324 (structuring transactions to evade reporting requirements (smurfing)).

Extraterritorial Jurisdiction

The Act makes 18 U.S.C. 1029, the federal statute condemning various crimes involving credit cards, PIN numbers and other access devices, applicable overseas if the card or device is issued by or controlled by an American bank or other entity and some article is held in or transported to or through the United States during the course of the offense, section 377. The change was part of the original

---

[3405] "As recent Congressional hearings have demonstrated, currency smuggling is an extremely serious law enforcement problem. Hundreds of millions of dollars in U.S. currency – representing the proceeds of drug trafficking and other criminal offenses – is annually transported out of the United States to foreign countries in shipments of bulk cash. Smugglers use all available means to transport the currency out of the country, from false bottoms in personal luggage, to secret compartments in automobiles, to concealment in durable goods exported for sale abroad. . . . "Presently, the only law enforcement weapon against such smuggling is section 5316 of title 31, United States Code, which makes it an offense to transport more than $10,000 in currency or monetary instruments into, or out of, the United State without filing a report with the United States Customs Service. The effectiveness of section 5316 as a law enforcement tool has been diminished, however, by a recent Supreme Court decision. In United States v. Bajakajian, 118 S.Ct. 2028 (1998), the Supreme Court held that section 5316 constitutes a mere reporting violation, which is not a serious offense for purposes of the Excessive Fines Clause of the Eighth Amendment. Accordingly, confiscation of the full amount of the smuggled currency is unconstitutional, even if the smuggler took elaborate steps to conceal the currency and otherwise obstruct justice. "Confiscation of the smuggled currency is, of course, the most effective weapon that can be employed against currency smugglers. Accordingly, in response to the Bajakajian decision, the Department of Justice proposed making the act of bulk cash smuggling itself a criminal offense, and to authorize the imposition of the full range of civil and criminal sanctions when the offense is discovered. Because the act of concealing currency for the purpose of smuggling it out of the United States is inherently more serious than simply failing to file a Customs report, strong and meaningful sanctions, such as confiscation of the smuggled currency, are likely to withstand Eighth Amendment challenges to the new statute," H.R.Rep.No. 107-250 at 36-7 (2001).

Justice Department proposals. Justice explained that, "[financial crime[] admits of no border, utilizing the integrated global financial network for ill purposes. This provision would apply the financial crimes prohibitions to conduct committed abroad, so long as the tools or proceeds of the crimes pass through or are in the United States," DoJ at §408. The section, however, appears to limit the otherwise applicable extraterritorial jurisdiction implicit in section 1029, since federal courts would likely recognize extraterritorial jurisdiction over a violation under either circumstance (issued by a U.S. entity or physical presence in the U.S.) as well as a number of others.[3406]

Venue

Section 1004 relies on dicta in United States v. Cabrales, 524 U.S. 1, 8 (1998), in order to permit a money laundering prosecution to be brought in the place where the crime which generated the funds occurred, "if the defendant participated in the transfer of the proceeds," 18 U.S.C. 1956(i).

Ordinarily, the Constitution requires that a crime be prosecuted in the state and district in which it occurs, in the case of money laundering,[3407] in the state and district in which the monetary transaction takes place. The Supreme Court in Cabrales held that a charge of money laundering in Florida, of the proceeds of a Missouri drug trafficking, could not be tried in Missouri. The Court declared in dicta, however, that "money laundering . . . arguably might rank as a continuing offense, triable in more than one place, if the launderer acquired the funds in one district and transported them into another," 524 U.S. at 8.[3408]

[3406] United States v. Bowman, 260 U.S. 94, 97-8 (1922); Ford v. United States, 273 U.S. 593, 623 (1927). For a general discussion of the extraterritorial application of federal criminal law, see, Doyle, Extraterritorial Application of American Criminal Law, CRS REP.NO. 94-166A (Mar. 13, 1999).

[3407] "The trial of all crimes . . . shall be held in the state where the said crimes shall have been committed; but when not committed within any state, the trial shall be at such place or places as the Congress may by law have directed," U.S.Const. Art.III, §2, cl.3. "[I]n all criminal prosecutions, the accused shall enjoy the right to a speedy and public trial, by an impartial jury of the state and district wherein the crime shall have been committed; which district shall have been previously ascertained by law," U.S.Const. Amend. VI.

[3408] See also, United States v. Rodriguez-Moreno, 526 U.S. 275, 280-81 n.4 (1999) (holding that acquiring and using a firearm in Maryland in connection with a kidnaping in New Jersey might constitutionally be prosecuted in New Jersey under a statute which outlawed possession of a firearm "during and in relation to" a crime of violence.

Forfeiture

Forfeiture is the government confiscation of property as a consequence of crime.[3409] The forfeiture amendments of the Act fall into two categories. Some make adjustments to those portions of federal forfeiture law which govern the confiscation of property derived from, or used to facilitate, various federal crimes. Others follow the pattern used for the war-time confiscation of the property of enemy aliens under the Trading With the Enemy Act, 50 U.S.C. App. 1 et seq. (TWEA), forfeitures which turn on the ownership of the property rather than upon its proximity to any particular crime.

Constitutional Considerations

The Act adds TWEA-like amendments to the International Emergency Economic Powers Act (IEEPA), 50 U.S.C. 1701 et seq., which already allowed the President to freeze the assets of foreign terrorists under certain conditions. Under IEEPA, as amended by section 106 of the Act, the President or his delegate may confiscate and dispose of any property, within the jurisdiction of the United States, belonging to any foreign individual, foreign entity, or foreign country whom they determine to have planned, authorized, aided or engaged in an attack on the United States by a foreign country or foreign nationals. The section also permits the government to present secretly (ex parte and in camera) any classified information upon which the forfeiture was based should the decision be subject to judicial review. The Justice Department requested the section as a revival of the President's powers in times of unconventional wars.[3410] By virtue of

---

[3409] For general background information, see, Doyle, Crime and Forfeiture, CRS REP.NO. 97-139A (Oct. 11, 2000).

[3410] "This section is designed to accomplish two principal objectives. First, the section restores to the President, in limited circumstances involving armed hostilities or attacks against the United States, the power to confiscate and vest in the United States property of enemies during times of national emergency, which was contained in the Trading with the Enemy Act, 50 App. U.S.C. §5(b)(TWEA) until 1977. Until the International Economic Emergency Act (IEEPA) was passed in 1977, section 5(b) permitted the President to vest enemy property in the United States during time of war or national emergency. When IEEPA was passed, it did not expressly include a provision permitting the vesting of property in the United States, and section 5(b) of TWEA was amended to apply only 'during the time of war.' 50 App. U.S.C. §5(b). "This new provision tracks the vesting language currently in section 5(b) of TWEA and permits the President, only in the limited circumstances when the United States is engaged in military hostilities or has been subject to an attack, to confiscate property of any foreign country, person, or organization involved in hostilities or attacks on the United States. Like the original provision in TWEA, it is an exercise of Congress's war power under Article I, section 8, clause 11 of the Constitution and is designed to apply to unconventional warfare where Congress has not formally declared war against a foreign nation. "The second principal purpose of this amendment to IEEPA is to ensure that reviewing courts may base their rulings on an examination of the complete administrative record in sensitive national security or terrorism cases without requiring the United States to compromise classified information. New section (c) would authorize a reviewing court, in the process of verifying that determinations made by the executive branch were based upon substantial evidence and were not arbitrary or capricious, to consider classified evidence ex parte and in camera. This would ensure that reviewing courts have the best and most complete information upon which to

section 316, property owners may initiate a challenge to a confiscation by filing a claim under the rules applicable in maritime confiscations. The section permits two defenses to forfeiture – that the property is not subject to confiscation under section 106 or that the claimant is entitled to the innocent owner defense of 18 U.S.C. 983(d).[3411] The characterization of the defenses as "affirmative defense" indicates that the claimant bears the burden of proof. The innocent owner defenses of 18 U.S.C. 983(d) are probably not available in cases under section 106, since that section is explicitly excepted from the coverage of 18 U.S.C. 983.[3412] The challenge proceedings permit the court to admit evidence, such as hearsay evidence, that would not otherwise be admissible under the Federal Rules of Evidence if the evidence is reliable and if national security might be imperiled should dictates of the Federal Rules be followed, §316(b). The section recognizes the rights of claimants to proceed alternatively under the Constitution or the Administrative Procedure Act.[3413]

The Justice Department also recommended enactment of an overlapping provision which ultimately passed as section 806 of the Act without any real discussion of the relationship of the two sections.[3414] Section 806 authorizes

---

base their decisions without forcing the United States to choose between compromising highly sensitive intelligence information or declining to take action against individuals or entities that may present a serious threat to the United States or its nationals. A similar accommodation mechanism was enacted by Congress in the Anti-Terrorism and Effective Death Penalty Act of 1996, 8 U.S.C. §1189(b)(2)," DoJ at §159.

[3411] "An owner of property that is confiscated under any provision of law relating to the confiscation of assets of suspected international terrorists, may contest that confiscation by filing a claim in the manner set forth in the Federal Rules of Civil Procedure (Supplemental Rules for Certain Admiralty and Maritime Claims), and asserting as an affirmative defense that – (1) the property is not subject to confiscation under such provision of law; or (2) the innocent owner provisions of section 983(d) of title 18, United States Code, apply to the case," Sec. 316(a).

[3412] 18 U.S.C. 983(i)(2)(D).

[3413] "The exclusion of certain provisions of Federal law from the definition of the term 'civil forfeiture statute' in section 983(i) of title 18, United States Code, shall not be construed to deny an owner of property the right to contest the confiscation of assets of suspected international terrorists under – (A) subsection (a) of this section; (B) the Constitution; or (C) subschapter II of chapter 5 of title 5, United States Code (commonly known as the 'Administrative Procedure Act')," Sec. 316(c)(1).

[3414] "Current law does not contain any authority tailored specifically to the confiscation of terrorist assets. Instead, currently, forfeiture is authorized only in narrow circumstances for the proceeds of murder, arson, and some terrorism offenses, or for laundering the proceeds of such offenses. However, most terrorism offenses do not yield 'proceeds,' and available current forfeiture laws require detailed tracing that is quite difficult for accounts coming through the banks of countries used by many terrorists. "This section increases the government's ability to strike at terrorist organizations' economic base by permitting the forfeiture of its property regardless of the source of the property, and regardless of whether the property has actually been used to commit a terrorism offense. This is similar in concept to the forfeiture now available under RICO. In parity with the drug forfeiture laws, the section also authorizes the forfeiture of property used or

confiscation of all property, regardless of where it is found, of any individual, entity, or organization engaged in domestic or international terrorism (as defined in 18 U.S.C. 2331),[3415] against the United States, Americans or their property, 18 U.S.C. 981(a)(1)(G). Section 806 as discussed below also calls for the more common confiscation of property derived from and or facilitating acts of domestic or international terrorism against the United States or its citizens. Confiscations under 806 may be challenged under the procedures of 18 U.S.C. 983, since they are not exempted there. To the extent that forfeiture under section 806 is based on international rather than domestic terrorism, claimants may also use the procedures of section 316.

Confiscation based solely on the fact that the property is owned by a criminal offender, rather than that it is derived from or facilitates some crime is fairly uncommon. It is the mark of common law forfeiture of estate. At common law, a felon forfeited all of his property. Most contemporary forfeiture statutes employ statutory forfeiture, a more familiar presence in American law,[3416] which consists of the confiscation of things whose possession is criminal, of the fruits of crime, and of the means of crime – untaxed whiskey, the drug dealer's profits, and the rum runner's ship.

Three characteristics set forfeiture of estate apart. The property is lost solely by reason of its ownership by a felon. All of a felon's property is confiscated, not merely that which is related to the crime for which he is convicted. Finally, it

---

intended to be used to facilitate a terrorist act, regardless of its source. There is no need for a separate criminal forfeiture provision because criminal forfeiture is incorporated under current law by reference. The provision is retroactive to permit it to be applied to the events of September 11, 2001," DoJ, at §403. The House Report on H.R. 2975 which contained versions of both sections is no more explicit on the relation of the two sections.

[3415] "(1) the term 'international terrorism' means activities that – (A) involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or of any State; (B) appear to be intended – (i) to intimidate or coerce a civilian population; (ii) to influence the policy of a government by intimidation or coercion; or (iii) to affect the conduct of a government by mass destruction, assassination or kidnapping; and (C) occur primarily outside the territorial jurisdiction of the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to intimidate or coerce, or the locale in which their perpetrators operate or seek asylum . . . (5) the term 'domestic terrorism' means activities that – (A) involve acts dangerous to human life that are a violation of the criminal laws of the United States or of any State; (B) appear to be intended – (i) to intimidate or coerce a civilian population; (ii) to influence the policy of a government by intimidation or coercion; or (iii) to affect the conduct of a government by mass destruction, assassination or kidnapping; and (C) occur primarily within the territorial jurisdiction of the United States," 18 U.S.C. 2331(1),(5)(as amended by section 802 of the Act).

[3416] Austin v. United States, 509 U.S. 602, 611-12 (1993)("Three kinds of forfeiture were established in England at the time the Eighth Amendment was ratified in the United States: deodand, forfeiture, and statutory forfeiture . . . . Of England's three kinds of forfeiture, only the third took hold in the United States").

occasions attainder which negates the felon's right to hold property or for title to property to pass through him to his heirs. It was with this in mind, that the Framers declared that "no attainder of treason shall work corruption of blood or forfeiture exception during the life of the person attainted."[3417] And for this reason, President Lincoln insisted that the confiscated real estate of Confederate supporters should revert their heirs at death.[3418]

Neither section 106 nor 806 require conviction of the terrorist property owner.[3419] Both call for forfeiture of all of the terrorist's property, without requiring any nexus to the terrorist's offenses other than terrorist ownership. Neither makes any explicit provision for the terrorist's heirs. Section 106 applies only to foreign persons, organizations, or countries, but section 806 recognizes no such distinction.

Of course, the Supreme Court long ago confirmed the constitutional validity of a seemingly similar pattern in TWEA under the President's war powers.[3420] The Court was careful to point out, however, that the TWEA procedure was not really forfeiture or confiscation for the benefit of the United States, but by express statutory provision a liquidation measure to protect the creditors of enemy property owners.[3421] Neither section 106 nor 806 are part of TWEA and neither

---

[3417] U.S.Const. Art.III, §3, cl.2.

[3418] 12 Stat. 589, 627 (1862). Some would suggest a fourth distinction: that it follows a felony conviction. This is hardly a distinction, since over time legislation creating statutory forfeitures has employed criminal in personam proceedings following criminal conviction as a means of accomplishing confiscation.

[3419] Although by operation of law property subject to civil forfeiture of section 806 may be confiscated upon conviction of the property owner for any crime of domestic or international terrorism, 28 U.S.C. 2461(c)("If a forfeiture of property is authorized in connection with a violation of an Act of Congress, and any person is charged in an indictment or information with such violation but no specific statutory provision is made for criminal forfeiture upon conviction, the Government may include the forfeiture in the indictment or information in accordance with the Federal Rules of Criminal Procedure, and upon conviction, the court shall order the forfeiture of the property in accordance with the procedures set forth in section 413 of the Controlled Substances Act").

[3420] Silesian American Corp. V. Clark, 332 U.S. 469 (1947); cf., Societe Internationale v. Rogers, 357 U.S. 197, 211 (1958)("this summary power to seize property which is believed to be enemy-owned is rescued from constitutional invalidity under the Due Process and Just Compensation Clauses of the Fifth Amendment only by those provisions of the Act which afford a non-enemy claimant a later judicial hearing as to the propriety of the seizure").

[3421] Zittman v. McGrath, 341 U.S. 471, 473-74 (1951)(citing 50 U.S.C.App. 34) ("While the statute under which the funds are to be 'held, administered and accounted for' authorizes the vesting of such foreign-owned property in the custodian and its administration 'in the interest of and for the benefit of the United States,' it is not a confiscation measure, but a liquidation measure for the

explicitly treats the proceeds of confiscation as a fund for the benefit of creditors. Moreover, broad as the President's war powers may be, they would hardly seem to provide a justification for section 806, which embraces domestic terrorism and is neither limited to foreign offenders nor predicated upon war-like hostilities.

Criminal forfeitures, civil forfeitures with punitive as well as remedial purposes, and civil forfeitures whose effect is so punitive as to negate any presumption of remedial purpose, all raise other constitutional points of interest. The Eighth Amendment's excessive fines clause prohibits criminal forfeitures, and civil forfeitures with at least some punitive purposes, that are grossly disproportionate to the gravity of the crimes which trigger them.[3422] The Fifth Amendment's double jeopardy clause applies to criminal forfeitures and civil forfeitures which are so punitive as to negate any presumption of remedial purposes.[3423] The same has been said of the applicability of the ex post facto clause.[3424]

The limitations on criminal forfeitures would apply to the forfeitures under section 806 when prosecuted as criminal forfeitures by operation of 28 U.S.C. 2461(c). The offenses that activate section 106 and 806 confiscations, however, are of such gravity that successful excessive fine clause challenges are unlikely, even if the value of confiscated property were extraordinarily high.

On the other hand, there is more than a little support for the argument that section 106 and 806 constitute punitive rather than remedial measures. They are potentially severe. Section 806 calls for the total impoverishment of those to whom it applies (all assets foreign and domestic), while section 106 anticipates confiscation of all assets within the jurisdiction of the United States. They seem to undermine any claim to remedial purpose by reaching those assets that neither facilitate the commission of terrorism nor constitute its fruits. Moreover, in its analysis of the language of section 806, the Justice Department described it as conceptually akin to the criminal forfeiture provisions of RICO.[3425] If the courts find section 106 or 806 are civil in name but criminal in nature, they may well

---

protection of American creditors. It provides for the filing and proving of claims and states that the funds 'shall be equitably applied for the payments of debts").

[3422] United States v. Bajakajian, 524 U.S. 321, 337 (1998); Austin v. United States, 509 U.S. 602, 622 (1993).

[3423] United States v. Ursery, 518 U.S. 267, 278 (1996).

[3424] See e.g., United States v. Certain Funds (Hong Kong and Shanghai Banking Corp.), 96 F.3d 20, 26-7 (2d Cir. 1996). Where the ex post facto clauses do not apply, the validity of retroactive statutes is judged by due process clause standards. There is a presumption against retroactive application in such instances absent a clear indication of contrary Congressional intent grounded in the view that due process demands certain minimal notice of the law's demands, Landgraf v. USI Film Products, 511 U.S. 244, 265-66 (1994).

[3425] DoJ, at §403.

conclude that efforts to enforce the sections are bound by the limitations of the double jeopardy and ex post facto clauses.

Other Forfeiture Amendments

In order to more effectively enforce money laundering penalties and prosecute civil forfeiture actions involving foreign individuals or entities, section 317 of the Act establishes a procedure for long-arm jurisdiction over individuals and entities located overseas and for the appointment of a federal receiver to take control of contested assets during the pendency of the proceedings.[3426]

In the case of inter-bank accounts where a bank in a foreign nation has an account in a bank located in the United States, section 319(a) allows seizure of funds in an account here when the foreign bank has received money laundering or drug trafficking deposits overseas.[3427] Confiscation proceedings are conducted pursuant to 18 U.S.C. 953.

[3426] 18 U.S.C. 1956(b). Cf., H.R.Rep.No. 107-250, at 54-5 (2001)("The first provision in this section creates a long arm statute that gives the district court jurisdiction over a foreign person, including a foreign bank, that commits a money laundering offense in the United States or converts laundered funds that have been forfeited to the Government to his own use. Thus, if the Government files a civil enforcement action under section 1956(b), or files a civil lawsuit to recover forfeited property from a third party, the district court would have jurisdiction over the defendant if the defendant has been served with process pursuant to the applicable statutes or rules of procedure, and the constitutional requirement of minimum contacts is satisfied in one of three ways: the money laundering offense took place in the United States; in the case of converted property, the property was the property of the United States by virtue of a civil or criminal forfeiture judgment; or in the case of a financial institution, the defendant maintained a correspondent bank account at another bank in the United States. Under this provision, for example, the district courts would have had jurisdiction over the defendant in the circumstances described in United States v. Swiss American Bank, 191 F.3d 30 (1st Cir. 1999). "The second provision, modeled on 18 U.S.C. 1345(b), gives the district court the power to restrain property, issue seizure warrants, or take other action necessary to ensure that a defendant in an action covered by the statute does not dissipate the assets that would be needed to satisfy a judgment. "This section also authorizes a court, on the motion of the Government or a State or Federal regulator, to appoint a receiver to gather and protect assets needed to satisfy a judgment under sections 1956 and 957, and the forfeiture provisions in sections 981 and 982. This authority is intended to apply in three circumstances: (1) when there is a judgment in a criminal case, including an order of restitution, following a conviction for a violation of section 1956 or 1957; (2) when there is a judgment in a civil case under section 1956(b) assessing a penalty for a violation of either section 1956 or 1957; and (3) when there is a civil forfeiture judgment under section 981 or a criminal forfeiture judgment, including a personal money judgment, under section 982. "The amendment also makes section 1956(b) applicable to violations of section 1957. It applies to conduct occurring before the effective date of the Act").

[3427] 18 U.S.C. 981(k). H.R.Rep.No. 107-250, at 57-8 (2001)("Section 114 creates a new provision in the civil forfeiture statute, 18 U.S.C. 981(k), authorizing the forfeiture of funds found in an interbank account. The new provision is necessary to reconcile the law regarding the forfeiture of funds in bank accounts with the realities of the global movement of electronic funds and the use of off-shore banks to insulate criminal proceeds from forfeiture. "To prevent drug dealers and other criminals from taking advantage of certain nuances of forfeiture law to insulate their

Federal law has for some time permitted criminal forfeiture orders to reach substitute assets if the property of the defendant subject to confiscation has become unavailable. Section 319(d) establishes a procedure under which a convicted defendant may be ordered to transfer property to this country from overseas if the property is subject to confiscation.[3428]

Prior to enactment of the Act, federal law permitted confiscation of any property in the United States that could be traced to a drug offense committed overseas, if the offense was punishable as a felony under the laws of the nation where it occurred and if the offense would have been a felony if committed here.[3429] Section 320 enlarges this provisions to cover not only drug offenses but any of the crimes in the money laundering predicate offense list of 18 U.S.C. 1956(c)(7)(B), and continues the reciprocal felony requirements.[3430] This treatment is

---

property from forfeiture even though it is deposited in a bank account in the United States, it is necessary to change the law regarding the location of the debt that a bank owes to its depositor, and the identity of the real party in interest with standing to contest the forfeiture. The amendment in this section addresses the location issue by treating a deposit made into an account in a foreign bank that has a correspondent account at a U.S. bank as if the deposit had been made into the U.S. bank directly. Second, the section treats the deposit in the correspondent account as a debt owed directly to the depositor, and not as a debt owed to the respondent bank. In other words, the correspondent account is treated as if it were the foreign bank itself, and the funds in the correspondent account were debts owed to the foreign bank's customers. "Under this arrangement, if funds traceable to criminal activity are deposited into a foreign bank, the Government may bring a forfeiture action against funds in that bank's correspondent account, and only the initial depositor, and not the intermediary bank, would have standing to contest it. "The section authorizes the Attorney General to suspend or terminate a forfeiture in cases where there exists a conflict of laws between the U.S. and the jurisdiction in which the foreign bank is located, where such suspension or termination would be in the interest of justice and not harm U.S. national interests").

[3428] Cf., H.R. Rep. No. 107-250, at 58-9 (2001) ("Section 116 authorizes a court to order a criminal defendant to repatriate his property to the United States in criminal cases. In criminal forfeiture cases, the sentencing court is authorized to order the forfeiture of 'substitute assets' when the defendant has placed the property otherwise subject to forfeiture 'beyond the jurisdiction of the court.' Frequently, this provision is applied when a defendant has transferred drug proceeds or other criminally derived property to a foreign country. In many cases, however, the defendant has no other assets in the United States of a value commensurate with the forfeitable property overseas. In such cases, ordering the forfeiture of substitute assets is a hollow sanction. "This section amends 21 U.S.C. 853 to make clear that a court in a criminal case may issue a repatriation order--either post-trial as part of the criminal sentence and judgment, or pre-trial pursuant to the court's authority under 21 U.S.C. 853(e) to restrain property--so that they will be available for forfeiture. Failure to comply with such an order would be punishable as a contempt of court, or it could result in a sentencing enhancement, such as a longer prison term, under the U.S. Sentencing Guidelines, or both").

[3429] 18 U.S.C. 981(a)(1)(B).

[3430] H.R. Rep. No. 107-250, at 56 (2001)("This section is intended to reinforce the United States' compliance with the Vienna Convention. It amends 18 U.S.C. 981(a)(1)(B) to allow the United States to institute its own action against the proceeds of foreign criminal offenses when such

comparable to the early coverage of the federal statute, 28 U.S.C. 2467, which permitted enforcement of foreign confiscation orders in the case of drug offenses or the crimes on the money laundering predicate offense list. Section 323 of the Act amends the foreign forfeiture enforcement statute to (1) expand the grounds for enforcement to include any crime which would have provided the grounds for confiscation had the offense been committed in the United States; (2) to authorize restraining orders to freeze the target property while enforcement litigation is pending; and (3) to limit the absence-of-timely-notice defense.[3431]

---

proceeds are found in the United States. As required by the Vienna Convention, it also authorizes the confiscation of property used to facilitate such crimes. The list of foreign crimes to which this section applies is determined by cross-reference to the foreign crimes that are money laundering predicates under 1956(c)(7)(B). This section will permit the forfeiture of property involved in conduct occurring before the effective date of the Act").

[3431] H.R. Rep. No. 107-250, at 59-60 (2001)("Under current law, 28 U.S.C. 2467(d) gives Federal courts the authority to enforce civil and criminal forfeiture judgments entered by foreign courts. This section amends that provision to include a mechanism for preserving property subject to forfeiture in a foreign country. "Specifically, a Federal court could issue a restraining order under 18 U.S.C. 983(j) or register and enforce a foreign restraining order, if the Attorney General certified that such foreign order was obtained in accordance with the principles of due process. A person seeking to contest the restraining order could do so on the ground that 28 U.S.C. 2467 was not properly applied to the particular case, but could not oppose the restraining order on any ground that could also be raised in the proceedings pending in a foreign court. This provision prevents a litigant from taking 'two bites at the apple' by raising objections to the basis for the forfeiture in the Federal court that he also raised, or is entitled to raise, in the foreign court where the forfeiture action is pending. It complements the existing provision in section 2467(e) providing that the Federal court is bound by the findings of fact of the foreign court, and may not look behind such findings in determining whether to enter an order enforcing a foreign forfeiture judgment. "This section also amends 28 U.S.C. 2467 to make clear that it is not necessary to prove that the person asserting an interest in the property received actual notice of the forfeiture proceedings. As is the case with respect to forfeitures under U.S. law, it is sufficient if the foreign nation takes steps to provide notice, in accordance with the principles of due process. See Gonzalez v. United States, 1997 WL 278123 (S.D.N.Y. 1997) ('the [G]overnment is not required to ensure actual receipt of notice that is properly mailed'); Albajon v. Gugliotta , 72 F. Supp. 2d 1362 (S.D. Fla. 1999) (notice sent to various addresses on claimant's identifications, and mailed after claimant released from jail, is sufficient to satisfy due process, even if claimant never received notice); United States v. Schiavo , 897 F. Supp. 644, 648 49 (D. Mass. 1995) (sending notice to fugitive's last known address is sufficient; due process satisfied even if he did not receive the notice). "Finally, 28 U.S.C. 2467 is amended to authorize the enforcement of a forfeiture judgment based on any foreign offense that would constitute an offense giving rise to a civil or criminal forfeiture of the same property if the offense had been committed in the United States. This is one of two safeguards that the statute contains against the enforcement of judgments that the United States does not consider appropriate for enforcement: if the judgment is based on an act that would not constitute a crime in the United States, such as removing assets from the reach of a repressive regime, it could not be enforced. In addition, section 2467 already provides that a foreign judgment may only be enforced by a Federal court at the request of the United States, and only after the Attorney General has certified that the judgment was obtained in accordance with the principles of due process. Thus, neither a foreign Government nor a foreign private party could enforce a foreign judgment on its own under this provision."). Note that the safeguard to which the report refers is the range of foreign offenses that will support an enforceable confiscation order, i.e., drug offenses and crimes on the money laundering predicate offense list,

A fugitive may not challenge a federal forfeiture.[3432] Section 322 applies this fugitive disentitlement to corporations whose major shareholder is a fugitive or whose representative in the confiscation proceedings is a fugitive.

Section 906 instructs the Attorney General, the Secretary of the Treasury, and the Director of Central Intelligence to submit a joint report with recommendations relating to the reconfiguration of the Foreign Terrorist Asset Tracking Center, the Office of Foreign Assets Control, and possibly FinCEN in "order to establish a capability to provide for the effective and efficient analysis and dissemination of foreign intelligence relating to the financial capabilities and resources of international terrorist organizations."

ALIEN TERRORISTS AND VICTIMS

The Act contains a number of provisions designed to prevent alien terrorists from entering the United States, particularly from Canada; to enable authorities to detain and deport alien terrorists and those who support them; and to provide humanitarian immigration relief for foreign victims of the attacks on September 11.

Border Protection

The border protection provisions:

- authorize the appropriations necessary to triple the number of Border Patrol, Customs Service, and Immigration and Naturalization Service (INS) personnel stationed along the Northern Border, section 401
- authorize appropriations of an additional $50 million for both INS and the Customers Service to upgrade their border surveillance equipment, section 402
- remove for fiscal year 2001 the $30,000 ceiling on INS overtime pay for border duty, section 404
- authorize appropriations of $2 million for a report to be prepared by the Attorney General on the feasibility of enhancing the FBI's Integrated Automated Fingerprint Identification System (IAFIS) and similar systems to improve the reliability of visa applicant screening, section 405
- authorize the appropriations necessary to provide the State Department and INS with criminal record identification information relating to visa applicants and other applicants for admission to the United States, section 403.

---

and that the amendment narrows that safeguard by adding additional foreign offenses, i.e., any foreign equivalent of a federal crime which would support a confiscation order.

[3432] 28 U.S.C. 2466.

- instruct the Attorney General to report on the feasibility of the use of a biometric identifier scanning system with access to IAFIS for overseas consular posts and points of entry into the United States, section 1007
- direct the Secretary of State to determine whether consular shopping is a problem, to take any necessary corrective action, and to report the action taken, section 418
- express the sense of the Congress that the Administration should implement the integrated entry and exit data system called for by the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (8 U.S.C. 1365a), section 414
- add the White House Office of Homeland Security to the Integrated Entry and Exit Data System Task Force (8 U.S.C. 1365a note), section 415
- call for the implementation and expansion of the foreign student visa monitoring program (8 U.S.C. 1372), section 416
- limit countries eligible to participate in the visa waiver program to those with machine-readable passports as of October 1, 2003 (8 U.S.C. 1187(c)), section 417
- instruct the Attorney General to report on the feasibility of using biometric scanners to help prevent terrorists and other foreign criminals from entering the country, section 1008[3433]
- authorize appropriations of $250,000 for the FBI to determine the feasibility of providing airlines with computer access to the names of suspected terrorists, section 1009
- authorize reciprocal sharing of the State Department's visa lookout data and related information with other nations in order to prevent terrorism, drug trafficking, slave marketing, and gun running, section 413

Detention and Removal

Foreign nationals (aliens) are deportable from the United States, among other grounds, if they were inadmissible at the time they entered the country or if they have subsequently engaged in terrorist activity, 8 U.S.C. 1227 (a)(1)(A), (a)(4)(B), 1182(a)(3)(B)(iv). Aliens may be inadmissible for any number of terrorism-related reasons, 8 U.S.C. 1182 (a)(3)(B). Section 411 of the Act adds to the terrorism-related grounds upon which an alien may be denied admission into the United States and consequently upon which he or she may be deported.

Prior law recognized five terrorism-related categories of inadmissibility. Section 411 redefines two of these – engaging in terrorist activity and representing a terrorist organization (8 U.S.C. 1182(a)(3)(B)(iv), (a)(3)(B)(i)(IV)) – and it adds

---

[3433] As the House Judiciary Committee explained, "A biometric fingerprint scanning system is a sophisticated computer scanning technology that analyzes a person's fingerprint and compares the measurement with a verified sample digitally stored in the system. The accuracy of these systems is claimed to be above 99.9%. The biometric identifier system contemplated by this section would have access to the database of the Federal Bureau of Investigation Integrated Automated Fingerprint Identification System," H.R. Rep. No. 107-236, at 78 (2001).

three more – espousing terrorist activity, being the spouse or child of an inadmissible alien associated with a terrorist organization, and intending to engage in activities that could endanger the welfare, safety or security fo the United States (8 U.S.C. 1182(a)(3)(B)(i)(VI), (a)(3)(B)(i)(VII), 1182(a)(3)(F). It defined engaging in terrorist activity, which is grounds for both inadmissibility and deportation, to encompass soliciting on behalf of a terrorist organization or providing material support to a terrorist organization, 8 U.S.C. 1182(a)(3)(B)(iii)(2000 ed.). It did not explain in so many words, however, what constituted a "terrorist organization," but it presumably included groups designated as terrorist organizations under section 219 of the Immigration and Nationality Act, 8 U.S.C. 1189.

Section 411 defines "terrorist organization" to include not only organizations designated under section 219 but also organizations which the Secretary of State has identified in the Federal Register as having provided material support for, committed, incited, planned, or gathered information on potential targets of, terrorist acts of violence, 8 U.S.C. 1182(a)(3)(B)(vi), (a)(3)(B)(iv). It then recasts the definition of engaging in terrorist activities to include solicitation on behalf of such organizations, or recruiting on their behalf, or providing them with material support, 8 U.S.C. 1182(a)(3)(B)(iv). Nevertheless, section 411 permits the Secretary of State or Attorney General to conclude that the material support prohibition does not apply to particular aliens, 8 U.S.C. 1182(a)(3)(B)(vi).

Prior law made representatives of terrorist organizations designated by the Secretary under section 219 (8 U.S.C. 1189) inadmissible, 8 U.S.C. 1182(a)(3)(B)(i) (IV)(2000 ed.). And so they remain. Section 411 makes representatives of political, social or similar groups, whose public endorsements of terrorist activities undermines U.S. efforts to reduce or eliminate terrorism, inadmissible as well, 8 U.S.C. 1882(a)(3) (B)(i)(IV).

An individual who uses his or her place of prominence to endorse, espouse, or advocate support for terrorist activities or terrorist organizations in a manner which the Secretary of State concludes undermines our efforts to reduce or eliminate terrorism becomes inadmissible under section 411, 8 U.S.C. 1182(a)(3)(B)(i)(VI).

The spouse or child of an alien, who is inadmissible on terrorist grounds for activity occurring within the last 5 years, is likewise inadmissible, unless the child or spouse was reasonably unaware of the disqualifying conduct or has repudiated the disqualifying conduct, 8 U.S.C. 1182(a)(3)(B)(i)(VII), 1182(a)(3)(B)(ii).

Finally, any alien, whom the Secretary of State or the Attorney General conclude has associated with a terrorist organization and intends to engage in conduct dangerous to the welfare, safety, security of the United States while in this country, is inadmissible, 8 U.S.C. 1182(a)(3)(F).

Section 219 of the Immigration and Nationality Act (8 U.S.C. 1189) permits the Secretary to designate as terrorist organizations any foreign group which he finds to have engaged in terrorist activities. A second subsection 411(c) permits him to designate groups which as subnational groups or clandestine agents, engage in "premeditated, politically motivated violence perpetrated against noncombatant targets," or groups which retain the capacity and intent to engage in terrorism or terrorist activity, 8 U.S.C. 1189(a)(1)(B).

Section 412 permits the Attorney General to detain alien terrorist suspects for up to seven days, 8 U.S.C. 1226a. He must certify that he has reasonable grounds to believe that the suspects either are engaged in conduct which threatens the national security of the United States or are inadmissible or deportable on grounds of terrorism, espionage, sabotage, or sedition. Within seven days, the Attorney General must initiate removal or criminal proceedings or release the alien. If the alien is held, the determination must be reexamined every six months to confirm that the alien's release would threaten national security or endanger some individual or the general public. The Attorney General's determinations are subject to review only under writs of habeas corpus issued out of any federal district court but appealable only to the United States Court of Appeals for the District Columbia. The Attorney General must report to the Judiciary Committee on the details of the operation of section 412.

Uncertain is the relationship between section 412 and the President's Military Order of November 13, 2001, which allows the Secretary of Defense to detain designated alien terrorist suspects, within the United States or elsewhere, without express limitation or condition except with regard to food, water, shelter, clothing, medical treatment, religious exercise, and a proscription on invidious discrimination, 66 Fed.Reg. 57833, 57834 (Nov. 16, 2001).

Victims

The Act contains a number of provisions designed to provide immigration relief for foreign nationals, victimized by the attacks of September 11. It provides for:

- permanent resident alien status for eligible aliens and members of their family who but for the events of September 11 would have been eligible for employer-sponsored permanent resident alien status, section 421[3434]

[3434] "The Act provides permanent resident status through the special immigrant program to an alien who was the beneficiary of a petition filed (on or before September 11) to grant the alien permanent residence as an employer-sponsored immigrant or of an application for labor certification (filed on or before September 11), if the petition or application was rendered null because of the disability of the beneficiary or loss of employment of the beneficiary due to physical damage to, or destruction of, the business of the petitioner or applicant as a direct result of the terrorist attacks on September 11, or because of the death of the petitioner or applicant as a direct result of the terrorist attacks. Permanent residence would be granted to an alien who was the spouse or child of an alien who was the beneficiary of a petition filed on or before September

- extended filing deadlines for aliens prevented from taking timely action because of immigration office closures, airline schedule disruptions or other similar impediments, section 422[3435]
- preservation of certain immigration benefits available to alien family members that would be otherwise lost as a consequence of the death of a victim of September 11, section 423[3436]

---

11 to grant the beneficiary permanent residence as a family-sponsored immigrant (as long as the spouse or child follows to join not later than September 11, 2003). Permanent residence would be granted to the beneficiary of a petition for a nonimmigrant visa as the spouse or the fiancé (and their children) of a U.S. citizen where the petitioning citizen died as a direct result of the terrorist attack. The section also provides permanent resident status to the grandparents of a child both of whose parents died as a result of the terrorist attacks, if either of such deceased parents was a citizen of the U.S. or a permanent resident," H.R.Rep.No. 107-236, at 66-7 (2001).

[3435] "The Act provides that an alien who was legally in a nonimmigrant status and was disabled as a direct result of the terrorist attacks on September 11 (and his or her spouse and children) may remain lawfully in the U.S. (and receive work authorization) until the later of the date that his or her status normally terminates or September 11, 2002. Such status is also provided to the nonimmigrant spouse and children of an alien who died as a direct result of the terrorist attacks. "The Act provides that an alien who was lawfully present as a nonimmigrant at the time of the terrorist attacks will be granted 60 additional days to file an application for extension or change of status if the alien was prevented from so filing as a direct result of the terrorist attacks. Also, an alien who was lawfully present as a nonimmigrant at the time of the attacks but was then unable to timely depart the U.S. as a direct result of the attacks will be considered to have departed legally if doing so before November 11. An alien who was in lawful nonimmigrant status at the time of the attacks (and his or her spouse and children) but not in the U.S. at that time and was then prevented from returning to the U.S. in order to file a timely application for an extension of status as a direct result of the terrorist attacks will be given 60 additional days to file an application and will have his or her status extended 60 days beyond the original due date of the application. "Under current law, winners of the fiscal year 2001 diversity visa lottery must enter the U.S. or adjust status by September 30, 2001. The Act provides that such an alien may enter the U.S. or adjust status until April 1, 2002, if the alien was prevented from doing so by September 30, 2001 as a direct result of the terrorist attacks. If the visa quota for the 2001 diversity visa program has already been exceeded, the alien shall be counted under the 2002 program. Also, if a winner of the 2001 lottery died as a direct result of the terrorist attacks, the spouse and children of the alien shall still be eligible for permanent residence under the program. The ceiling placed on the number of diversity immigrants shall not be exceeded in any case. "Under the Act, in the case of an alien who was issued an immigrant visa that expires before December 31, 2001, if the alien was unable to timely enter the U.S. as a direct result of the terrorist attacks, the validity shall be extended until December 31. "Under the Act, in the case of an alien who was granted parole that expired on or after September 11, if the alien was unable to enter the U.S. prior to the expiration date as a direct result of the terrorist attacks, the parole is extended an additional 90 days. "Under the Act, in the case of an alien granted voluntary departure that expired between September 11 and October 11, 2001, voluntary departure is extended an additional 30 days," H.R.Rep.No. 107-236, at 67-8 (2001).

[3436] "Current law provides that an alien who was the spouse of a U.S. citizen for at least 2 years before the citizen died shall remain eligible for immigrant status as an immediate relative. This also applies to the children of the alien. The Act provides that if the citizen died as a direct result of the terrorist attacks, the 2 year requirement is waived. "The Act provides that if an alien spouse, child, or unmarried adult son or daughter had been the beneficiary of an immigrant visa petition filed by a permanent resident who died as a direct result of the terrorist attacks, the alien

---

- limited easing of age restrictions on visas available to aliens under 21 years of age for those whose 21st birthday occurred immediately before or soon after September 11, section 424[3437]
- temporary administrative relief for alien family members of a victim of September 11 who are not otherwise entitled to relief under the Act, section 425
- a denial of benefits of the Act to terrorists and their families, section 427
- authority for the Attorney General to establish evidentiary standards to implement the alien victim provisions of the Act, section 426.

OTHER CRIMES, PENALTIES, & PROCEDURES

New Crimes

The Act creates new federal crimes for terrorist attacks on mass transportation facilities, for biological weapons offenses, for harboring terrorists, for affording terrorists material support, for misconduct associated with money laundering already mentioned, for conducting the affairs of an enterprise which affects interstate or foreign commerce through patterned commission of terrorist offenses, and for fraudulent charitable solicitation. Although strictly speaking these are new federal crimes, they generally supplement existing law filling gaps and increasing penalties.

Pre-existing federal law criminalized, among other things, wrecking trains, 18 U.S.C. 1992, damaging commercial motor vehicles or their facilities, 18 U.S.C. 33, or threatening to do so, 18 U.S.C. 35, destroying vessels within the navigable waters of the United States, 18 U.S.C. 2273, destruction of vehicles or other property used in or used in activities affecting interstate or foreign commerce by fire or explosives, 18 U.S.C. 844(i), possession of a biological agent or toxin as a weapon or a threat, attempt, or conspiracy to do so, 18 U.S.C. 175, use of a weapon of mass destruction affecting interstate or foreign commerce or a threat, attempt, or conspiracy to do so, 18 U.S.C. 2332a, commission of a federal crime of

---

will still be eligible for permanent residence. In addition, if an alien spouse, child, or unmarried adult son or daughter of a permanent resident who died as a direct result of the terrorist attacks was present in the U.S. on September 11 but had not yet been petitioned for permanent residence, the alien can self-petition for permanent residence. "The Act provides that an alien spouse or child of an alien who 1) died as a direct result of the terrorist attacks and 2) was a permanent resident (petitioned-for by an employer) or an applicant for adjustment of status for an employment-based immigrant visa, may have his or her application for adjustment adjudicated despite the death (if the application was filed prior to the death)," H.R.Rep.No. 107-236, at 68 (2001).

[3437] "Under current law, certain visas are only available to an alien until the alien's 21st birthday. The Act provides that an alien whose 21st birthday occurs this September and who is a beneficiary for a petition or application filed on or before September 11 shall be considered to remain a child for 90 days after the alien's 21st birthday. For an alien whose 21st birthday occurs after this September, (and who had a petition for application filed on his or her behalf on or before September 11) the alien shall be considered to remain a child for 45 days after the alien's 21st birthday," H.R.Rep.No. 107-236, at 68 (2001).

violence while armed with a firearm, or of federal felony while in possession of an explosive, 18 U.S.C. 924(c), 844(h), conspiracy to commit a federal crime, 18 U.S.C. 371.

The Act outlaws terrorist attacks and other actions of violence against mass transportation systems. Offenders may be imprisoned for life or any term of years, if the conveyance is occupied at the time of the offense, or imprisoned for not more than twenty years in other cases, section 801. Under its provisions, it is a crime to willfully:

- wreck, derail, burn, or disable mass transit;
- place a biological agent or destructive device on mass transit recklessly or with the intent to endanger;
- burn or place a biological agent or destructive device in or near a mass transit facility knowing a conveyance is likely to be disabled;
- impair a mass transit signal system;
- interfere with a mass transit dispatcher, operator, or maintenance personnel in the performance of their duties recklessly or with the intent to endanger;
- act with the intent to kill or seriously injure someone on mass transit property;
- convey a false alarm concerning violations of the section;
- attempt to violate the section;
- threaten or conspire to violate the section

when the violation involves interstate travel, communication, or transportation of materials or that involves a carrier engaged in or affecting interstate or foreign commerce, 18 U.S.C. 1993.

Prior to enactment of the Act, federal law proscribed the use of biological agents or toxins as weapons, 18 U.S.C. 175. As suggested by the Justice Department,[3438] the Act, in section 817, makes two substantial changes. It makes it a federal offense, punishable by imprisonment for not more than ten years and/or a fine of

---

[3438] "Current law prohibits the possession, development, acquisition, etc. of biological agents or toxins for use as a weapon. 18 U.S.C. §175. This section amends the definition of 'for use as a weapon' to include all situations in which it can be proven that the defendant had a purpose other than a prophylactic, protective, or peaceful purpose. This will enhance the government's ability to prosecute suspected terrorists in possession of biological agents or toxins, and conform the scope of the criminal offense in 18 U.S.C. §175 more closely to the related forfeiture provision in 18 U.S.C. §176 [which permits confiscations in cases where the amounts possessed exceed the quantities justifiable for peaceful purposes]. Moreover, the section adds a subsection to 18 U.S.C. §175 which defines an additional offense of possessing a biological agent or toxin of a type or in a quantity that, under the circumstances, is not reasonably justified by a prophylactic, protective or other peaceful purpose. This section also enacts a new statute, 18 U.S.C. 175b, which generally makes it an offense for a person to possess a listed biological agent or toxin if the person is disqualified from firearms possession under 18 U.S.C. §922(g). . . ." DoJ at §305.

not more than $250,000, to possess a type or quantity of biological material that cannot be justified for peaceful purposes, 18 U.S.C. 175(b). Second, consistent with federal prohibitions on the possession of firearms, 18 U.S.C. 922(g), and explosives, 18 U.S.C. 842(i), it makes it a federal offenses for certain individuals – such as convicted felons, illegal aliens, and fugitives – to possess biological toxins or agents, 18 U.S.C. 175b.[3439] Offenders face the same sanctions, imprisonment for not more than ten years and/or a fine of not more than $250,000.

It is a federal crime to harbor aliens, 8 U.S.C. 1324, or those engaged in espionage, 18 U.S.C. 792; or to commit misprision of a felony (which may take the form of harboring the felon), 18 U.S.C. 4; or to act as an accessory after the fact to a federal crime (including by harboring the offender), 18 U.S.C. 3. The Justice Department had asked that a terrorist harboring offense be added to the espionage section. It also recommended venue and extraterritorial auxiliaries.[3440]

The Act, in section 803, instead establishes a separate offense which punishes harboring terrorists by imprisonment for not more than ten years and/or a fine of not more than $250,000, 18 U.S.C. 2339. The predicate offense list consists of:

- destruction of aircraft or their facilities, 18 U.S.C. 32;
- biological weapons offenses, 18 U.S.C. 175;
- chemical weapons offenses, 18 U.S.C. 229;
- nuclear weapons offenses, 18 U.S.C. 831;
- bombing federal buildings, 18 U.S.C. 844(f);
- destruction of an energy facility, 18 U.S.C. 1366;
- violence committed against maritime navigational facilities, 18 U.S.C. 2280; • offenses involving weapons of mass destruction, 18 U.S.C. 2232a;
- international terrorism, 18 U.S.C. 2232b;
- sabotage of a nuclear facility, 42 U.S.C. 2284;
- air piracy, 49 U.S.C. 46502.

It grants the Justice Department request to permit prosecution either in the place where the harboring occurred or where the underlying act of terrorism

---

[3439] The section covers those under felony indictment, those convicted of a felony, fugitives, drug addicts, illegal aliens, mental defectives, aliens from countries which support terrorism, and those dishonorably discharged from the U.S. armed forces, 18 U.S.C. 175b(b)(2).

[3440] "18 U.S.C. §792 makes it an offense to harbor or conceal persons engaged in espionage. There is no comparable provision for terrorism, though the harboring of terrorists creates a risk to the nation readily comparable to that posed by harboring spies. This section accordingly amends 18 U.S.C. §792 to make the same prohibition apply to harboring or concealing persons engaged in federal terrorism offenses as defined in section 309 of the bill," DoJ at §307; Draft at §307(2)("There is extraterritorial Federal jurisdiction over any violation (including, without limitation, conspiracy or attempt) of this section. A violation of this section may be prosecuted in any Federal judicial district in which the underlying offense was committed, or in Federal judicial district as provided by law").

committed by the sheltered terrorist might be prosecuted. The Constitution, however, may insist that prosecution take place where the crime of harboring occurred.[3441]

Sections 2339A and 2339B of the title 18 of the United States Code ban providing material support to individuals and to organizations that commit various crimes of terrorism. The Act amends the sections in several ways in section 805. Section 2339B (support of a terrorist organization) joins section 2339A (support of a terrorist) as a money laundering predicate offense, 18 U.S.C. 1956(c)(7)(D) The predicate offense list of 18 U.S.C. 2339A (support to terrorists) grows to include:

- chemical weapons offenses, 18 U.S.C. 229;
- terrorist attacks on mass transportation, 18 U.S.C. 1993 ;
- sabotage of a nuclear facility, 42 U.S.C. 2284; and
- sabotage of interstate pipelines, 49 U.S.C. 60123(b).

And it adds expert advice or assistance to the types of assistance that may not be provided under section 2339A. This last addition may encounter the same First Amendment vagueness problems some courts have found in assistance which takes the form of "training" and "personnel," Humanitarian Law Project v. Reno, 205 F.3d 1130, 1137-136 (9th Cir. 2000).[3442] Finally, the section announces that a

---

[3441] U.S. Const. Art. III, §2, cl.3 ("The trial of all crimes . . . shall be held in the state where the said crimes shall have been committed . . . ."); Amend. IV ("In all criminal prosecutions, the accused shall enjoy the right to a speedy and public trial, by an impartial jury of the state and district wherein the crime shall have been committed. . . ."); United States v. Cabrales, 524 U.S. 1 (1998)(a defendant charged with one count of conspiracy to launder the proceeds of a Missouri drug operation and two counts of laundering in Florida could not be prosecuted in Missouri on the laundering counts). The Court might be thought to have retreated somewhat from Cabrales when it later approved prosecution for carrying a firearm in relation to a crime of violence in federal court in New Jersey (where the underlying kidnaping occurred) notwithstanding the fact that the firearm had been acquired in Maryland after the defendants left New Jersey with their victim in tow, United States v. Rodriguez-Moreno, 526 U.S. 275, 280-81 n.4 (1999)("By way of comparison, last Term in [Cabrales] we considered whether venue for money laundering, in violation of 18 U.S.C. 1956(a)(1)(B) (ii) and 1957, was proper in Missouri, where the laundered proceeds were unlawfully generated, or rather, only in Florida, where the prohibited laundering transactions occurred. As we interpreted the laundering statutes at issue, they did not proscribe the anterior criminal conduct that yielded the funds allegedly laundered. The existence of criminally generated proceeds was a circumstance element of the offense but the proscribed conduct – defendant's money laundering activity – occurred after the fact of an offense begun and completed by others. Here, by contrast, given the 'during and in relation to' language [of section 924], the underlying crime of violence is a critical part of the §924(c)(1) offense").

[3442] The Justice Department sought the expansion along with the enlargement of the predicate offense list, "18 U.S.C. §2339A prohibits providing material support or resources to terrorists. The existing definition of `material support or resources' is generally not broad enough to encompass expert services and assistance – for example, advice provided by a person with expertise in aviation matters to facilitate an aircraft hijacking, or advice provided by an accountant to facilitate the concealment of funds used to support terrorist activities. This section accordingly amends 18

prosecution for violation of section 2339A (support of terrorists) may be brought where the support is provided or where the predicate act of terrorism occurs. There may be some question whether the Constitution permits prosecution where the predicate act occurs.[3443]

Section 813 of the Act also accepts the Justice Department's suggestion that various terrorism offenses be added to the predicate offense list for RICO (racketeer influenced and corrupt organizations) which proscribes acquiring or operating, through the patterned commission of any of a series of predicate offenses, an enterprise whose activities affect interstate or foreign commerce, 18 U.S.C. 1961.[3444]

Prior law, 18 U.S.C. 2325-2327, outlawed violation of Federal Trade Commission (FTC) telemarketing regulations promulgated under 15 U.S.C. 6101 et seq. Section 1011 of the Act brings fraudulent charitable solicitations within the FTC's regulatory authority.[3445]

New Penalties

The Act increases the penalties for acts of terrorism and for crimes which terrorists might commit. More specifically it establishes an alternative maximum penalty for acts of terrorism, raises the penalties for conspiracy to commit certain terrorist offenses, envisions sentencing some terrorists to life-long parole, and increases the penalties for counterfeiting, cybercrime, and charity fraud.

The Justice Department suggested an alternative term of imprisonment up to life imprisonment for anyone convicted of an offense designated a terrorist crime. It characterized its proposal as analogous to the standard fine provisions of 18 U.S.C. 3571(b),(c). Section 3571 sets a basic maximum fine of $250,000 for any

---

U.S.C. §2339A to include expert services and assistance, making the offense applicable to experts who provide services or assistance knowing or intending that the services or assistance is to be used in preparing for or carrying out terrorism crimes. This section also amends 18 U.S.C. §2339A to conform its coverage of terrorism crimes to the more complete list specified in section 309 of the bill ('Federal terrorism offenses')," DoJ at 306.

[3443] U.S.Const. Art.III, §2, cl.3; Amend. IV; United States v. Cabrales, 524 U.S. 1 (1998); United States v. Rodriguez-Moreno, 526 U.S. 275 (1999).

[3444] "The list of predicate federal offenses for RICO, appearing in 18 U.S.C. §1961(1), includes none of the offenses which are most likely to be committed by terrorists. This section adds terrorism crimes to the list of RICO predicates, so that RICO can be used more frequently in the prosecution of terrorist organizations. As in various other provisions, the list of offenses in section 309 of the bill ('Federal terrorism offenses') is used in identifying the relevant crimes," DoJ, at §304.

[3445] For a general discussion, see, Wellborn, Combating Charitable Fraud: An Overview of State and Federal Law, CRS REP.NO. RS21058 (Nov. 7, 2001).

individual who convicted of a federal felony notwithstanding any lower maximum fine called for in the statute that outlaws the offense.[3446]

The proposal, however, failed to identify the critical elements that would trigger the alternative.[3447] Both practical and constitutional challenges might be thought to attend this failure to distinguish between those convicted of some "garden variety" crime of terrorism and the more serious offender meriting the alternative, supplementary penalty. Perhaps for this reason, the Act opted to simply increase the maximum penalties for various crimes of terrorism, particularly those which involve the taking of a human life and are not already capital offenses, section 810. Thus, it increases the maximum terms imprisonment for:

- for life-threatening arson or arson of a dwelling committed within a federal enclave, from 20 years to any term of years or life, 18 U.S.C. 81;
- for causing more than $100,000 in damage to, or significantly impairing the operation of an energy facility, from 10 to 20 years (or any term of years or life, if death results), 18 U.S.C. 1366;
- for providing material support to a terrorist or a terrorist organization, from 10 to 15 years (or any term of years or life, if death results), 18 U.S.C. 2339A, 2339B;
- for destruction of national defense materials, from 10 to 20 years (or any term of years or life, if death results), 18 U.S.C. 2155;
- for sabotage of a nuclear facility, from 10 to 20 years (or any term of years or life, if death results), 42 U.S.C. 2284;
- for carrying a weapon or explosive abroad an aircraft with U.S. special aircraft jurisdiction, from 15 to 20 years (or any term of years or life, if death results), 49 U.S.C. 46505; and

---

[3446] "Under existing law, the maximum prison terms for federal offenses are normally determined by specifications in the provisions which define them. These provisions can provide inadequate maxima in cases where the offense is aggravated by its terrorist character or motivation. This section accordingly adds a new subsection (e) to 18 U.S.C. §3559 which provides alternative maximum prison terms, including imprisonment for any term of years or for life, for crimes likely to be committed by terrorists. This is analogous to the maximum fine provisions of 18 U.S.C. §3571(b)-(c) – which supersede lower fine amounts specified in the statutes defining particular offenses – and will more consistently ensure the availability of sufficiently high maximum penalties in terrorism cases. As in several other provisions of this bill, the list of the serious crimes most frequently committed by terrorists set forth in section 309 of the bill ('Federal terrorism offenses' is used in defining the scope of the provision,"DoJ, at §302.

[3447] "A person convicted of any Federal terrorism offense may be sentenced to imprisonment for any term of years or for life, notwithstanding any maximum term of imprisonment specified in the law describing the offense. The authorization of imprisonment under this subsection is supplementary to, and does not limit, the availability of any other penalty authorized by the law describing the offense, including the death penalty, and does not limit the applicability of any mandatory minimum term of imprisonment, including any mandatory life term, provided by the law describing the offense," Draft at §302.

- for sabotage of interstate gas pipeline facilities, from 15 to 20 years (or any term of years or life, if death results), 49 U.S.C. 60123.

It is a separate federal offense punishable by imprisonment for not more than five years to conspire to commit any federal felony, 18 U.S.C. 371. Co-conspirators are likewise subject to punishment for the underlying offense and for any other crimes committed in furtherance of the conspiracy. Nevertheless, some federal criminal statutes impose the same penalties for both the crimes they proscribe and any conspiracy to commit them. The Justice Department urged similar treatment for crimes of terrorism.[3448] Again, the Act, in section 811, opts for a less sweeping approach and establishes equivalent sanctions for conspiracy and the underlying offense in cases of:

- arson committed within a federal enclave, 18 U.S.C. 81;
- killing committed while armed with a firearm in a federal building, 18 U.S.C. 930(c);
- destruction of communications facilities, 18 U.S.C. 1362;
- destruction of property within a federal enclave, 18 U.S.C. 1363;
- causing a train wreck, 18 U.S.C. 1922;
- providing material support to a terrorist, 18 U.S.C. 2339A;
- torture committed overseas under color of law, 18 U.S.C. 2340A;
- sabotage of a nuclear facility, 42 U.S.C. 2284;
- interfering with a flight crew within U.S. special aircraft jurisdiction, 49 U.S.C. 46504;
- carrying a weapon or explosive abroad an aircraft within U.S. special aircraft jurisdiction, 49 U.S.C. 46505; and
- sabotage of interstate gas pipeline facilities, 49 U.S.C. 60123.

When federal courts impose a sentence of a year or more upon a convicted defendant, they must also impose a term of supervised release, 18 U.S.C. 3583; U.S.S.G. §5D1.1. Supervised release is not unlike parole, except that it is ordinarily imposed in addition to (rather than in lieu of) a term, or portion of a term, of imprisonment. The term may be no longer than 5 years for most crimes and violations of the conditions of release may result in imprisonment for up to

---

[3448] "The maximum penalty under the general conspiracy provision of federal criminal law (18 U.S.C. §371) is five years, even if the object of the conspiracy is a serious crime carrying a far higher maximum penalty. For some individual offenses and types of offense, special provisions authorize conspiracy penalties equal to the penalties for the object offense – see e.g., 21 U.S.C. §846 (drug crimes) – but there is no consistently applicable provision of this type for the crimes that are likely to be committed by terrorists. "This section accordingly adds a new §2332c to the terrorism chapter of the criminal code – parallel to the drug crime conspiracy provision in 21 U.S.C. §846 – which provides maximum penalties for conspiracies to commit terrorism crimes that are equal to the maximum penalties authorized for the objects of such conspiracies. This will more consistently provide adequate penalties for terrorist conspiracies. As in various other provisions of this bill, the relevant class of offenses is specified by the notion of 'Federal terrorism offense,' which is defined in section 309 of the bill," DoJ at §303.

an additional 5 years, 18 U.S.C. 3583(e). The terms of supervisory release for drug dealers, however, are often cast as mandatory minimums with no statutory ceiling. Thus, for example, a dealer convicted of distributing more than a kilogram of heroin must receive a term of supervised release of "at least 5 years" in addition to a term of imprisonment imposed for the offense, 21 U.S.C. 841(b). Although a majority feel that the more specific drug provisions of 21 U.S.C. 841 trump the more general limitations of 18 U.S.C. 3583, some of the federal appellate courts believe the two should be read in concert where possible (e.g., at least but not more than 5 years).[3449] The Justice Department recommended a maximum supervisory term of life for those convicted of acts of terrorism (subject to the calibrations of the Sentencing Commission),[3450] a recommendation which the Act accepted in section 812 but only in the case of terrorists whose crimes resulted in death or were marked by a foreseeable risk of death or serious bodily injury, 18 U.S.C. 3583(j).

Sometime ago, Congress outlawed computer fraud and abuse (cybercrime) involving "federal protected computers" (i.e., those owned or used by the federal government or by a financial institution or used in interstate or foreign commerce), 18 U.S.C. 1030. Section 814 of the Act increases the penalty for intentionally damaging a protected computer from imprisonment for not more than 5 years to imprisonment for not more than 10 years (from not more than 10 to not more than 20 years for repeat offenders).[3451]

[3449] Compare, United States v. Barragan, 263 F.3d 919, 925-26 (9th Cir. 2001); United States v. Pratt, 239 F.3d 640, 646-48 (4th Cir. 2001); United States v. Heckard, 238 F.3d 1222, 1237 (10th Cir. 2001); and United States v. Aguayo-Delgado, 220 F.3d 926, 933 (8th Cir. 2000); with, United States v. Meshack, 225 F.3d 556, 578 (5th Cir. 2001); and United States v. Samour, 199 F.3d 821, 824-25 (6th Cir. 2001).

[3450] "Existing federal law (18 U.S.C. 3583(b)) generally caps the maximum period of post-imprisonment supervision for released felons at 3 or 5 years. Thus, in relation to a released but still unreformed terrorist, there is no means of tracking the person or imposing conditions to prevent renewed involvement in terrorist activities beyond a period of a few years. The drug laws (21 U.S.C. §841) mandate longer supervision periods for persons convicted of certain drug trafficking crimes, and specify no upper limit on the duration of supervision, but there is nothing comparable for terrorism offenses. "This section accordingly adds a new subsection to 18 U.S.C. 3583 to authorize longer supervision periods, including potentially lifetime supervision, for persons convicted of terrorism crimes. This would permit appropriate tracking and oversight following release of offenders whose involvement with terrorism may reflect lifelong ideological commitments. As in other provisions in this bill, the covered class of crimes is federal terrorism offenses, which are specified in section 390 of the bill. "This section affects only the maximum periods of post-release supervision allowed by statute. It does not limit the authority of the Sentencing Commission and the courts to tailor the supervision periods imposed in particular cases to offense and offender characteristics, and the courts will retain their normal authority under 18 U.S.C. §3583(e)(1) to terminate supervision if it is no longer warranted," DoJ at §308.

[3451] It provides a comparable increase to not more than 20 years (from not more than 10 years) for those who recklessly damage a protected computer following a prior computer abuse conviction. Civil and criminal liability for simply causing protected computer damage (as opposed to

Finally, section 1011 increases the penalty for fraudulently impersonating a Red Cross member or agent (18 U.S.C. 917) from imprisonment for not more than 1 year to imprisonment for not more than 5 years.

Other Procedural Adjustments

In other procedural adjustments designed to facilitate criminal investigations, the Act:

- increases the rewards for information in terrorism cases
- expands the Posse Comitatus Act exceptions
- authorizes "sneak and peek" search warrants
- permits nationwide and perhaps worldwide execution of warrants in terrorism cases
- eases government access to confidential information
- allows the Attorney General to collect DNA samples from prisoners convicted of any crime of violence or terrorism
- lengthens the statute of limitations applicable to crimes of terrorism
- clarifies the application of federal criminal law on American installations and in residences of U.S. government personnel overseas
- adjusts federal victims' compensation and assistance programs

A section found in the Senate bill, but ultimately dropped, would have changed the provision of law that required Justice Department prosecutors to adhere to the ethical standards of the legal profession where they conduct their activities (the McDade-Murtha Amendment), 28 U.S.C. 530B.[3452]

Rewards

The Attorney General already enjoys the power to pay rewards in criminal cases, but his powers under other authorities is often subject to caps on the amount he might pay. Thus as a general rule, he may award amounts up to $25,000 for the capture of federal offenders, 18 U.S.C. 3059, and may pay rewards in any amount in recognition of assistance to the Department of Justice as long as the Appropriations and Judiciary Committees are notified of any rewards in excess of

---

intentionally or reckless causing the damage) is limited to special circumstances, e.g., damage in excess of $5000, damage causing physical injury, etc.; section 814 adds to the list of circumstances upon which liability may be predicated. To the list of predicate circumstances, it adds causing damage to a computer used by the government for the administration of justice, national defense, or national security.

[3452] When presenting the final bill to the House, the Chairman of the Judiciary Committee noted, "the Senate bill contained revisions of the so-called McDade law. This compromise version does not contain those changes, and I agreed to review this subject in a different context," 147 Cong.Rec. H7196 (daily ed. Oct. 23, 2001)(remarks of Rep. Sensenbrenner); for general background, see, Doyle, McDade-Murtha Amendment: Ethical Standards for Justice Department Attorneys, CRS REP.NO. RL30060 (Dec. 14, 2001).

$100,000, 18 U.S.C. 3059B. Although he has special reward authority in terrorism cases, individual awards were capped at $500,000, the ceiling for the total amount paid in such rewards was $5 million, and rewards of $100,000 or more required his personal approval or that of the President, 18 U.S.C. 3071-3077. Over the last several years, annual appropriation acts have raised the $500,000 cap to $2 million and the $5 million ceiling to $10 million, e.g., P.L. 106-553, 114 Stat. 2762-67 (2000); P.L. 106-113, 113 Stat. 1501A-19 (1999); P.L.105-277, 112 Stat. 2681-66 (1998).

The Act supplies the Attorney General with the power to pay rewards to combat terrorism in any amount and without an aggregate limitation, but for rewards of $250,000 or more it insists on personal approval of the Attorney General or the President and on notification of the Appropriations and Judiciary Committees, section 501 (18 U.S.C. 3071). In addition, the counterterrorism fund of section 101 can be used "without limitation" to pay rewards to prevent, investigate, or prosecute terrorism.[3453]

The Secretary of State's reward authority was already somewhat more generous than that of the Attorney General. He may pay rewards of up to $5 million for information in international terrorism cases as long as he personally approves payments in excess $100,000, 22 U.S.C. 2708. The Act removes the $5 million cap and allows rewards to be paid for information concerning the whereabouts of terrorist leaders and facilitating the dissolution of terrorist organizations, section 502.

Posse Comitatus

The Posse Comitatus Act and its administrative auxiliaries, 18 U.S.C. 1385, 10 U.S.C. 375, ban use of the armed forces to execute civilian law, absent explicit statutory permission. One existing statutory exception covers Department of Justice requests for technical assistance in connection with emergencies involving biological, chemical or nuclear weapons, 18 U.S.C. 2332e, 10 U.S.C. 382. The Act enlarges the exception to include emergencies involving other weapons of mass destruction, section 104.[3454]

Delayed notification of a search (sneak and peek)

Rule 41 of the Federal Rules of Criminal Procedure seemed to preclude "sneak and peek" warrants before passage of the Act. A sneak and peek warrant is one that authorizes officers to secretly enter, either physically or virtually; conduct a

---

[3453] The fund is otherwise available to reestablish capacity lost in terrorist attacks, to conduct threat assessments for federal agencies, and to reimburse federal agencies for the costs of detaining terrorist suspects overseas.

[3454] For a general discussion of the Posse Comitatus Act, see, Doyle, The Posse Comitatus Act & Related Matters: The Use of the Military to Execute Civilian Law, CRS REP.NO. 95-964 (June 1, 2000).

search, observe, take measurements, conduct examinations, smell, take pictures, copy documents, download or transmit computer files, and the like; and depart without taking any tangible evidence or leaving notice of their presence. The Rule required that after the execution of a federal search warrant officers leave a copy of the warrant and an inventory of what they have seized (tangible or intangible), and they were to advise the issuing court what they had done, F.R. Crim. P. 41(d). To what extent did Rule 41 portray the standards for a reasonable search and seizure for purposes of the Fourth Amendment?

The Fourth Amendment clearly requires officers to knock and announce their purpose before entering to execute a warrant, Richards v. Wisconsin, 520 U.S. 385 (1997), but with equal clarity recognizes exceptions for exigent circumstances such as where compliance will lead to the destruction of evidence, flight of a suspect, or endanger the officers, Wilson v. Arkansas, 514 U.S. 927 (1995). It is undisputed that Title III (the federal wiretap statute) is not constitutionally invalid because it permits delayed notice of the installation of an interception device, Dalia v. United States, 441 U.S. 238 (1979). Finally, there is no doubt that the Fourth Amendment imposes no demands where it does not apply. Thus, chapter 121 (court authorization for disclosure of the contents of e-mail stored with third party service providers) may permit delayed notification of the search of e-mail in remote storage with a third party for more than 180 days without offending the Fourth Amendment, because there is no Fourth Amendment justifiable expectation of privacy under such circumstances, cf., United States v. Miller, 425 U.S. 435 (1976).

The lower federal courts are divided over the extent to which the Rule reflects Fourth Amendment requirements. The Ninth Circuit saw the Fourth Amendment reflected in Rule 41, United States v. Freitas, 800 F.2d 1451, 1453 (9th Cir. 1986).[3455] The Second Circuit was less convinced and preferred to hold

---

[3455] "The district court held that a search warrant permitting agents to observe, but not seize tangible property was impermissible under Rule 41. That holding conflicts with language in United States v. New York Telephone Co., 434 U.S. 159, 169 (1977): Although Rule 41(h) defines property to include documents, books, papers, and any other tangible objects, it does not restrict or purport to exhaustively enumerate all the items which may be seized pursuant to Rule 41. . . . Rule 41 is not limited to tangible items. That case held seizures of intangibles were not precluded by the definition of property appearing in Rule 41(b). Without doubt there was a search in this case. Its purpose, we hold, was to seize intangible, not tangible, property. The intangible property to be seized was information regarding the status of the suspected clandestine methamphetamine laboratory. The search was authorized by a warrant supported by what the district court concluded was probable cause. . . . The question remains, however, whether a warrant lacking both a description of the property to be seized and a notice requirement conforms to Rule 41. . . . we hold that there was no compliance with Rule 41 under the facts of this case. . . . While it is clear that the Fourth Amendment does not prohibit all surreptitious entries, it is also clear that the absence of any notice requirement in the warrant casts strong doubt on its constitutional adequacy. We resolve those doubts by holding that in this case the warrant was constitutionally defective in failing to provide explicitly for notice within a reasonable, but short, time subsequent to the surreptitious entry. Such time should not exceed seven days except upon a strong showing

sneak and peek searches to the demands of Rule 41, United States v. Pangburn, 983 F.2d 449 (2d Cir. 1993).[3456] The Fourth Circuit was, if anything, less convinced. Moreover, the facts in the case demonstrate the potential impact of the issue on computer privacy, United States v. Simons, 206 F.3d 392 (4th Cir. 2000).[3457]

---

of necessity. We take this position because surreptitious searches and seizures of intangibles strike at the very heart of the interests protected by the Fourth Amendment. The mere thought of strangers walking through and visually examining the center of our privacy interests, our home, arouses our passion for freedom as does nothing else. That passion, the true source of the Fourth Amendment, demands that surreptitious entries be closely circumscribed," United States v. Freitas (Freitas I), 800 F.2d 1451, 1455-456 (9th Cir. 1986). The court remanded the case for a determination of whether grounds existed for a good faith exception to application of the exclusionary rule. It subsequently declined to exclude the evidence on those grounds, United States v. Freitas (Freitas II), 856 F.2d 1425 (9th Cir. 1988).

[3456] "No provision specifically requiring notice of the execution of a search warrant is included in the Fourth Amendment. Accordingly, in Dalia v. United States, 441 U.S. 238, 247 (1979), the Supreme Court found no basis for a constitutional rule proscribing all covert entries. Resolving the particular issue raised in Dalia, the Court determined that the Fourth Amendment does not prohibit per se a covert entry performed for the purpose of installing otherwise legal electronic bugging equipment. Rule 41 of the Federal Rules of Criminal Procedure does require notice of the execution of a search warrant but does not prescribe when the notice must be given. Rule 41 by its terms provides for notice only in the case of seizures of physical property. . . . The Supreme Court also has held that the authority conferred by Rule 41 is not limited to the seizure of tangible items. See United States v. New York Telephone Co., 434 U.S. 159, 169 (1977). Despite the absence of notice requirements in the Constitution and Rule 41, it stands to reason that notice of a surreptitious search must be given at some point after the covert entry. . . .Although the Freitas I court specifically determined that the warrant was constitutionally defective for failure to include a notice requirement, we made no such determination in United States v. Villegas, 899 F.2d 1324 (1999). Although the Freitas I court found that covert entry searches without physical seizure strike at the very heart of the Fourth Amendment-protected interests, we used no such language in Villegas. Indeed, it was our perception that a covert entry search for intangibles is less intrusive than a conventional search with physical seizure because the latter deprives the owner not only of privacy but also of the use of his property. . . . We prefer to root out notice requirement in the provisions of Rule 41 rather than in the somewhat amorphous Fourth Amendment interests concept developed by the Freitas I court. The Fourth Amendment does not deal with notice of any kind, but Rule 41 does. It is from the Rule's requirements for service of a copy of the warrant and for provision of an inventory that we derive the requirements of notice in cases where a search warrant authorizes covert entry to search and to seize intangibles," United States v. Pangburn, 983 F.2d 449, 453-55 (2d Cir. 1993).

[3457] In Simons, a search team entered Simons' office at night in his absence and "copied the contents of Simons' computer; computer diskettes found in Simons' desk drawer; computer files stored on the zip drive or on zip drives diskettes; videotapes; and various documents, including personal correspondence. No original evidence was removed from the office. Neither a copy of the warrant nor a receipt for the property seized was left in the office or otherwise given to Simons at that time, and Simons did not learn of the search for approximately 45 days." A property list, however, was returned to the magistrate. In the view of the Fourth Circuit, "[t]here are two categories of Rule 41 violations; those involving constitutional violations and all others. The violations termed 'ministerial' in our prior cases obviously fall into the latter category. Nonconstitutional violations of Rule 41 warrant suppression only when the defendant is prejudiced by the violation, or when there is evidence of intentional and deliberate disregard of a provision in the Rule. First, we conclude that the failure of the team executing the warrant to

The Justice Department urged that the conflict be resolved with a uniform rule which permitted sneak and peek warrants under the same circumstances that excused delayed notification of government access to e-mail to longer-term, remote, third party storage.[3458]

The Act, in section 213, stops short of the Justice Department proposal. Characterized as a codification of the Second Circuit decision, 147 Cong. Rec. H7197 (daily ed. Oct. 23, 2001), the Act extends the delayed notification procedure of chapter 121, which operates in an area to which the Fourth Amendment is inapplicable, to cases to which the Fourth Amendment applies, 18 U.S.C. 3103a. Its sneak and peek authorization reaches all federal search and seizure warrants where the court finds reasonable cause to believe that notification would have the kind of adverse results depicted in 18 U.S.C. 2705. Section 2705 describes both exigent circumstances (e.g., risk of destruction of evidence or bodily injury) and circumstances that are not likely to excuse notification when it is required by the Fourth Amendment (e.g., jeopardizing an investigation; delaying a trial). The sneak and peek authorization, however, does not reach tangible evidence, or wire or electronic communication unless the court finds the seizure "reasonably necessary." It is not clear whether reasonable necessity means a seizure necessary to the investigation that is also reasonable in a Fourth Amendment sense, i.e., in the presence of exigent circumstances, or whether it means a seizure which a reasonable judge might find necessary for the

---

leave either a copy of the warrant or a receipt for the items taken did not render the search unreasonable under the Fourth Amendment. The Fourth Amendment does not mention notice, and the Supreme Court has stated that the constitution does not categorically proscribe covert entries, which necessarily involve a delay in notice. And insofar as the August search satisfied the requirements of the Fourth Amendment, i.e., it was conducted pursuant to a warrant based on probable cause issued by a neutral and detached magistrate, we perceive no basis for concluding that the 45-day delay in notice rendered the search unconstitutional. Having concluded that the Rule 41(d) violation at issue here did not infringe on Simons' constitutional rights, we must now evaluate his argument that the violation was deliberate. . . . The district court did not address the intent issue when it ruled on Simons' motion to suppress. . . . We therefore remand for the district court to consider whether the Government intentionally and deliberately disregarded the notice provision of Rule 41(d) when it carried out the August 6, 1998 search," 206 F.3d at 403.

[3458] "The law that currently governs notice to subjects of warrants where there is a showing to the court that immediate notice would jeopardize an ongoing investigation or otherwise interfere with lawful law enforcement activities, is a mix of inconsistent rules, practices, and court decisions varying widely from jurisdiction to jurisdiction across the country. This greatly hinders the investigation of many terrorism cases and other cases. This section resolves this problem by establishing a statutory, uniform standard for all such circumstances. It incorporates by reference the familiar, court-enforced standards currently applicable to stored communications under 18 U.S.C. §2705, and applies them to all instances where the court is satisfied that immediate notice of execution of a search warrant would jeopardize an ongoing investigation or otherwise interfere with lawful law-enforcement activities," DoJ at §353.

investigation.[3459] The doctrine of constitutional avoidance argues against the latter interpretation. By the same token, when the Act permits delay for a reasonable period, it should probably be understood to mean constitutionally "reasonable," that is, a brief period reasonable in light of the exigent circumstances which allow the delay or their like.

Nationwide terrorism search warrants

The Fourth Amendment demands that warrants be issued by a neutral magistrate, Coolidge v. New Hampshire, 403 U.S. 443 (1971); the Sixth Amendment, that crimes be prosecuted in the districts where they occur, United States v. Cabrales, 524 U.S. 1 (1998). The Federal Rules direct magistrates to issue warrants only for property within their judicial district, although they permit execution outside the district for property located in the district when the warrant is sought but removed before execution can be had, F.R. Crim. P. 41(a).

The Act, in section 219, allows a magistrate in the district in which a crime of terrorism has occurred to issue a search warrant to be executed either "within or outside the district," (F.R.Crim.P. 41(a)(3)) in domestic and international terrorism cases.[3460] The provision may anticipate execution both in this country and overseas.[3461] The Fourth Amendment does not apply to the overseas searches

---

[3459] Since neither the restriction nor its reasonable necessity exception appeared in the Justice Department's initial proposal, the Department's justification does not address the question.

[3460] The amended rule uses the definitions of domestic and international terrorism found in 18 U.S.C. 2331, as modified by section 802 of the Act: "(1) the term 'international terrorism' means activities that – (A) involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or of any State; (B) appear to be intended – (i) to intimidate or coerce a civilian population; (ii) to influence the policy of a government by intimidation or coercion; or (iii) to affect the conduct of a government by mass destruction, assassination or kidnapping; and (C) occur primarily outside the territorial jurisdiction of the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to intimidate or coerce, or the locale in which their perpetrators operate or seek asylum . . . (5) the term 'domestic terrorism' means activities that – (A) involve acts dangerous to human life that are a violation of the criminal laws of the United States or of any State; (B) appear to be intended – (i) to intimidate or coerce a civilian population; (ii) to influence the policy of a government by intimidation or coercion; or (iii) to affect the conduct of a government by mass destruction, assassination or kidnapping; and (C) occur primarily within the territorial jurisdiction of the United States," 18 U.S.C. 2331(1),(5).

[3461] The Justice Department, with whom the proposal originated, was somewhat cryptic on this point. Its analysis suggests execution in one of the several judicial districts of the United States, but not so precisely as to negate any other construction. "The restrictiveness of the existing rule creates unnecessary delays and burdens for the government in the investigation of terrorist activities and networks that span a number of districts, since warrants must be separately obtained in each district. This section resolves that problem by providing that warrants can be obtained in any district in which activities related to the terrorism may have occurred, regardless of where the warrants will be executed," DoJ at §351.

of the property of foreign nationals, United States v. Verdugo-Urquidez, 494 U.S. 259 (1990). It does apply to the search of American property overseas involving American authorities, although the lower federal courts are divided over the exact level of participation required to trigger coverage.[3462] Neither Rule 41 nor any other provision of federal law apparently contemplated extraterritorial execution, cf., F.R. Crim. P. 41, Advisory Committee Notes: 1990 Amendment (discussing a proposal for extraterritorial execution that the Supreme Court rejected).[3463]

If the Act anticipates overseas execution there may be some question whether it creates a procedure to be used in lieu of extradition when the person for whom the search warrant has been issued is located outside the United States. The section refers to warrants for "search of property or for a person within or outside the district," §219 (emphasis added). The Judicial Conference in 1990 recommended an amendment to Rule 41, which the Supreme Court rejected, that would have permitted the overseas execution of federal search warrants. In doing so, the Conference suggested extraterritorial execution be limited to warrants to search for property and not reach warrants to search for persons, "lest the rule be read as a substitute for extradition proceedings," F.R. Crim. P. 41, Advisory Committee Notes: 1990 Amendment. There is no indication, however, that the section is at odds with either the Fourth or Sixth Amendment.

[3462] United States v. Barona, 56 F.3d 1087, 1092 (9th Cir. 1995)("United States agents' participation in the investigation is so substantial that the action is a joint venture between United States and foreign officials"); United States v. Behety, 32 F.3d 503, 510 (11th Cir. 1994)("if American law enforcement officials substantially participated in the search or if the foreign officials conducting the search were actually acting as agents for their American counterparts"); United States v. Maturo, 982 F.2d 57, 61 (2d Cir. 1992)("where the conduct of foreign law enforcement officials rendered them agents, or virtual agents, of United States law enforcement officials" or "where the cooperation between the United States and foreign law enforcement agencies is designed to evade constitutional requirements applicable to American officials"); United States v. Mitro, 880 F.2d 1480, 1482 (1st Cir. 1989)("where American agents participated in the foreign search or the foreign officers acted as agents for their American counterparts"); United States v. Mount, 757 F.2d 1315, 1318 (D.C.Cir. 1985)("if American officials or officers participated in some significant way"); United States v. Marzano, 537 F.2d 257, 270 (7th Cir. 1976)(declining to adopt the "joint venture" standards, but finding level of American participation in the case before it insignificant); United States v. Morrow, 537 F.2d 120, 139 (5th Cir. 1976)("if American law enforcement officials participated in the foreign search, or if the foreign authorities actually conducting the search were acting as agents for their American counterparts"); each of the decisions also suggests that evidence secured in a manner which shocked the conscience of the court would be excluded.

[3463] The Code still carries remnants of the consular courts which speak of the overseas execution of arrest warrants in places where the United States has "extraterritorial jurisdiction," 18 U.S.C. 3042. The history of the provisions makes it clear that the phrase "extraterritorial jurisdiction" was intended to coincide with those places in which the U.S. had consular courts, see, S.Rep. 217, 73d Cong., 2d Sess. 3 (1934), reprinted, 78 Cong.Rec. 4982-983 (1934)("The countries to which the proposed bill, if enacted into law, would relate are the following, in which the United States exercises extraterritorial jurisdiction: China, Egypt, Ethiopia, Muscat, and Morocco"); 22 U.S.C. 141 (1926 ed.)(conferring judicial powers on consular courts there identified as those located in China, Egypt, Ethiopia, Muscat, Morocco, Siam and Turkey).

Terrorists' DNA

The courts have generally concluded that the collection of DNA information from convicted prisoners does not offend constitutional standards per se.[3464] Existing federal law allowed the Attorney General to collect samples from federal prisoners convicted of a variety of violent crimes, 42 U.S.C. 14135a. The Act enlarges the predicate offense list to include any crime of violence or any terrorism offense, section 503.[3465]

Access to Educational Records

Finally, the Act calls for an ex parte court order procedure under which senior Justice Department officials may seek authorization to collect educational records relevant to an investigation or prosecution of a crime of terrorism, section 507 (as an exception to the confidentiality requirements of the General Education Provisions Act, 20 U.S.C. 1232g), section 508 (as an exception to the confidentiality requirements of the National Education Statistics Act, 20 U.S.C. 9007).

Statute of Limitations

Prosecution for murder in violation of federal law may be initiated at any time, 18 U.S.C. 3281. A five year statute of limitations applied for most other federal crimes before passage of the Act, with a few exceptions. Among the relevant exceptions were an eight year statute of limitations for several terrorist offenses, 18 U.S.C. 3286,[3466] and a ten year statute of limitations for a few arson and

---

[3464] Roe v. Marcotte, 193 F.3d 72 (2d Cir. 1999); Shaffer v. Saffle, 148 F.3d 1180 (10th Cir. 1998); Rise v. Oregon, 59 F.3d 1556 (9th Cir. 1995); Jones v. Murray, 962 F.2d 302 (4th Cir. 1992).

[3465] Summarizing the law in place at the time, the Department of Justice argued that, "The statutory provisions governing the collection of DNA samples form convicted federal offenders (42 U.S.C. §14135a(d)) are restrictive, and do not include persons convicted for the crimes that are most likely to be committed by terrorists. DNA samples cannot now be collected even from persons federally convicted of terrorist murders in most circumstances. For example, 49 U.S.C. §46502, which applies to terrorists who murder people by hijacking aircraft, 18 U.S.C. §844(i), which applies to terrorists who murder people by blowing up buildings, and 18 U.S.C. 2332, which applies to terrorists who murder U.S. nationals abroad, are not included in the qualifying federal offenses for purposes of DNA sample collection under existing law. This section addresses the deficiency of the current law in relation to terrorists by extending DNA sample collection to all persons convicted of terrorism crimes," DoJ at §353. For a general discussion, see, Fischer, DNA Identification: Applications and Issues, CRS REP.NO. RL30717 (Jan. 12, 2001).

[3466] 18 U.S.C. 32 (destruction of aircraft or aircraft facilities), 37 (violence at international airports), 112 (assaults on foreign dignitaries), 351 (crimes of violence against Members of Congress), 1116 (killing foreign dignitaries), 1203 (hostage taking), 1361 (destruction of federal property), 1751 (crimes of violence against the President), 2280 (violence against maritime navigation), 2281 (violence on maritime platforms), 2332 (terrorist violence against Americans overseas), 2332a (use of weapons of mass destruction), 2332b (acts of terrorism transcending national boundaries), 2340A (torture); 49 U.S.C. 46502 (air piracy), 46504 (interference with a

explosives offenses, 18 U.S.C. 3295. The Justice Department recommended the elimination of a statute of limitations in terrorism cases.[3467]

The Act takes less dramatic action in section 809. It eliminates the statute of limitations for any crime of terrorism[3468] that risks or results in a death or serious bodily injury, 18 U.S.C. 3286. In the absence of such a risk or result, all other terrorism offenses become subject to the eight year statute of limitations unless already covered by the ten year statute for explosives and arson offenses, 18 U.S.C. 3286.

---

flight crew), 46505 (carrying a weapon aboard an aircraft), and 46506 (assault, theft, robbery, sexual abuse, murder, manslaughter or attempted murder or manslaughter in the special aircraft jurisdiction of the United States).

[3467] "This section amends 18 U.S.C. §3286 to provide that terrorism of offenses may be prosecuted without limitation of time. This will make it possible to prosecute the perpetrators of terrorist acts whenever they are identified and apprehended. "This section expressly provides that it is applicable to offenses committed before the date of enactment of the statute, as well as those committed thereafter. This retroactivity provision ensures that no limitation period will bar the prosecution of crimes committed in connection with the September 11, 2001 terrorist attacks. The constitutionality of such retroactive applications of changes in statutes of limitations is well-settled, See, e.g., United States v. Grimes, 142 F.3d 1342, 1350-51 (11th Cir. 1998); People v. Frazer, 982 P.2d 180 (Cal. 1999). "Existing federal law (18 U.S.C. §3282) bars prosecuting most offenses after five years. 18 U.S.C. §3286, as currently formulated, extends the limitation period for prosecution for certain offenses that may be committed by terrorists – but only to eight years. While this is a limited improvement over the five-year limitation period for most federal offenses, it is patently inadequate in relation to the catastrophic human and social costs that frequently follow from such crimes as destruction of aircraft (18 U.S.C. §32), aircraft hijackings ([49] U.S.C. §§46502, 46504-06, attempted political assassinations (18 U.S.C. §§351, 1116, 1751), or hostage taking (18 U.S.C. §1203). These are not minor acts of misconduct which can properly be forgiven or forgotten merely because the perpetrator has avoided apprehension for some period of time. Anomalously, existing law provides longer limitation periods for such offenses as bank frauds and certain artwork thefts (18 U.S.C.§§3293-94) than it does for crimes characteristically committed by terrorists. "In many American jurisdictions, the limitation periods for prosecution for serious offenses are more permissible than those found in federal law, including a number of states which have no limitation period for the prosecution of felonies generally. While this section does not go so far, it does eliminate the limitation period for prosecution of the major crimes that are most likely to be committed by terrorists ('Federal terrorism offenses'), as specified in section 309 of this bill," DoJ at 301.

[3468] As defined by 18 U.S.C. 2332b(g)(5)(B), with the amendments of §808, this includes, in addition to the offenses already listed in 18 U.S.C. 3296 – 18 U.S.C. 81 (arson within U.S. special maritime and territorial jurisdiction); 175 & 175b (biological weapons); 229 (chemical weapons); 831 (nuclear weapons); 842(m) & (n) (plastic explosives); 844(f)(bombing federal property where death results); 844(i)(bombing property used in interstate commerce); 930(c)(possession of a firearm in a federal building where death results), 956(a)(conspiracy within the U.S. to commit murder, kidnapping, or to maim overseas); 1030(a) (1), (5)(A)(i), (5)(B)(ii)-(v)(computer abuse); 1114 (killing federal officers or employees); 1362 (destruction of communications facilities); 1363 (malicious mischief within the U.S. special maritime and territorial jurisdiction); 1366(a)(destruction of an energy facility); 1992 (train wrecking); 1993 (terrorist attack on mass transit); 2155 (destruction of national defense materials); 2339 (harboring terrorists); 2339A (material support to terrorists), 2339B (material support to terrorist organizations); 42 U.S.C. 2284 (sabotage of nuclear facilities); and 49 U.S.C. 60123(b)(destruction of pipeline facilities).

Application of the statute of limitations rarely provokes a constitutional inquiry. Nevertheless, due process precludes prosecution when it can be shown that pre-indictment delay "caused substantial prejudice to [a defendant's] rights to a fair trial and that the delay was an intentional device to gain tactical advantage over the accused."[3469] Moreover, a judicial difference of opinion has appeared in those cases when an existing period of limitation is enlarged legislatively and the new period made applicable to past offenses. The lower federal courts have long noted that the Constitution poses no impediment to enlarging a period of limitation as long as it does not revive an expired period.[3470] Recently, however, the California Supreme Court held that retroactive revival of an expired statute of limitations offended neither the California nor the United States Constitution.[3471]

Section 809 applies "to the prosecution of any offense committed before, on, or after the date of enactment of this section," the very words used in the Justice Department proposal. The Justice Department, in describing its proposal, cited both federal law (Grimes, where the court held that extensions may be applied where the earlier period of limitations has not expired) and California law (Frazer, where the court held that extensions may revive an expired period of limitations). The implication is that the Justice Department understood its proposal to apply to past offenses whether the earlier statute of limitations had expired or not. Other than its use of identical terminology, Congress gave no hint of whether it intended to adopt this view for section 809. Whether the federal courts could be persuaded to overcome their previously expressed constitutional reservations is equally uncertain.

Extraterritoriality

Crime is usually outlawed, prosecuted and punished where it is committed. In the case of the United States, this is ordinarily a matter of practical and diplomatic preference rather than constitutional necessity. Consequently, although prosecutions are somewhat uncommon, a surprising number of federal criminal laws have extraterritorial application. In some instances, the statute proscribing the misconduct expressly permits the exercise of extraterritorial jurisdiction, 18 U.S.C. 2381 (treason) ("Whoever, owing allegiance to the United States . . . within the United States or elsewhere. . ."). In others, such as those banning assassination of Members of Congress, 18 U.S.C. 351, or the murder of federal law

---

[3469] United States v. Marion, 404 U.S. 307, 325 (1971); United States v. Lovasco, 431 U.S. 783,790 (1977).

[3470] United States v. De La Matta, 266 F.3d 1275, 1286 (11th Cir. 2001); United States v. Grimes, 142 F.3d 1342, 1351 (11th Cir. 1998); United States v. Morrow, 177 F.3d 272, 294 (5th Cir. 1999); Falter v. United States, 23 F.2d 420, 425-26 (2d Cir. 1928).

[3471] People v. Frazer, 24 Cal.4th 737, 759, 982 P.2d 180, 1294, 88 Cal.Rptr.2d 312, 327 (1999).

enforcement officers, 18 U.S.C. 1114, the courts have assumed Congress intended the prohibitions to have extraterritorial reach.[3472]

The Act touches upon extraterritoriality only to a limited extent and in somewhat unusual ways. Congress has made most common law crimes – murder, sexual abuse, kidnaping, assault, robbery, theft and the like – federal crimes when committed within the special maritime and territorial jurisdiction of the United States. The special maritime and territorial jurisdiction of the United States represents two variations of extraterritorial jurisdiction.

The special maritime jurisdiction of the United States extends to the vessels of United States registry. Historically, the territorial jurisdiction of the United States was thought to reach those areas over which Congress enjoyed state-like legislative jurisdiction. For some time, those territories were located exclusively within the confines of the United States, but over the years they came to include at least temporarily, Hawaii, the Philippines, and several other American overseas territories and possessions. Recently, the lower federal courts have become divided over the question of whether laws, enacted to apply on federal enclaves within the United States and within American territories overseas, might also apply to areas in foreign countries over which the United States has proprietary control.[3473]

The Act resolves the conflict by declaring within the territory of the United States those overseas areas used by American governmental entities for their activities or residences for their personnel, at least to the extent that crimes are committed by or against an American, section 804 (18 U.S.C. 7 (9)). The section is inapplicable where it would otherwise conflict with a treaty obligation or where the offender is covered by the Military Extraterritorial Jurisdiction Act, 18 U.S.C. 3261.

Victims

Federal law has provided for crime victim compensation and assistance programs for some time. Moreover, Congress enacted September 11th Victim Compensation Fund legislation before it passed the Act. Consequently, the Act's victim provisions focus on adjustments to existing programs, primarily to those

---

[3472] United States v. Layton, 855 F.2d 1388 (9th Cir. 1988)(at the time of the overseas murder of Congressman Ryan for which Layton was convicted the statute was silent as to its extraterritorial application; several years later Congress added an explicit extraterritorial provision, 18 U.S.C. 351(i)); United States v. Benitez, 741 F.2d 1312 (11th Cir. 1984)(18 U.S.C. 1114 has since expanded to protect all federal officers and employees, including members of the armed forces and those assisting them).

[3473] Compare, United States v. Gatlin, 216 F.3d 207 (2d Cir. 2000); United States v. Laden, 92 F.Supp.2d 189 (S.D.N.Y. 2000); with, United States v. Corey, 232 F.3d 1166 (9th Cir. 2000); United States v. Erdos, 474 F.2d 157 (4th Cir. 1973).

of the Victims of Crime Act of 1984, 42 U.S.C. 10601 et seq., and to those maintained for the benefit of public safety officers and their survivors, 42 U.S.C. 3796 et seq.

Public safety officers - police officers, firefighters, ambulance and rescue personnel -killed or disabled in the line of duty (and their heirs) are entitled to federal benefits. Prior to the Act, death benefits were set at $100,000 and the total amount available for disability benefits in a given year was capped at $5 million, 42 U.S.C. 3796 (2000 ed.). No benefits could be paid for suicides, if the officer was drunk or grossly negligent, if the beneficiary contributed to the officer's death or injury, or if the officer were employed other than in a civilian capacity, 42 U.S.C. 3796 (2000 ed.). The Act increases the death benefit to $250,000 (retroactive to January 1, 2001), section 613; and for deaths and disability connected with acts of terrorism waives the $5 million disability cap and the disqualifications for gross negligence, contributing cause, or employment in a noncivilian capacity, section 611.

Most of fines collected for violation of federal criminal laws are deposited in the Crime Victims Fund which is available for child abuse prevention and treatment grants, victim services within the federal criminal justice system, and grants to state victim compensation and victim assistance programs, 42 U.S.C. 10601 to 10608. The Act:

- authorizes private contributions to the fund (42 U.S.C. 10601(b)), section 621(a)
- instructs the Department of Justice, which administers the fund, to distribute in every fiscal year (if amounts in the Fund are sufficient) amounts equal to between 90% and 110% of the amount distributed in the previous fiscal year (120% in any year when the amount on hand is twice the amount distributed the previous year)(42 U.S.C. 10601(c)), section 621(b)
- reduces by 1% the amounts available for compensation and assistance grants (from 48.5% to 47.5% after child abuse and federal victim priorities have been met), and increases from 3% to 5% the amount available for Justice Department discretionary spending for demonstration projects and services to assist the victims of federal crimes (42 U.S.C. 10601(d), 10603(c)), section 621(c)
- converts the general reserve fund to an antiterrorism reserve fund and reduces the cap on the reserve from $100 million to $50 million (42 U.S.C. 10601(d) (5)), section 621(d)
- waives the Fund's availability caps with respect to funds transferred to it in response to the terrorist attacks of September 11 (42 U.S.C. 10601 note)), section 621(e)
- lowers the annual reduction rate on individual compensation program grants; beginning in 2003 individual grants are limited to 60% (rather than 40%) of the amount of awarded in the previous year (42 U.S.C. 10602(a)), section 622(a)

- eliminates the requirement that state compensation programs permit compensation for state residents who are the victims of terrorism overseas (42 U.S.C. 10602(b)(6)(B)), section 622(b)
- provides that compensation under the September 11th Victim Compensation Fund should be counted as income in considering eligibility for any federal indigent benefit program (42 U.S.C. 10602(c)), section 622(c)
- drops "crimes involving terrorism" from the definition of "compensable crime"; it is unclear whether the phrase was removed as redundant or pursuant to a determination to compensate victims other than through the Crime Victims Fund (42 U.S.C. 10602(d)), section 622(d)(1)
- makes it clear that the Virgin Islands is eligible to receive grants (42 U.S.C. 10602(d)), section 622(d)(2)
- adds the September 11th Victim Compensation Fund to the "double dipping" restriction that applies to the victim compensation programs and confirms that state compensation programs will not be rendered ineligible for grants by virtue of a refusal to pay dual compensation to September 11th Fund victims (42 U.S.C. 10602(e)), section 622(e)
- makes federal agencies performing law enforcement functions in the District of Columbia, Puerto Rico, the Virgin Islands, and other U.S. territories and possessions eligible for victim assistance grants (42 U.S.C. 10603(a)(6)), section 623(a)
- prohibits program discrimination against crime victims based on their disagreement with the manner in which the state is prosecuting the underlying offense (42 U.S.C. 10603(b)(1)(F)), section 623(b)
- allows Justice Department discretionary grants for purposes of program evaluation and compliance and for fellowships, clinical internships and training programs (42 U.S.C. 10603(c)(1)(A), (3)(E)), section 623(c),(e)
- reverses the preference for victim service grants over demonstration projects and training grants, so that not more than 50% of the amounts available for crime victim assistance grants shall be used for victim service grants and not less than 50% for demonstration projects and training grants (42 U.S.C. 10603(c)(2)), section 623(d)
- makes federal and local agencies and private entities eligible for supplemental grants for services relating to victims of terrorism committed within the U.S. (42 U.S.C. 10603b(b)), section 624(a)
- allows supplemental grants for services relating to victims of terrorism committed overseas regardless of whether the victims are eligible for compensation under Title VIII of the Omnibus Diplomatic Security and Antiterrorism Act (100 Stat. 879 (1986))(Title VIII victims were previously ineligible) (42 U.S.C. 10603b(a)(1)), section 624(b)
- establishes a "double dipping" restriction under which compensation to the victims of overseas terrorism is reduced by the amount received under Title VIII of the Omnibus Act (42 U.S.C. 10603c(b)), section 624(c)

Increasing Institutional Capacity

A major portion of the Act is devoted to bolstering the institutional capacity of federal law enforcement agencies to combat terrorism and other criminal threats. In addition to the counterterrorism discussed above in the context of the Attorney General's reward prerogatives, it increases funding authorization for an FBI technical support center, section 103, and allows the FBI to hire translators without regard to otherwise applicable employment restrictions such as citizenship, section 205.

In the area of cybercrime, the Attorney General is instructed to establish regional forensic laboratories, section 817, and the Secret Service, to establish a national network of electronic crime task forces, modeled after its New York Electronic Crimes Task Force, section 105. The Act likewise clarifies the Secret Service's investigative jurisdiction with respect to computer crime (18 U.S.C. 1030) and to crimes involving credit cards, PIN numbers, computer passwords, or any frauds against financial institutions (18 U.S.C. 3056), section 506.

For a period of up to 180 days after the end of Operation Enduring Freedom, section 1010 allows the Department of Defense (DoD) to contract with state and local law enforcement authorities to perform various security functions on its military installations and facilities, 10 U.S.C. 2465.

The Act also authorizes appropriations for wide range anti-terrorism purposes including:

- $25 million a year for FY 2003 through FY 2007 for state and local terrorism prevention and antiterrorism training grants for first responders, section 1005 (28 U.S.C. 509 note)
- necessary sums (FY 2002 through FY 2007) for Office of Justice Programs (OJP) grants to state and local governments to enhance their capacity to respond to terrorist attacks, section 1014 (42 U.S.C. 3711)
- $250 million a year (FY 2002 through FY 2007) for OJP grants to state and local governments integrated information and identification systems, section 1015 (42 U.S.C. 14601)
- $50 million per fiscal year for the Attorney General to develop and support regional computer forensic laboratories (28 U.S.C. 509 note), section 816
- $50 million (FY 2002) and $100 million (FY 2003) for Bureau of Justice Assistance grants (42 U.S.C. 3796h) for federal-state-local law enforcement information sharing systems, section 701
- $20 million (FY 2002) for the activities of National Infrastructure Simulation and Analysis Center in DoD's Defense Threat Reduction Agency, section 1016 (42 U.S.C. 5195c)
- $5 million for DEA police training in South and Central Asia, section 1007.

Miscellaneous

Finally, the Act addresses the issuance of licenses for the drivers of vehicles carrying hazardous materials and the use of trade sanctions against countries that support terrorism.

The Act requires background checks for criminal records and immigration status of applicants for licenses to operate vehicles carrying hazardous materials including chemical and biological materials (49 U.S.C. 5101a), section 1012.

The Trade Sanctions Reform and Export Enhancement Act, 22 U.S.C. 7201 to 7209, limits the President's authority to unilaterally impose export restrictions on food and medical supplies. The limitations do not apply to restrictions on products that might be used for the development or production of chemical or biological weapons or of weapons of mass destruction, 22 U.S.C. 7203(2)(c). The Act expands the exception to include products that might to used for the design of chemical or biological weapons or of weapons of mass destruction as well, section 221(a)(1).

Only one year licenses may be issued for trade with countries that sponsor terrorism, 22 U.S.C. 7205. The Act brings areas of Afghanistan controlled by the Taliban within the same restriction, section 221(a)(2).

Neither of these changes or anything else in the trade sanctions legislation precludes the assessment of civil or criminal liability for violations of 18 U.S.C. 2339A (providing support to terrorists), of 18 U.S.C. 2339B (providing support to terrorist organizations), or of various presidential orders under the International Emergency Economic Powers Act,[3474] or of restrictions on foreign involvement in weapons of mass destruction or missile proliferation, sections 221(b), 807.[3475]

[3474] I.e., Executive Order No. 12947, 50 U.S.C. 1701 note (prohibiting transactions with terrorists); Executive Order No. 13224, 50 U.S.C. 1701 note (blocking property of persons who support terrorism); Executive Order No. 12978, 50 U.S.C. 1701 note (blocking assets of significant narcotics traffickers).

[3475] For a general discussion of trade sanctions legislation, see, Jurenas, Exempting Food and Agriculture Products from U.S. Economic Sanctions: Status and Implementation, CRS ISSUE BRIEF IB100061.

USA PATRIOT Improvement and Reauthorization Act of 2005: A Legal Analysis, RL33332 (December 21, 2006)

BRIAN T. YEH & CHARLES DOYLE, CONG. RESEARCH SERV., USA PATRIOT IMPROVEMENT AND REAUTHORIZATION ACT OF 2005: A LEGAL ANALYSIS (2006), *available at* http://www.intelligencelaw.com/library/secondary/crs/pdf/RL33332_12-21-2006.pdf.

Order Code RL33332
Updated December 21, 2006

Brian T. Yeh
Legislative Attorney
American Law Division

Charles Doyle
Senior Specialist American Law Division

Summary

Several sections of the USA PATRIOT Act and one section of the Intelligence Reform and Terrorism Prevention Act of 2004 were originally scheduled to expire on December 31, 2005. In July 2005, both Houses approved USA PATRIOT reauthorization acts, H.R. 3199 and S. 1389, and the conference committee filed a report, H.Rept. 109-333. A separate bill, the USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006 (S. 2271), provided civil liberties safeguards not included in the conference report. Both H.R. 3199 and S. 2271 were signed into law (P.L. 109-177 and P.L. 109-178) by the President on March 9, 2006.

This report describes the USA PATRIOT Improvement and Reauthorization Act of 2005 (the Act) and, where appropriate, discusses the modifications to law made by the USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006. Consisting of seven titles, the Act, among other things:

- Makes permanent 14 of the 16 expiring USA PATRIOT Act sections as well as the material support of terrorism amendments scheduled to expire on December 31, 2006.
- Creates a new sunset of December 31, 2009, for USA PATRIOT Act sections 206 and 215 ("roving" FISA wiretaps and FISA orders for business records), and for the "lone wolf" amendment to FISA.
- Provides for greater congressional and judicial oversight of section 215 orders, section 206 roving wiretaps, and national security letters.

- Requires high-level approval for section 215 FISA orders for library, bookstore, firearm sale, medical, tax return, and educational records.
- Enhances procedural protections and oversight concerning delayed notice, or "sneak and peek" search warrants.
- Expands the list of predicate offenses in which law enforcement may obtain wiretap orders to include more than 20 federal crimes.
- Revises criminal penalties and procedures concerning criminal and terrorist activities committed at seaports or aboard vessels.
- Reenforces federal money laundering and forfeiture authority, particularly in connection with terrorist offenses.
- Allows the Attorney General to determine whether a state qualifies for expedited habeas corpus procedures for state death row inmates.
- Establishes a new National Security Division within the Department of Justice (DOJ), supervised by a new Assistant Attorney General.
- Creates a new federal crime relating to misconduct at an event designated as a "special event of national significance," whether or not a Secret Service protectee is in attendance.
- Intensifies federal regulation of foreign and domestic commerce in methamphetamine precursors.

Much of the information contained in this report may also be found under a different arrangement in CRS Report RL33239, *USA PATRIOT Improvement and Reauthorization Act of 2005: Section-by-Section Analysis of the Conference Bill*.

Introduction

By operation of section 224 of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act) of 2001,[3476] several of the USA PATRIOT Act's amendments to the Foreign Intelligence Surveillance Act (FISA)[3477] and the Electronic Communications Privacy Act (ECPA)[3478] concerning law enforcement and intelligence investigative tools, were originally scheduled to expire on December 31, 2005.[3479] Section 6001(a) of the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004 (concerning "lone wolf" terrorists) was also scheduled to sunset on that date. Without any legislative action, these provisions as well as amendments to them would have ceased to exist after the sunset date, and most of the pre-existing provisions of law would have been revived automatically.

[3476] P.L. 107-56, 115 Stat. 272 (2001).

[3477] 50 U.S.C. 1801-1862.

[3478] 18 U.S.C. 2510-2522, 2701-2712, 3121-3127.

[3479] 115 Stat. 295 (2001).

During the 109th Congress, the House and Senate each passed USA PATRIOT Reauthorization Acts, H.R. 3199 and S. 1389 respectively,[3480] which made permanent 14 of the 16 expiring USA PATRIOT Act sections and extended the sunset on section 206 (regarding FISA court orders for multipoint, or "roving," wiretaps) and section 215 (access to business records requested under FISA), as well as the sunset on section 6001(a) of IRTPA. The two bills differed in several respects, including the new sunset date (under S. 1389, December 31, 2009, while H.R. 3199 offered a ten-year extension to December 31, 2015). On December 8, 2005, House and Senate conference committee members filed a report representing a compromise between the Senate version and the version passed by the House, H.Rept. 109-333 (2005).

The House agreed to the conference report accompanying H.R. 3199 on December 14, 2005. However, with several Members of the Senate raising concerns about the sufficiency of the conference report's safeguards for civil liberties, the Senate voted to reject a motion to invoke cloture on the conference report, thus taking no action before the end of 2005. To provide the Senate with additional time to consider the conference report, Congress enacted legislation to postpone the expiration of the USA PATRIOT Act provisions and of IRTPA's "lone wolf" amendment,[3481] until February 3, 2006,[3482] and thereafter further extended the sunset until March 10, 2006.[3483]

On March 1, 2006, the Senate passed a separate bill, the USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006 (S. 2271), that provides three civil liberties safeguards not included in the conference report.[3484] Passage of S. 2271 helped to pave the way for the Senate to invoke cloture on the conference report upon reconsideration, and the Senate agreed to the conference report on

---

[3480] H.R. 3199 was introduced by Representative Sensenbrenner; S. 1389 by Senator Specter for himself and Senators Feinstein and Kyl. H.R. 3199 was reported by committee, H.Rept. 109-174, and initially passed the House on July 21, 2005, 151 CONG. REC.H6308-309 (daily ed. July 21, 2005). The Senate by unanimous consent substituted the text of S. 1389, as reported by the Judiciary Committee, after striking all but the enacting clause from H.R. 3199, 151 CONG. REC. S9559, S9562 (daily ed. July 29, 2005). The Record, however, reprints the House-passed bill and identifies it as H.R. 3199 as passed by the Senate, 151 CONG. REC. S9562-9579 (daily ed. July 29, 2005). For purposes of convenience, we assume that the Senate-passed version of H.R. 3199 is S. 1389 as reported and will refer to it as S. 1389.

[3481] P.L. 108-458, 118 Stat. 3742 (2004).

[3482] P.L. 109-160, 119 Stat. 2957 (2005).

[3483] P.L. 109-170, 120 Stat. 3 (2006).

[3484] Technically, these provisions were not amendments to the conference report itself, but rather the bill amended specified sections of FISA and the national security letter statutes *after* they have been amended by H.R. 3199.

March 2. Under suspension of the rules, the House passed S. 2271 on March 7, and both H.R. 3199 and S. 2271 were signed into law by the President on March 9.

This report provides a summary and legal analysis of the USA PATRIOT Improvement and Reauthorization Act of 2005 (the "Act" or the "Reauthorization Act"), P.L. 109-177, 120 Stat. 192 (2006), and, where appropriate, discusses the modifications to law made by the USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006, P.L. 109-178, 120 Stat. 278 (2006). For organizational purposes, the report is divided according to the seven titles of the Act and, within those titles, arranged by topic headings.

Title I: USA PATRIOT Improvement and Reauthorization Act

Title I is in many ways the heart of the Act. It makes permanent most of the USA PATRIOT Act sections that were scheduled to expire. To several, like section 215, it adds substantive changes such as civil liberties safeguards. It addresses issues raised by USA PATRIOT Act sections other than those for which the sun was setting. It more clearly states the "National Security Letter" provisions of law, in ways perhaps necessary to make them constitutionally viable. Elsewhere, it looks at the issues faced in the USA PATRIOT Act four years after the fact. In some instances it adds to the tools available; in others it adds further checks against abuse.

Temporary USA PATRIOT Act Sections Made Permanent

Section 102(a) of the Act repeals section 224 of the USA PATRIOT Act that had mandated 16 of its sections to expire initially on December 31, 2005, and later extended to March 10, 2006 by P.L. 109-170, 120 Stat. 3 (2006). Although the Act adopts a new sunset date on two of the sections, as discussed below, it makes permanent the following 14 sections:

(1) Sec. 201 (ECPA wiretapping in certain terrorism investigations)
(2) Sec. 202 (ECPA wiretapping in computer fraud and abuse investigations)
(3) Sec. 203(b) (law enforcement sharing of court-ordered wiretap-generated foreign intelligence information wiretap information)
(4) Sec. 203(d) (law enforcement sharing of foreign intelligence information notwithstanding any other legal restriction)
(5) Sec. 204 (technical exception for foreign intelligence pen register/trap & trace device use)
(6) Sec. 207 (duration of FISA wiretap and search orders involving agents of a foreign power)
(7) Sec. 209 (seizure of stored voice mail by warrant rather than ECPA order)
(8) Sec. 212 (communications providers emergency disclosures of communications content or related records to authorities)

(9) Sec. 214 (FISA pen register order amendments including extension to electronic communications, e.g., Internet use)
(10) Sec. 217 (law enforcement access to computer trespassers' communications within the intruded system)
(11) Sec. 218 (FISA wiretap or search orders with an accompanying law enforcement purpose [removal of "the wall" of separation between criminal catchers and spy catchers])
(12) Sec. 220 (nationwide service of court orders directed to communication providers)
(13) Sec. 223 (civil liability and disciplinary action for certain ECPA or FISA violations)
(14) Sec. 225 (civil immunity for assistance in executing a FISA order)

USA PATRIOT Act Sections Still Subject to Sunset

The Act adopts a sunset of December 31, 2009, for USA PATRIOT Act sections 206 (regarding FISA court orders for multipoint, or "roving," wiretaps) and 215 (access to business records requested under FISA).[3485]

Extension of the "Lone Wolf" Amendment, and the Material Support of Terrorism Amendments Made Permanent

The Act makes two changes to the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004, P.L. 108-458, 118 Stat. 3638 (2004). First, it postpones the expiration of section 6001(a) of IRTPA, 118 Stat. 3742 (2004), until December 31, 2009.[3486] Section 6001(a) defines an "agent of a foreign power" to include any person, other than a United States person, who "engages in international terrorism or activities in preparation therefore."[3487] Thus, so-called "lone wolf" terrorists may be subjected to foreign intelligence surveillance despite not being an agent of a foreign power or an international terrorist organization.[3488]

Second, the Act makes permanent section 6603 of IRTPA by repealing the sunset provision (section 6603(g)) that would have caused the section to be ineffective on December 31, 2006.[3489] Section 6603 of IRTPA amends federal law regarding material support of terrorists and terrorist organizations, primarily in 18 U.S.C.

[3485] § 102(b), P.L. 109-177, 120 Stat. 195 (2006).

[3486] § 103, P.L. 109-177, 120 Stat. 195 (2006).

[3487] 50 U.S.C. 1801(b)(1)(C).

[3488] For more information on the "lone wolf" amendment, see CRS Report RS22011, *Intelligence Reform and Terrorism Prevention Act of 2004: "Lone Wolf" Amendment to the Foreign Intelligence Surveillance Act*, by Elizabeth B. Bazan and Brian T. Yeh.

[3489] § 104, P.L. 109-177, 120 Stat. 195 (2006).

2339A[3490] and 2339B.[3491] Briefly, section 6603: (1) amends the definitions of "material support or resources," "training," and "expert advice or assistance" as those terms are used in 18 U.S.C. 2339A and 2339B, and of "personnel" as used in section 2339B; (2) adds a more explicit knowledge requirement to section 2339B; (3) expands the extraterritorial jurisdiction reach of section 2339B; (4) enlarges the list of federal crimes of terrorism, 18 U.S.C. 2332b(g)(5); (5) adds the enlarged list to the inventory of predicate offenses for 18 U.S.C. 2339A (material support for the commission of certain terrorist crimes) and consequently for 18 U.S.C. 2339B (material support for designated terrorist organizations); and (6) precludes prosecution for certain violations committed with the approval of the Secretary of State and concurrence of the Attorney General.[3492]

Section 215 FISA Orders for "Business Records"

Section 215 of the USA PATRIOT Act amended the business record sections of FISA to authorize the Director of the Federal Bureau of Investigation (FBI) or a designee of the Director, to apply to the FISA court to issue orders granting the government access to any tangible item (including books, records, papers, and other documents), no matter who holds it, in foreign intelligence, international terrorism, and clandestine intelligence cases.[3493] The Act contains several

---

[3490] Section 2339A outlaws providing, attempting to provide, or conspiring to provide, material support or resources for the commission of any of several designated federal crimes that a terrorist might commit.

[3491] Section 2339B outlaws providing, attempting to provide, or conspiring to provide, material support or resources to a designated foreign terrorist organization.

[3492] For more information regarding section 6603 of IRTPA, see CRS Report RL33035, *Material Support of Terrorists and Foreign Terrorist Organizations: Sunset Amendments*, by Charles Doyle.

[3493] Section 215 authority appears to have been relatively little used. In April 2005, Justice Department officials testified to the House Judiciary Committee that, as of March 31, 2005, only 35 orders have been issued under section 215 authority, none of which involved library, book store, medical, or gun sale records. Oversight Hearing on the "Implementation of the USA PATRIOT Act: Foreign Surveillance Intelligence Act (FISA)": Hearings Before the Subcomm. on Crime, Terrorism, and Homeland Security of the House Comm. on the Judiciary, 109th Cong., 1st Sess. (2005) (statement of Kenneth L. Wainstein, U.S. Attorney for the District of Columbia), at 8, available on Jan. 13, 2006 at [http://judiciary.house.gov/media/pdfs/wainstein042805.pdf]. At the same time, the Justice Department argues against the creation of a safe haven in public services that terrorists have been known to use. Oversight Hearing on the "Implementation of the USA PATRIOT Act: Foreign Surveillance Intelligence Act (FISA)": Hearings Before the Subcomm. on Crime, Terrorism, and Homeland Security of the House Comm. on the Judiciary, 109th Cong., 1st Sess. (2005) (statement of James A. Baker, Counsel for Intelligence Policy, Office of Intelligence Policy and Review, U.S. Dep't of Justice), at 3, available on Jan. 13, 2006 at [http://judiciary.house.gov/media/pdfs/baker042805.pdf] ("While section 215 has never been used to obtain such records, last year, a member of a terrorist group closely affiliated with al

provisions to guard against abuses of section 215 authority, including greater congressional oversight, enhanced procedural protections, more elaborate application requirements, and a judicial review process.

Greater Congressional Oversight

Section 106(h) of the Act directs the Attorney General to submit to Congress an annual report regarding the use of section 215 authority. This report is to be filed with the House and Senate Committees on the Judiciary, the House Permanent Select Committee on Intelligence, and the Senate Select Committee on Intelligence. The annual report, due every April, must contain the following information regarding the preceding year:

- the total number of applications made for section 215 production orders ("215 orders") approving requests for the production of tangible things,
- the total number of such orders granted as requested, granted as modified, or denied, and
- the number of 215 orders either granted, modified, or denied for the production of each of the following: library circulation records, library patron lists, book sales records, or book customer lists; firearms sales records; tax return records; educational records; and medical records containing information that would identify a person.[3494]

Prior to the Act, the law had required public disclosure of only the first two items listed above; by adding the third reporting requirement, the Act provides for a more detailed account of whether and when section 215 authority has been used to request these categories of sensitive information.

Section 106A of the Act provides for the Inspector General of the Department of Justice to conduct a comprehensive audit to determine the effectiveness, and identify any abuses, concerning the use of section 215 authority, for calendar years 2002-2006. The audit is to be performed in accordance with the detailed requirements set forth in this section. The results of the audit are to be submitted in an unclassified report to the House and Senate Committees on the Judiciary and Intelligence; for calendar years 2002, 2003, and 2004, the report is due not later than March 9, 2007; for calendar years 2005 and 2006, the report is due not later than December 31, 2007.

Enhanced Procedural Protections

Qaeda used Internet service provided by a public library to communicate with his confederates. Furthermore, we know that spies have used public library computers to do research to further their espionage and to communicate with their co-conspirators ... . A terrorist using a computer in a library should not be afforded greater privacy protection that a terrorist using a computer in his home.").

[3494] §106(h)(2), P.L. 109-177, 120 Stat. 200 (2006), adding new 50 U.S.C. 1862(b)(3).

Section 106(a)(2) of the Act adds 50 U.S.C. 1861(a)(3), requiring that an application for a 215 order for the production of certain sensitive categories of records, such as library, bookstore, firearm sales, tax return, educational, and medical records, must be personally approved by one of the following three high-level officials: the FBI Director, the FBI Deputy Director, or the Executive Assistant Director for National Security. This provision was included as an attempt to allay concerns over federal authorities abusing section 215 authority to obtain sensitive types of records.[3495]

The Act also instructs the Attorney General to promulgate specific minimization standards that apply to the collection and dissemination of information obtained through the use of the section 215 authority.[3496] These procedures are intended to limit the retention, and regulate the dissemination, of nonpublicly available information concerning unconsenting U.S. persons, consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information. Federal authorities are required to observe these minimization procedures regarding the use or disclosure of information received under a 215 order; furthermore, they may not use or disclose such information except for lawful purposes. Finally, the Act clarifies that otherwise privileged information does not lose its privileged character simply because it was acquired through a 215 order.

Application Requirements and Orders

Prior to the Act's enactment, an application for a 215 order to be submitted to the FISA court for approval only needed to state that the requested records were sought for an authorized investigation. The Act amends 50 U.S.C. 1861(b)(2) to require that such an application must include a "statement of facts" demonstrating that there are reasonable grounds to believe that the tangible things sought are "relevant" to an authorized or preliminary investigation to protect against international terrorism or espionage, or to obtain foreign intelligence information not concerning a U.S. person.[3497] Section 106(b)(2)(A)

[3495] 50 U.S.C. 1861(a)(2)(B) already prohibits the government from seeking a section 215 order in an investigation of a U.S. person solely upon the basis of activities protected by the First Amendment to the U.S. Constitution. For more information about section 215 under existing law and its potential use against libraries or their patrons, see CRS Report RS21441, Libraries and the USA PATRIOT Act, by Charles Doyle and Brian T. Yeh.

[3496] §106(g), P.L. 109-177, 120 Stat. 198, 199 (2006), adding new 50 U.S.C. 1861(g).

[3497] The "relevancy" standard set forth in the Act was criticized by several Members of Congress during the floor debate on the conference report. See, e.g., 152 CONG. REC. S1382 (daily ed. Feb. 16, 2006) (statement of Sen. Feingold) ("Relevance is a very broad standard that could arguably justify the collection of all kinds of information about law-abiding Americans."). The Senate-passed version of the USA PATRIOT Improvement and Reauthorization Act, S. 1389, required that the statement of facts show that the records or things sought are relevant to an authorized investigation and that the things sought pertain to, or are relevant to the activities of, a foreign

of the Act also provides that certain tangible items are "presumptively relevant" to an investigation if the application's statement of facts shows that the items sought pertain to:

- a foreign power or an agent of a foreign power,
- the activities of a suspected agent of a foreign power who is the subject of such authorized investigation, or
- an individual in contact with, or known to, a suspected agent of a foreign power who is the subject of such authorized investigation.

Finally, the application for a 215 order must include an enumeration of the minimization procedures applicable to the retention and dissemination of the tangible items sought.[3498]

The FISA court judge shall approve an application for a 215 order as requested or as modified, upon a finding that the application complies with statutory requirements. The order must contain a particularized description of the items sought, provide for a reasonable time to assemble them, notify recipients of nondisclosure requirements, and be limited to things subject to a grand jury subpoena or order of a U.S. court for production.[3499] The ex parte order shall also direct that the retention and dissemination of the tangible things obtained under the order must adhere to the minimization procedures.

Judicial Review and Enforcement

Section 106(f) of the Act establishes a detailed judicial review process for recipients of 215 orders to challenge their legality before a judge selected from a pool of FISA court judges. If the judge determines that the petition is not frivolous after an initial review, the judge has discretion to modify or set aside a FISA order upon a finding that it does not comply with the statute or is otherwise unlawful.[3500] However, if the judge does not modify or rescind the 215 order, then the judge must immediately affirm the order and direct the recipient to comply with it.

---

power or agent of foreign power, or pertain to an individual in contact with or known to a suspected agent of a foreign power. The Act does not require such a connection. For more information about the Senate-passed version of the Act, see CRS Report RL33027, USA PATRIOT Act: Background and Comparison of House- and Senate-Approved Reauthorization and Related Legislative Action, by Charles Doyle.

[3498] §106(b), P.L. 109-177, 120 Stat. 196 (2006), adding new 50 U.S.C. 1861(b)(2)(B).

[3499] §106(d), P.L. 109-177, 120 Stat. 197 (2006), amending 50 U.S.C. 1861(c)(2).

[3500] §106(f)(2), P.L. 109-177, 120 Stat. 198 (2006), adding new 50 U.S.C. 1861(f)(1). The review of a petition challenging a 215 order shall be conducted in camera, new 50 U.S.C. 1803(e)(2).

The FISA Court of Review and the U.S. Supreme Court are granted jurisdiction to consider appeals of the FISA court judge's decision to affirm, modify, or set aside a 215 order. The Chief Justice of the United States, in consultation with the Attorney General and the Director of National Intelligence, is directed to establish security measures for maintaining the record of the 215 order judicial review proceedings.

Nondisclosure Requirement for 215 Orders

A section 215 order is accompanied by a nondisclosure requirement that prohibits the recipient from disclosing to any other person that the FBI has sought the tangible things described in the order. Prior to the Act's enactment, the only exception to this "gag order" was for disclosure to those persons necessary for compliance with the production order.[3501] The Act expands the list of exceptions, expressly permitting a recipient of a 215 order to disclose its existence to an attorney to obtain legal advice, as well as to other persons approved by the FBI.[3502]

Under the Act, the recipient is not required to inform the FBI or the authorized government agency of the intent to consult with an attorney to obtain legal assistance; however, upon the request of the FBI Director (or his designee), the recipient must disclose to the FBI the identity of the person to whom the disclosure will be or was made, which could include the name of the attorney.[3503] During the Senate debate over the conference report, some Members of Congress raised concerns that this provision of the Act might have an unintended "chilling effect" on the individual's right to seek legal counsel regarding the Section 215 order.[3504] Thus, section 4 of the USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006, P.L. 109-178, 120 Stat. 280 (2006), amends FISA to exempt explicitly from the identification disclosure requirement the name of the attorney sought to obtain legal advice with respect to the Section 215 production order.[3505]

[3501] 50 U.S.C. 1861(d).

[3502] §106(e), P.L. 109-177, 120 Stat. 197 (2006), adding new 50 U.S.C. 1861(d)(1)(B), (C).

[3503] §106(e), P.L. 109-177, 120 Stat. 197 (2006), adding new 50 U.S.C. 1861(d)(2)(C).

[3504] See, e.g., 152 CONG. REC. S1326 (daily ed. Feb. 15, 2006) (statement of Sen. Sununu) ("[W]e feel the provision in the conference report that required the recipient ... to disclose the name of their attorney to the FBI was punitive and might have the result of discouraging an individual from seeking legal advice.").

[3505] Under the Act, the recipient of a Section 215 order is prohibited from disclosing to any other person that the FBI has sought the tangible things described in the order, except to the following individuals: (A) those persons necessary for compliance with the order, (B) an attorney to obtain legal advice with respect to the order, or (C) other persons as permitted by the FBI Director or his designee. The USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006 amends

While the Act provided a judicial review process for recipients of 215 orders to challenge their legality, the Act does not expressly grant the right to petition the FISA court to modify or quash the nondisclosure requirement imposed in connection with the production order. The Act was criticized for its lack of an express right to challenge the nondisclosure order during the Senate debate over the conference report.[3506]

Section 3 of the USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006, P.L. 109-178, 120 Stat. 278 (2006), addresses this omission by establishing a judicial review procedure for a section 215 nondisclosure orders. For one year after the date of the issuance of a 215 production order, the nondisclosure requirement remains in full effect and may not be challenged.[3507] During the floor debates over S. 2271, this one-year mandatory moratorium and automatic gag order had been criticized and defended by Members of Congress.[3508]

After the one-year waiting period has expired, the recipient of the production order may petition the FISA court to modify or set aside the nondisclosure requirement. Within 72 hours, if the judge assigned to consider the petition determines after an initial review that the petition is frivolous, the judge shall immediately deny the petition and affirm the nondisclosure order. If, after the initial review, the judge determines that the petition is not frivolous, the judge shall promptly consider the petition under procedural measures that the FISA court has established to protect national security, including conducting the review in camera.[3509]

FISA to provide that the FBI Director or his designee may require anyone to disclose the identity of persons falling within categories A and C only. It notably omits B, which effectively removes from the identity disclosure requirement attorneys sought for legal assistance.

[3506] See, e.g., 152 CONG. REC. S1326 (daily ed. Feb. 15, 2006) (statement of Sen. Sununu) ("I think it is important that we stand for the principle that a restriction on free speech such as a gag order can be objected to in a court of law before a judge. You can at least have your case heard. That does not mean you will win, necessarily, but you can at least have your case heard.").

[3507] By contrast, the Act does not impose a one-year moratorium on challenging the nondisclosure order accompanying a NSL, § 115, P.L. 109-177, 120 Stat. 211 (2006), adding new 18 U.S.C. 3511(b)(1).

[3508] Compare 152 CONG. REC. S1496 (daily ed. Feb. 27, 2006) (statement of Sen. Specter) ("My own view is it is preferable there not be a waiting period at all, that the court have the discretion to enter the orders [modifying or quashing a gag order] immediately if it finds cause to do so.") with 152 CONG. REC. S1559 (daily ed. Mar. 1, 2006) (statement of Sen. Kyl) ("The delay is perfectly appropriate and necessary to preserve valuable personnel resources — these orders are approved by judges before issuance, so it makes little sense to allow recipients to challenge the non-disclosure requirement only a week or even a day after the court issues them.").

[3509] § 3, P.L. 109-178, 120 Stat. 178 (2006), amending new 50 U.S.C. 1861(f)(2)(A)(ii).

The FISA court judge has discretion to modify or set aside a nondisclosure order upon a finding that there is no reason to believe that disclosure may endanger the national security of the United States; interfere with a criminal, counterterrorism, or counterintelligence investigation; interfere with diplomatic relations; or endanger the life or physical safety of any person. If, at the time the individual files the petition for judicial review of a nondisclosure order, the Attorney General, Deputy Attorney General, an Assistant Attorney General, or the Director of the FBI certifies that disclosure may endanger the national security of the United States or interfere with diplomatic relations, then the FISA judge must treat such government certification as conclusive unless the judge finds that the certification was made in bad faith.[3510]

If the judge grants a petition to quash the nondisclosure requirement, upon the request of the government, such order is stayed pending review of the decision to the FISA Court of Review. If the judge denies the petition to modify or set aside the nondisclosure requirement, the recipient of the 215 order is precluded from filing another such petition for one year.[3511] The FISA Court of Review has jurisdiction to consider a petition by the government or by the recipient of a 215 order and to review a FISA judge's decision to affirm, modify, or set aside such production order or the nondisclosure order imposed in connection with it. The U.S. Supreme Court has jurisdiction to review a decision of the FISA Court of Review concerning this matter.

National Security Letters

Five federal statutes, in roughly the same terms, authorize federal intelligence investigators (generally the FBI) to request that communications providers, financial institutions and credit bureaus provide certain types of customer business records, including subscriber and transactional information related to Internet and telephone usage, credit reports, and financial records.[3512] Unlike a section 215 production order for tangible items, a national security letter (NSL) need not receive prior approval of a judge. However, NSLs are more limited in scope compared to a section 215 order, in terms of the types of information that can be obtained. For example, NSLs cannot be used to receive "content information" — the content of a telephone communication or e-mail message is unavailable through a NSL, but a NSL could request the phone number dialed or the e-mail addresses used.

[3510] Id., amending new 50 U.S.C. 1861(f)(2)(C)(ii).

[3511] Id., amending new 50 U.S.C. 1861(f)(2)(C)(iii).

[3512] 12 U.S.C. 3414; 15 U.S.C.1681u, 1681v; 18 U.S.C. 2709; 50 U.S.C. 436. For more information concerning national security letters, see CRS Report RL33320, National Security Letters in Foreign Intelligence Investigations: Legal Background and Recent Amendments, by Charles Doyle.

A federal court in the Southern District of New York has held that the FBI's practices and procedure surrounding the exercise of its authority under one of these NSL statutes, 18 U.S.C. 2709, violate the Fourth and First Amendments.[3513] In the opinion of the court, the constitutional problem stems from the effective absence of judicial review before or after the issuance of a NSL under section 2709 and from the facially absolute, permanent confidentiality restrictions ("gag order") that the statute places on NSL recipients.[3514] Another federal court in the District of Connecticut enjoined enforcement of a NSL gag order on First Amendment grounds.[3515]

Section 115 of the Act attempts to address these potential constitutional deficiencies by authorizing judicial review of a NSL.[3516] In addition to providing the right to challenge the validity of the NSL request, section 115 expressly grants NSL recipients the power to petition a federal district court to modify or quash a nondisclosure requirement that may be imposed in connection with the request.

Judicial Review and Enforcement of NSL requests

Under the Act, the recipient of a NSL request may petition a U.S. district court for an order modifying or setting aside the request. The federal court may modify or quash the NSL request if compliance would be unreasonable, oppressive, or otherwise unlawful.

[3513] Doe v. Ashcroft, 334 F.Supp.2d 471 (S.D.N.Y. 2004), vacated by sub nom. Doe I v. Gonzales, 449 F. 3d 415 (2d Cir. 2006)(The U.S. Court of Appeals for the Second Circuit noted that the Reauthorization Act, passed during the pendency of the appeal of this case, "dramatically altered § 2709" and "substantially shifted the legal footing" on which John Doe I stood. Because the Reauthorization Act added 18 U.S.C. 3511(a), permitting NSL recipients to challenge the legality of the NSL in federal court, John Doe I no longer pursued the Fourth Amendment claim. Thus, the appellate court vacated as moot the Fourth Amendment portion of the Southern District of New York opinion. The plaintiffs argued, however, that the revised § 2709(c), as amended by the Reauthorization Act, still violates John Doe I's First Amendment rights. The appellate court remanded the case for the district court to consider whether the revised version of 18 U.S.C. 2709(c) violates the First Amendment either on its face or as applied to John Doe I. Doe I, 449 F. 3d at 418-19.).

[3514] Ashcroft, 334 F.Supp.2d at 526-27.

[3515] Doe v. Gonzalez, 386 F.Supp.2d 66 (D.Conn. 2005), dismissed as moot by Doe II v. Gonzales, 449 F. 3d 415 (2d Cir. 2006) (On appeal, the Government conceded that John Doe II may reveal its identity under new procedures established by the Reauthorization Act, set forth in 18 U.S.C. 3511(b), and the Government informed the appellate court that it would no longer oppose the preliminary injunction issued by the district court. The U.S. Court of Appeals for the Second Circuit thus concluded that "the Government has effectively rendered this appeal moot by its own voluntary actions." Doe II, 449 F. 3d at 420.).

[3516] § 115, P.L. 109-177, 120 Stat. 211 (2006), adding new 18 U.S.C. 3511.

Section 115 also provides the government with the means to enforce the NSL through court action. If a NSL recipient fails to respond to the request for information, the Attorney General may seek a federal district court order to compel compliance with the request.[3517] Disobedience of the U.S. district court's order to respond to a NSL is punishable as contempt of court.

Section 115 directs that any court proceedings concerning NSL matters must be closed, subject to any right to an open hearing in a contempt proceeding, to prevent unauthorized disclosure of the NSL request. In addition, all petitions, filings, records, orders, and subpoenas must be kept under seal to prevent unauthorized disclosure. Finally, the government may request that its evidence be considered ex parte and in camera.

Nondisclosure Orders for NSLs

Section 116 of the Act amends all five NSL statutes to prohibit service providers from disclosing to any person that the FBI has sought or obtained access to the information sought through the NSL, only if the investigative agency has certified that disclosure may endanger any individual or the national security of the United States, interfere with diplomatic relations, or interfere with a criminal or intelligence investigation. Thus, a nondisclosure order does not automatically attach to the NSL, as it does in the case of a Section 215 order under FISA.

Assuming that this certification occurs and the gag order is in place, disclosure by the NSL recipient is permitted to any person whose assistance is needed to comply with the NSL request or to an attorney to obtain legal advice or legal assistance concerning the NSL.[3518] Although the individual is not required to inform the FBI or the authorized government agency of the intent to consult with an attorney to obtain legal assistance, upon the request of the FBI Director (or his designee), or upon the request of the government agency authorized to issue the NSL, the recipient must disclose to the FBI or the government agency the identity of the person to whom the disclosure will be or was made.[3519] According to the sponsor of H.R. 3199, "without this safeguard, a recipient could disclose the

---

[3517] § 115, P.L. 109-177, 120 Stat. 212 (2006), adding new 18 U.S.C. 3511(c). Critics of this new provision claim that it effectively transforms NSLs into national security subpoenas. See ACLU, ACLU Letter to Congress Urging A "No" Vote On the USA PATRIOT Improvement and Reauthorization Act Conference Report (Dec. 12, 2005), available on Jan. 13, 2006 at [http://www.aclu.org/safefree/general/22394leg20051207.html].

[3518] § 116, P.L. 109-177, 120 Stat. 213-217 (2006), amending 18 U.S.C. 2709(c)(1); 15 U.S.C. 1681u(d)(1); 15 U.S.C. 1681v(c)(1); 12 U.S.C. 3414(a)(3)(A); 12 U.S.C. 3414(a)(5)(D)(I); and 50 U.S.C. 436(b)(1).

[3519] § 116, P.L. 109-177, 120 Stat. 213-217 (2006), amending 18 U.S.C. 2709(c)(4); 15 U.S.C. 1681u(d)(4); 15 U.S.C. 1681v(c)(4); 12 U.S.C. 3414(a)(3)(D); 12 U.S.C. 3414(a)(5)(D)(iv); and 50 U.S.C. 436(b)(4).

government's investigative efforts to a person with ties to hostile foreign governments or entities."[3520]

However, the potential that this identity disclosure requirement may chill the right to seek legal counsel was reduced by Section 4 of the USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006, P.L. 109-178, 120 Stat. 280 (2006). (Section 4 also had removed a similar disclosure requirement concerning a Section 215 production order under FISA.) Section 4 amends the five NSL statutes by adding language expressly exempting the identity of attorneys from the disclosure requirement established by the Act:

> *At the request of the Director of the Federal Bureau of Investigation or the designee of the Director, any person making or intending to make a disclosure under this section shall identify to the Director or such designee the person to whom such disclosure will be made or to whom such disclosure was made prior to the request, except that nothing in this section shall require a person to inform the Director or such designee of the identity of an attorney to whom disclosure was made or will be made to obtain legal advice or legal assistance with respect to the [NSL] request...*[3521]

Section 117 of the Act punishes a person who was notified of a NSL nondisclosure requirement but nevertheless knowingly and willfully violates that directive, with imprisonment of not more than one year, or not more than five years if committed with the intent to obstruct an investigation or judicial proceeding.[3522] The law prior to the Act's enactment did not provide a felony charge for such disclosure to an unauthorized person.

Section 115 of the Act grants a NSL recipient with an explicit statutory right to challenge in court the gag order that may attach to the NSL request — a right that a recipient of a section 215 FISA production order lacks under the Act but which was subsequently provided by the USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006. Section 115 creates a bifurcated procedure for handling petitions for judicial review of the nondisclosure requirement accompanying a NSL:

[3520] 152 Cong. Rec. H583 (daily ed. Mar. 7, 2006) (statement of Rep. Sensenbrenner).

[3521] § 4, P.L. 109-178, 120 Stat. 280 (2006), amending 18 U.S.C. 2709(c)(4) (emphasis added). The language used to describe this exception in 18 U.S.C. 2709(c)(4) is substantially similar to that used in the amendments to the other NSL statutes.

[3522] § 117, P.L. 109-177, 120 Stat. 217 (2006), adding new 18 U.S.C. 1510(e).

(1) If the petition is filed within one year of the NSL request, the U.S. district court may modify or set aside the gag order if it finds no reason to believe that disclosure may:

- endanger the national security of the United States,
- interfere with a criminal, counterterrorism, or counterintelligence investigation,
- interfere with diplomatic relations, or
- endanger the life or physical safety of any person.

If, at the time of the petition, a high-ranking government official[3523] certifies that disclosure may:

- endanger the national security of the United States, or
- interfere with diplomatic relations,

then the court must treat the government certification as conclusive unless the court finds that the certification was made in bad faith.

(2) If the petition challenging the gag order is filed one year or more after the NSL issuance, a high-ranking government official must, within 90 days of the petition, either terminate the gag order or re-certify that disclosure may:

- endanger the national security of the United States,
- interfere with a criminal, counterterrorism, or counterintelligence investigation,
- interfere with diplomatic relations, or
- endanger the life or physical safety of any person.

If such recertification occurs, then a court may modify or quash the gag order if it finds no reason to believe that disclosure may:

- endanger the national security of the United States,
- interfere with a criminal, counterterrorism, or counterintelligence investigation,
- interfere with diplomatic relations, or
- endanger the life or physical safety of any person.

[3523] If the NSL is issued by the Department of Justice, this person must be the Attorney General, Deputy AG, or the Director of the FBI; if the NSL information is requested by any agency, department, or instrumentality other than the Justice Department, then the individual must be its head or deputy. New 18 U.S.C. 3511(b)(2).

However, if the recertification was made by the Attorney General, Deputy Attorney General, an Assistant Attorney General, or the Director of the FBI, and if such recertification stated that disclosure may:

- endanger the national security of the United States, or
- interfere with diplomatic relations

then such certification is to be treated by the court as conclusive unless it was made in bad faith.

If court denies the petition for an order to modify the nondisclosure requirement, the NSL recipient is precluded from filing another such petition for one year.

Although the Act provides a process to challenge the nondisclosure requirement, critics believe that this judicial review is not meaningful, in light of the "conclusive presumption" provision: "A recipient would technically be given a right to challenge the gag order but if the government asserted national security, diplomatic relations or an ongoing criminal investigation the court would be required to treat that assertion as conclusive, making the 'right' an illusion."[3524] In addition, some Members of Congress have raised First Amendment and due process concerns over the indefinite gag order and the conclusive presumption.[3525] However, others have defended the conclusive presumption as necessary to ensure that sensitive information is not publicly disclosed:

> *Only the FBI, the people who are investigating the matter, not individual district judges, are in a position to determine when the disclosure of classified information would harm national security. Obviously, that is not something that a Federal district judge has any expertise on. ... It is also important that the FBI make the final determination whether the disclosure would harm national security. And only the agents in charge of these counterterrorism investigations will be able to evaluate how the disclosure of a particular piece of information could potentially, for example, reveal sources and methods of intelligence and who, therefore, might be tipped off as a result of the disclosure.*[3526]

[3524] ACLU, ACLU Letter to Congress Urging A "No" Vote On the USA PATRIOT Improvement and Reauthorization Act Conference Report (Dec. 12, 2005), available Jan. 13, 2006 at [http://www.aclu.org/safefree/general/22394leg20051207.html].

[3525] See, e.g., 152 CONG. REC. S1567 (daily ed. Mar. 1, 2006) (statement of Sen. Leahy); 152 CONG. REC. H588 (daily ed. Mar. 7, 2006) (statement of Rep. Nadler); 152 CONG. REC. S1382, 1383 (daily ed. Feb. 16, 2006) (statement of Sen. Feingold).

[3526] 152 CONG. REC. S1394, 1395 (daily ed. Feb. 16, 2006) (statement of Sen. Kyl).

NSLs Not Applicable to Libraries

Section 5 of the USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006, P.L. 109-178, 120 Stat. 281 (2006), entitled "Privacy Protections for Library Patrons," addresses the concern that a library could potentially be subject to an NSL issued under 18 U.S.C. 2709 to obtain certain transactional and subscriber records pertaining to its patrons.[3527] Because libraries often offer patrons the ability to access the Internet, the law prior to the Act was unclear as to whether libraries might be considered "electronic communication service providers" for purposes of 18 U.S.C. 2709. Section 5 amends 18 U.S.C. 2709 by adding the following section:

> *"A library ..., the services of which include access to the Internet ..., is not a wire or electronic communication service provider for purposes of this section, unless the library is providing the services defined in section 2510(15) of this title..."*[3528]

This provision "makes very clear that libraries operating in their traditional role, including the lending of books, including making books available in digital form, including providing basic Internet access, are not subject to National Security Letters."[3529] However, if the library "provides" the services described in 18 U.S.C. 2510(15), which are "electronic communication services," then such library would still be subject to NSLs. 18 U.S.C. 2510(15) defines "electronic communication service" to mean any service that provides to users the ability to send or receive wire or electronic communications. A reasonable interpretation of this definition suggests that to be considered an electronic communication service provider under 18 U.S.C. 2510(15), a library must independently operate the means by which transmission, routing, and connection of digital communication occurs.[3530] In contrast, a local county library likely has a service contract with an Internet Service Provider (ISP) to furnish the library with the electronic communication service, as many businesses and individuals do; the fact that the library has set up a computer with Internet access for the use of its patrons probably does not, by itself, turn the library into a communications service "provider." Under this

---

[3527] However, a library could still be subject to a Section 215 order under FISA for the production of tangible items such as loan records. S. 2271 does not carve out any exception for libraries under Section 215. For more information on this issue, see CRS Report RS21441, Libraries and the USA PATRIOT Act, by Charles Doyle and Brian T. Yeh.

[3528] 18 U.S.C. 2709(f) as amended by P.L. 109-178, 120 Stat. 281 (emphasis added).

[3529] 152 CONG. REC. S1326 (daily ed. Feb. 15, 2006) (statement of Sen. Sununu).

[3530] See 152 CONG. REC. S1558 (daily ed. Mar. 1, 2006) (statement of Sen. Leahy) ("[A] library may be served with an NSL only if it functions as a true internet service provider, as by providing services to persons located outside the premises of the library. I expect that this will occur rarely or never and that in most if not all cases, the Government will need a court order to seize library records for foreign intelligence purposes.").

characterization, the actual "provider" of Internet access is the ISP, not the library.[3531] Therefore, a public library offering "basic" Internet access would likely not be considered an electronic communication service provider, at least for purposes of being an entity subject to the NSL provisions in 18 U.S.C. 2709.[3532]

Congressional Oversight of NSLs

Section 118 of the Act requires that any reports to a Congressional committee regarding NSLs shall also be provided to the House and Senate Judiciary Committees. In addition, the Attorney General must submit a report semiannually on all NSL requests made under the Fair Credit Reporting Act, to the House and Senate Judiciary Committees, the House and Senate Intelligence Committees, and the House Committee on Financial Services and the Senate Committee on Banking, Housing, and Urban Affairs.[3533]

The Attorney General is also instructed to submit to Congress an annual report describing the total number of requests made by the Department of Justice under the NSL statutes. This report is to be unclassified, in order to permit public scrutiny.

Section 119 of the Act directs the Inspector General of the Department of Justice to perform a comprehensive audit of the effectiveness and use of NSLs, including any improper or illegal use, for submission to the House and Senate Judiciary and Intelligence Committees for calendar years 2003-2006. This report is to be unclassified. Section 119 also requires the Attorney General and Director of National Intelligence to analyze the feasibility of applying minimization procedures to NSL to ensure the protection of the constitutional rights of U.S. persons. This feasibility study is to be submitted to the House and Senate Judiciary and Intelligence Committees by February 1, 2007, or upon completion of the audit of the use of NSLs for calendar years 2003 and 2004, whichever is earlier.

[3531] See 152 CONG. REC. S1390 (daily ed. Feb. 16, 2006) (statement of Sen. Sununu) ("Some have noted or may note that basic Internet access gives library patrons the ability to send and receive e-mail by, for example, accessing an Internet-based e-mail service. But in that case, it is the website operator who is providing the communication service — the Internet communication service provider itself — and not the library, which is simply making available a computer with access to the Internet."). Thus, the NSL request could be served on the ISP rather than the library.

[3532] See 152 CONG. REC. S1390 (daily ed. Feb. 16, 2006) (statement of Sen. Durbin) ("By way of comparison, a gas station that has a pay phone isn't a telephone company. So a library that has Internet access, where a person can find an Internet e-mail service, is not a communications service provider; therefore, it would not fall under the purview of the NSL provision in 18 U.S.C. 2709. It is a critically important distinction.").

[3533] § 118(b), P.L. 109-177, 120 Stat. 217, 218 (2006), adding new 15 U.S.C. 1681v(f).

Section 206 FISA "Roving" Wiretaps

Unlike a criminal wiretap order issued under Title III of the Omnibus Crime Control and Safe Streets Act of 1968,[3534] which may be approved if a judge finds probable cause for believing that an individual is committing, has committed, or is about to commit a particular enumerated offense,[3535] a FISA wiretap may be issued upon a finding of probable cause to believe that the target of the electronic surveillance is a foreign power or agent of a foreign power.[3536] Section 206 of the USA PATRIOT Act amended FISA to authorize the installation and use of multipoint, or "roving," wiretaps, for foreign intelligence investigations.[3537] A roving wiretap order applies to the suspect rather than a particular phone or computer that the target might use, and thus allows law enforcement officials to use a single wiretap order to cover any communications device that the target uses or may use.[3538] Without this authority, investigators must seek a new FISA court order each time they need to change the name of the location to be monitored, as well as the specified person or entity that is needed to assist in facilitating the wiretap.[3539]

Section 206 of the USA PATRIOT Act permits a general command for the assistance of third parties (for example, common carriers and Internet service providers) for the installation and use of these multipoint wiretaps, where the target of the surveillance has taken steps to thwart the identification of a communications company or other person whose assistance may be needed to carry out the surveillance. Thus, if the FISA court finds that the target's actions may have the effect of thwarting specific identification, section 206 temporarily authorizes FISA orders that need not specifically identify the communications carriers, landlords or others whose assistance the order commands.[3540]

[3534] 18 U.S.C. 2510 et seq.

[3535] See list of predicate offenses at 18 U.S.C. 2516(1)(a)-(r).

[3536] 50 U.S.C. 1805(a).

[3537] 50 U.S.C. 1805(c)(2)(B).

[3538] According to the Department of Justice, "This new authority has put investigators in a better position to avoid unnecessary cat-and- mouse games with terrorists, who are trained to thwart surveillance." U.S. Dep't of Justice, Report from the Field, The USA PATRIOT Act at Work , 22 (July 2004), available on Jan. 13, 2006 at [http://www.lifeandliberty.gov/docs/071304_report_from_the_field.pdf].

[3539] Oversight Hearing on "Reauthorization of the USA PATRIOT Act": Hearings Before the House Comm. on the Judiciary, 109th Cong., 1st Sess. (2005) (statement of James B. Comey, Deputy Attorney General, U.S. Dep't of Justice), at 9-10, available on Jan. 13, 2006 at [http://judiciary.house.gov/media/pdfs/comey060805.pdf].

[3540] 50 U.S.C. 1805(c)(2)(B).

Prior to the enactment of the Act, a FISA roving surveillance order had to specify the identity of the target only if it was known; otherwise, it was sufficient for the order to describe the target.[3541] Section 108 of the Act amends the FISA roving surveillance authority to require that an application for an order, as well as the wiretap order itself, describe the specific target of the electronic surveillance if the target's identity is not known.[3542] It also clarifies that the FISA court must find that the prospect of a target thwarting surveillance is based on specific facts in the application. Furthermore, if the government begins to direct surveillance at a new facility or place, the nature and location of which were unknown at the time the original surveillance order was issued, the government must notify the FISA court within 10 days[3543] after such change, of the following information:[3544]

- the nature and location of each new facility or place at which the surveillance is directed,
- the facts and circumstances relied upon by the applicant to justify the applicant's belief that each new facility or place is or was being used, or is about to be used, by the target of the surveillance,
- an explanation of any proposed minimization procedures that differ from those contained in the original application or order, if such change is necessitated by the new facility or place, and
- the total number of electronic surveillances that have been or are being conducted under the roving surveillance order.

The Act also enhances congressional oversight over the use of all foreign intelligence electronic surveillance authority, by adding the Senate Judiciary Committee as a recipient of the semi-annual FISA reports that the Attorney General currently must submit to the House and Senate Intelligence committees,[3545] and by modifying the FISA report requirements to include a description of the total number of applications made for orders approving roving electronic surveillance.[3546]

[3541] 50 U.S.C. 1805(c)(1)(A). Furthermore, a roving wiretap order need not identify the nature and location of the places or facilities targeted for surveillance if they are unknown. 50 U.S.C. 1805(c)(1)(B). This provision remains unchanged after enactment of the Act.

[3542] § 108(a), P.L. 109-177, 120 Stat. 203 (2006), amending 50 U.S.C. 1804(a)(3) and 50 U.S.C. 1805(c)(1)(A).

[3543] The 10 day period may be extended up to 60 days if the court finds good cause to justify the longer period.

[3544] § 108(b)(4), P.L. 109-177, 120 Stat. 203 (2006), adding new 50 U.S.C. 1805(c)(3).

[3545] § 108(c)(1), P.L. 109-177, 120 Stat. 204 (2006), amending 50 U.S.C. 1808(a)(1).

[3546] § 108(c)(2), P.L. 109-177, 120 Stat. 204 (2006), amending 50 U.S.C. 1808(a)(2).

Delayed Notice Search Warrants

A delayed notice search warrant, or "sneak and peek" warrant, is one that authorizes law enforcement officers to secretly enter a home or business, either physically or virtually, conduct a search, and depart without taking any tangible evidence or leaving notice of their presence. The Department of Justice has defended the necessity and legality of delayed notification search warrants:

> *This tool can be used only with a court order, in extremely narrow circumstances when immediate notification may result in death or physical harm to an individual, flight from prosecution, evidence tampering, witness intimidation, or serious jeopardy to an investigation. The reasonable delay gives law enforcement time to identify the criminal's associates, eliminate immediate threats to our communities, and coordinate the arrests of multiple individuals without tipping them off beforehand. In all cases, law enforcement must give notice that property has been searched or seized.*[3547]

Until the USA PATRIOT Act was enacted, the Federal Rules of Criminal Procedure required contemporaneous notice in most instances.[3548] At the time, the courts were divided over whether the failure to provide contemporaneous notice, in the absence of exigent circumstances, constituted a constitutional violation or a violation of the Rule, and over the extent of permissible delay in cases presenting exigent circumstances.[3549] Section 213 of the USA PATRIOT Act created an express statutory authority for delayed notice search warrants in any criminal investigation, not just those involving suspected terrorist activity.[3550]

[3547] U.S. Dep't of Justice, Dispelling Some of the Major Myths about the USA PATRIOT Act, available on Jan. 13,2006 at [http://www.lifeandliberty.gov/subs/u_myths.htm].

[3548] FED. R. CRIM. P. 41(d), 18 U.S.C. App. (2000 ed.).

[3549] See United States v. Pangburn, 983 F.2d 449 (2d Cir. 1993); United States v. Freitas, 800 F.2d 1451 (9th Cir. 1986); United States v. Simmons, 206 F.3d 392 (4th Cir. 2000).

[3550] 18 U.S.C. 3103a. Critics have expressed concerns about the constitutionality of delayed notice search warrants as well as potential abuse of the power. See, e.g., EPIC Report ("The expansion of this extraordinary authority to all searches constitutes a radical departure from Fourth Amendment standards and could result in routine surreptitious entries by law enforcement agents."); American Civil Liberties Union (ACLU), Surveillance Under the USA PATRIOT Act (April 3, 2003), available on Jan. 13, 2006 at [http://www.aclu.org/safefree/general/17326res20030403.html] ("Notice is a crucial check on the government's power because it forces the authorities to operate in the open, and allows the subjects of searches to protect their Fourth Amendment rights. For example, it allows them to point out irregularities in a warrant. ... Search warrants often contain limits on what may be

Delayed notification of the execution of a sneak and peek search warrant is permissible for a reasonable period of time (with the possibility of court-approved extensions for good cause shown), if:

- the court that issued the warrant finds reasonable cause to believe that contemporaneous notice of the search may result in adverse consequences (flight, destruction of evidence, intimidation of a witness, danger to an individual, serious jeopardy to an investigation, or undue trial delay), and
- the warrant prohibits the seizure of any tangible property, any wire or electronic communication, and any stored wire or electronic information, except where the court finds reasonable necessity for the seizure.

Responding to concerns that the "reasonable period" for delaying notification of a search warrant is an undefined and indefinite standard under current law, section 114 of the Act establishes a specific limitation on the length of the delay, requiring notice to be given no more than 30 days after the date of the warrant's execution, with the possibility for 90 day extensions if the facts of a case justify.[3551] Several Members of Congress have criticized this 30-day delayed notice provision, arguing instead for notice to be given to the target of the search warrant within 7 days.[3552] However, it should be noted that the Act's 30-day delay period was itself a compromise between the House and Senate-passed versions of the Reauthorization Act; the House bill allowed 180 days, while the Senate limited the delay to 7 days.

In addition, section 114 removes "unduly delaying a trial" as one of the "adverse consequences" that justifies delayed notification. Some commentators have noted that "seriously jeopardizing an investigation," which is retained by the Act as a ground for permitting delayed notice, is an overly broad "catch-all" provision that law enforcement officials could abuse.[3553] There may also be some question of whether it qualifies as a constitutionally acceptable exigent circumstance.

---

searched, but when the searching officers have complete and unsupervised discretion over a search, a property owner cannot defend his or her rights.").

[3551] § 114, 109-177, 120 Stat. 210 (2006), amending 18 U.S.C. 3103a(b)(3).

[3552] See, e.g., 152 CONG. REC. S1384 (daily ed. Feb. 16, 2006) (statement of Sen. Feingold) (asserting that seven days is what courts have previously approved), and 152 CONG. REC. S1495 (daily ed. Feb. 27, 2006) (statement of Sen. Specter) (stating that, in his view, seven days is "the best requirement"). However, other Members of Congress have challenged the argument that seven days is the constitutionally-permissible limit. See 152 CONG. REC. S1397 (daily ed. Feb. 16, 2006) (statement of Sen. Sessions) (claiming that the Court of Appeals for the Fourth Circuit has previously allowed a 45-day period for delayed notice of a search warrant, although the court did not suggest that this was necessarily a constitutional upper limit).

[3553] See ACLU, ACLU Letter to Congress Urging A "No" Vote On the USA PATRIOT Improvement and Reauthorization Act Conference Report (Dec. 12, 2005), available on Jan. 13, 2006 at [http://www.aclu.org/safefree/general/22394leg20051207.html].

However, Justice Department officials defend this provision, observing that before the delayed notice can be approved, a federal judge must agree with the government's evaluation of the circumstances that indicate that contemporaneous notice of a search might seriously jeopardize an ongoing investigation.[3554]

Finally, section 114 enhances oversight of delayed notice search warrants, by requiring that no later than 30 days after the expiration or denial of such a warrant, the issuing or denying judge must notify the Administrative Office of the U.S. Courts of:

- the fact that the delayed notice search warrant was applied for,
- the fact that the warrant was either granted, modified, or denied,
- the length of time of the delay in giving notice, and
- the offense specified in the warrant or the application.[3555]

Beginning with the fiscal year ending September 30, 2007, the Director of the Administrative Office is required to transmit a detailed, annual report to Congress that summarizes the use and number of warrants authorizing delayed notice.

Emergency Disclosures by Service Providers

Section 212 of the USA PATRIOT Act permits electronic communications service providers to disclose voluntarily the contents of stored electronic communications to a Federal, State, or local governmental entity in emergency situations involving a risk or danger of death or serious physical injury to any person.[3556] Service providers are also permitted to disclose customer records to governmental entities in emergencies involving an immediate risk of serious physical injury or danger of death to any person.[3557]

[3554] Oversight Hearing on the "Implementation of the USA PATRIOT Act: Sections 201, 202, 223 of the Act that Address Criminal Wiretaps, and Section 213 of the Act that Addresses Delayed Notice": Hearings Before the Subcomm. on Crime, Terrorism, and Homeland Security of the House Comm. on the Judiciary, 109th Cong., 1st Sess. (2005) (statement of Chuck Rosenberg , Chief of Staff to Deputy Attorney General, U.S. Dep't of Justice), at 3-4, available Jan. 13, 2006 at [http://judiciary.house.gov/media/pdfs/rosenberg050305.pdf] (stating that "[t]here are a variety of ways in which investigators and prosecutors should not be precluded from obtaining a delayed notice search warrant simply because their request does not fall into one of the other four circumstances listed in the statute").

[3555] § 114, 109-177, 120 Stat. 210, 211 (2006), amending 18 U.S.C. 3103a(d)(1).

[3556] 18 U.S.C. 2702(b)(8).

[3557] 18 U.S.C. 2702(c)(4).

To provide congressional oversight over the use of this authority, section 107(a) of the Act requires the Attorney General annually to report to the Judiciary Committees of the House and Senate concerning the number of service providers' voluntary emergency disclosures of the contents of electronic communications to the Department of Justice. The report must also summarize the basis for the voluntary disclosure in circumstances where the investigation pertaining to the disclosure was closed without the filing of criminal charges. In addition, section 107(b) of the Act removes the immediacy requirement from the customer records provision and defines "governmental entity" to mean a department or agency of the United States or any State or political subdivision thereof.

Duration of FISA Surveillance and Physical Search Orders and Congressional Oversight Of Their Usage

The Act extends the maximum duration of FISA electronic surveillance and physical search orders against any agent of a foreign power who is not a U.S. person (e.g., a lone wolf terrorist), by amending section 105(e) of FISA.[3558] Initial orders authorizing such searches may be for a period of up to 120 days, with renewal orders permitted to extend the period for up to one year.

In addition, the Act extends the life time for both initial and extension orders authorizing installation and use of FISA pen registers, and trap and trace surveillance devices[3559] from a period of 90 days to one year, in cases where the government has certified that the information likely to be obtained is foreign intelligence information not concerning a U.S. person.[3560]

Section 109(a) of the Act enhances congressional oversight over the use of physical searches under FISA, by requiring, on a semi-annual basis, the Attorney General:

- to make full reports concerning all physical searches to the Senate Judiciary Committee in addition to the House and Senate Intelligence committees, and

---

[3558] § 105, P.L. 109-177, 120 Stat. 195 (2006), amending 50 U.S.C. 1805(e) and 50 U.S.C. 1824(d).

[3559] These surveillance devices are used to intercept non-content transactional information which reveals the source and destination of wire and electronic communications, such as telephone dialing information, Internet IP addresses, and e-mail routing and addressing. See definitions of these terms, 18 U.S.C. 3127(3), 18 U.S.C. 3127(4).

[3560] § 105(c), P.L. 109-177, 120 Stat. 195, 196 (2006), adding new 50 U.S.C. 1842(e)(2).

- to submit to the House Judiciary Committee a report with statistical information concerning the number of emergency physical search orders authorized or denied by the Attorney General.[3561]

Section 109(b) requires that the report the Attorney General submits to the House and Senate Judiciary Committees semi-annually concerning the number of applications and orders for the FISA use of pen registers or trap and trace devices, must include statistical information regarding the emergency use of such devices.[3562]

Information Related to FISA Pen Register and Trap & Trace Devices

Law enforcement officials may secure an order authorizing the installation and use of a pen register or trap and trace device to obtain information relevant to a criminal investigation, 18 U.S.C. 3122, 3123. They are also entitled to a court order directing a communications provider to supply certain customer information when relevant to a criminal investigation, 18 U.S.C. 2703.[3563] Foreign intelligence officials are entitled to secure a FISA order for installation and use of a pen register or trap and trace device in connection with certain foreign intelligence investigations, 50 U.S.C. 1841-1846. Under its national security letter authority the FBI may request communications providers to supply customer name, address, length of service and local and long distance toll billing records, 18 U.S.C. 2709. Under section 215 of the USA PATRIOT Act, the FBI may obtain a FISA tangible item order for customer records held by a communications provider, 50 U.S.C. 1861.

Section 128(a) of the Act provides that the FISA court may, in its pen register/trap and trace order, direct a service provider to supply customer information relating to use of the device.[3564] The information to be made available is more extensive than what is available under 18 U.S.C. 2709, or to law enforcement officials, but it is not as extensive as the scope of information under a FISA section 215 "tangible item" order; that is —

[3561] § 109(a), P.L. 109-177, 120 Stat. 204 (2006), amending 50 U.S.C. 1826.

[3562] § 109(b), P.L. 109-177, 120 Stat. 204, 205 (2006), amending 50 U.S.C. 1846.

[3563] The information available under section 2703 includes "the — (A) name; (B) address; (C) local and long distance telephone connection records, or records of session times and durations; (D) length of service (including start date) and types of service utilized; (E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and (F) means and source of payment for such service (including any credit card or bank account number), of a subscriber to or customer of such service)," 18 U.S.C. 2703(c)(2).

[3564] § 128(a), P.L. 109-177, 120 Stat. 228 (2006), adding new 50 U.S.C. 1842(d)(2)(C).

(I) in the case of the customer or subscriber using the service covered by the order (for the period specified by the order) —
(I) the name of the customer or subscriber;
(II) the address of the customer or subscriber;
(III) the telephone or instrument number, or other subscriber number or identifier, of the customer or subscriber, including any temporarily assigned network address or associated routing or transmission information;
(IV) the length of the provision of service by such provider to the customer or subscriber and the types of services utilized by the customer or subscriber;
(V) in the case of a provider of local or long distance telephone service, any local or long distance telephone records of the customer or subscriber;
(VI) if applicable, any records reflecting period of usage (or sessions) by the customer or subscriber; and
(VII) any mechanisms and sources of payment for such service, including the number of any credit card or bank account utilized for payment for such service; and
(I) if available, with respect to any customer or subscriber of incoming or outgoing communications to or from the service covered by the order —
(I) the name of such customer or subscriber;
(II) the address of such customer or subscriber;
(III) the telephone or instrument number, or other subscriber number or identifier, of the customer or subscriber, including any temporarily assigned network address or associated routing or transmission information;
(IV) the length of the provision of service by such provider to the customer or subscriber and the types of services utilized by the customer or subscriber.

The Senate Select Committee on Intelligence observed with respect to an identically worded section in S. 1266, "the FISA audit staff was informed that when a federal court issues an order for criminal pen register or trap and trace device, the court has the authority under 18 U.S.C. 2703(d) to routinely require the service provider to supply subscriber information in its possession for the numbers or e-mail addresses captured by the devices. The FISA pen register/trap and trace provision has no comparable authority. Section 215 of this bill addresses this discrepancy."[3565]

The amendment would likely simplify the process, but critics might ask why it is necessary since information already seems to be available through use of the

[3565] S.Rept. 109-85, at 8 (2005).

national security letter authority under 18 U.S.C. 2709 or the FISA business records "tangible item" authority when used in conjunction with the FISA pen register/trap and trace authority.

Section 128(b) of the Act amends the FISA oversight reporting requirements so that Judiciary Committees receive full reports on the use of the FISA's pen register and trap and trace authority every six months.[3566]

Additions to the Definition of Federal Crime of Terrorism

Crimes designated as federal crimes of terrorism under 18 U.S.C. 2332b(g)(5) trigger the application of other federal laws, for example, 18 U.S.C. 1961(1)(g) (RICO predicates), 18 U.S.C. 3142 (bail), 18 U.S.C. 3286 (statute of limitations), and 18 U.S.C. 3583 (supervised release). Section 112 of the Act adds two additional offenses to the definition of federal crimes of terrorism: receiving military-type training from a foreign terrorist organization,[3567] and drug trafficking in support of terrorism (the "narco-terrorism" provisions of Section 1010A of the Controlled Substances Import and Export Act).[3568]

Expanded List of Predicate Offenses For Wiretaps

Generally, federal law requires the government to obtain a court order authorizing the interception of wire, oral or electronic communications in the investigation of certain crimes ("predicate offenses") specifically enumerated in 18 U.S.C. 2516(1). Section 113 of the Act expands the list of predicate offenses in which law enforcement may seek wiretap orders to include crimes relating to biological weapons, violence at international airports, nuclear and weapons of mass destruction threats, explosive materials, receiving terrorist military training, terrorist attacks against mass transit, arson within U.S. special maritime and territorial jurisdiction, torture, firearm attacks in federal facilities, killing federal employees, killing certain foreign officials, conspiracy to commit violence overseas, harboring terrorists, assault on a flight crew member with a dangerous weapon, certain weapons offenses aboard an aircraft, aggravated identity theft, "smurfing" (a money laundering technique whereby a large monetary transaction is separated into smaller transactions to evade federal reporting requirements on large transactions), and criminal violations of certain provisions of the Sherman Antitrust Act.

[3566] § 128(b), P.L. 109-177, 120 Stat. 229 (2006), amending 50 U.S.C. 1846(a).

[3567] 18 U.S.C. 2339D.

[3568] § 122, P.L. 109-177, 120 Stat. 225 (2006) adds new 21 U.S.C. 960A concerning "narco-terrorism."

Attacks Against Railroad Carriers and Mass Transportation Systems

Section 110 of the Act merges 18 U.S.C. 1992 (outlawing train wrecking) and 18 U.S.C. 1993 (outlawing attacks on mass transportation system) into a new 18 U.S.C. 1992 intended to provide uniform offense elements and penalties for attacks on all transportation systems on land, on water, or through the air. In addition, the Act explicitly provides criminal punishment for the planning of terrorist attacks and other acts of violence against railroads and mass transportation systems;[3569] previous law had only criminalized committing such attacks or attempting, threatening, or conspiring to do so.

Punishment under this new criminal statute is imprisonment for not more than 20 years, but if the offense results in the death of any person, then imprisonment of any years or for life or the death penalty, although the death penalty is not available for inchoate forms of the offense (planning, conveying false information, attempting, threatening, or conspiring). Furthermore, the new 18 U.S.C. 1992 enhances the penalties for committing these criminal acts in circumstances that constitute an aggravated offense, by authorizing imprisonment for any term of years or life, or where death results, the death penalty. Finally, the new 18 U.S.C. 1992 defines covered conveyances and their systems to include passenger vessels.[3570]

Asset Forfeiture

Federal law permits U.S. confiscation of property derived from certain drug offenses committed in violation of foreign law,[3571] and also permits U.S. confiscation of all assets, foreign or domestic, associated with certain terrorist offenses.[3572] Section 111 of the Act amends the general civil forfeiture statute to authorize seizure of property within U.S. jurisdiction constituting, derived from, or traceable to, any proceeds obtained in (or any property used to facilitate) an offense that involves trafficking in nuclear, chemical, biological, or radiological weapons technology or material, if such offense is punishable under foreign law by death or imprisonment for a term exceeding one year or would be so punishable if committed within U.S. jurisdiction.[3573]

[3569] § 110(a), P.L. 109-177, 120 Stat. 206 (2006), adding new 18 U.S.C. 1992(a)(8) (making it a crime to surveil, photograph, videotape, diagram, or otherwise collect information with the intent to plan or assist in planning, an attack against mass transportation systems).

[3570] § 110(a), P.L. 109-177, 120 Stat. 207, 208 (2006), adding new 18 U.S.C. 1992(d)(7).

[3571] 18 U.S.C. 981(a)(1)(B).

[3572] 18 U.S.C. 981(a)(1)(G).

[3573] §111, P.L. 109-177, 120 Stat. 209 (2006), amending 18 U.S.C. 981(a)(1)(B)(I).

In addition, the Act changes the reference for the definition of terrorism as used in the asset forfeiture provision under section 806 of the USA PATRIOT Act. Prior to the Act, 18 U.S.C. 981(a)(1)(G) called for the confiscation of property of those planning or engaged in acts of domestic or international terrorism (as defined in 18 U.S.C. 2331) against the United States or its citizens. Domestic terrorism is defined in 18 U.S.C. 2331 (section 802 of the USA PATRIOT Act), and includes acts dangerous to human life in violation of state or federal law committed to influence the policy of a government or civilian population by intimidation or coercion, 18 U.S.C. 2331(5). Critics might suggest that the juxtaposition of the definition and the confiscation provisions of section 981(a)(1)(G) could result in the confiscation of the property of political action organizations whose members became involved in a picket sign swinging melee with counter-demonstrators.[3574] In contrast, 18 U.S.C. 2332b(g)(5)(B) seems less susceptible to such challenges since it defines terrorism by reference to violations of specific federal terrorist offenses rather than the generic, violation of state or federal law found in section 2331.

Thus, section 120 of the Act replaces terrorism defined in 18 U.S.C. 2331 with terrorism defined in 18 U.S.C. 2332b(g)(5)(B) as the ground for confiscation under section 981(a)(1)(G). It does so by amending 18 U.S.C. 981(a)(1)(G) so that it calls for the confiscation of property of those planning or engaged acts of domestic or international terrorism (as defined in 18 U.S.C. 2332b(g)(5)(B)) against the United States or its citizens.

Victims Access Forfeiture Fund

Section 981 of title 18 of the United States Code describes various forms of property that are subject to confiscation by the United States because of their proximity to various federal crimes. The proceeds from the confiscation of crime-related property are generally available for law enforcement purposes to the law enforcement agencies that participate in the investigation and prosecution that results in the forfeiture, e.g., 18 U.S.C. 981(e). The funds realized from the collection of criminal fines are generally available for victim compensation and victim assistance purposes, 42 U.S.C. 10601. Victims of violent federal crimes are

---

[3574] 151 CONG. REC. H6262 (daily ed. July 21, 2005)(statement of Rep. Delahunt) ("This is about domestic terrorism and the definition of domestic terrorism. And while it does not create a new crime under the PATRIOT Act, the definition triggers an array of expanded governmental authorities, including enhanced civil asset seizure powers. It is so broadly defined that it could include acts of civil disobedience because they may involve acts that endanger human life..."); 151 CONG. REC. H6262-263 (daily ed. July 21, 2005) (statement of Rep. Sensenbrenner)("There are various definitions of terrorism under Federal law. In title XVIII there has been a confusion over a new definition created in the USA PATRIOT Act for domestic terrorism. That provision is supposed to be used for administrative procedures such as nationwide searches, but another part of the PATRIOT Act, section 806, uses the reference for asset forfeiture, which is more of a penalty. This has raised concerns about those who exercise their first amendment rights. As a result, groups from both sides of the political spectrum have wanted to change the definition for domestic terrorism. This amendment fixes the problem...").

entitled to restitution, 18 U.S.C. 3663A, and victims of other federal crimes are eligible for restitution, 18 U.S.C. 3663.

Section 127 of the Act expresses the sense of Congress that under section 981 victims of terrorist attacks should have access to the assets of terrorists that have been forfeited.

Miscellanea

This section of the report discusses miscellaneous provisions of Title I of the Act which are not easily classifiable within the subheadings above.

FISA Court Rules and Procedures

Section 109(d) of the Act requires the FISA court to publish its rules and procedures and transmit them in unclassified form to all judges on the FISA court, the FISA Court of Review, the Chief Justice of the United States, and the House and Senate Judiciary and Intelligence Committees.

The U.S. Citizenship and Immigration Services

The Act directs the Secretary of Homeland Security to report to the House and Senate Judiciary Committees semi-annually regarding the internal affairs operations and investigations of the U.S. Citizenship and Immigration Services. The first such written report is to be submitted no later than April 1, 2006.[3575]

Cigarette Smuggling

Federal law proscribes trafficking in contraband cigarettes.[3576] Violations are punishable by imprisonment for up to five years,[3577] and constitute racketeering predicate offenses.[3578] During debate on the House floor, several Members pointed to the fact that in at least one instance terrorists had resorted to cigarette smuggling as a financing mechanism.[3579]

[3575] § 109(c), P.L. 109-177, 120 Stat. 205 (2006).

[3576] 18 U.S.C. 2341-2346

[3577] 18 U.S.C. 2344.

[3578] 18 U.S.C. 1961(1). Federal racketeer influenced and corrupt organization laws (RICO) proscribe the acquisition or operation of an enterprise, whose activities affected interstate or foreign commerce, through the patterned commission of other specifically designated crimes (predicate offenses); offenders face imprisonment for up to 20 years and confiscation of offense related property, 18 U.S.C. 1961-1963.

[3579] 151 CONG. REC. H6284 (daily ed. July 21, 2005) (statements of Reps. Coble, Sensenbrenner, Cantor, and Kildee).

Section 121 amends federal law by lowering the threshold definition of contraband cigarettes, from "a quantity in excess of 60,000 cigarettes" to 10,000 cigarettes, and adds a new provision for contraband smokeless tobacco, defined as a quantity in excess of 500 cans or packages of smokeless tobacco. Additionally, the Act creates a federal cause action against violators (other than Indian tribes or Indians in Indian country) for manufacturers, exporters, and state and local authorities.[3580]

Narco-Terrorism

The federal Controlled Substances Act prohibits drug trafficking with severe penalties calibrated according to the kind and volume of drugs and the circumstances involved[3581] (e.g., trafficking in 50 grams or more of crack cocaine is punishable by imprisonment for not less than 10 years and for not more than life; distributing a small amount of marijuana for no remuneration is punishable by imprisonment for not more than one year).[3582] Drug offenses that involved additional egregious circumstances are often subject to multiples of the sanctions for the underlying offense.[3583] Providing material support for the commission of a terrorist crime or to a designated foreign terrorist organization is likewise a federal crime, punishable by imprisonment for not more than 15 years.[3584]

Section 122 of the Act outlaws drug trafficking — for the benefit of a foreign terrorist organization as defined in the immigration laws, 8 U.S.C. 1182(a)(3)(B), or of a person who has or is engaged in terrorism as defined in 22 U.S.C. 2656f(d)(2) (politically motivated violence against civilian targets) — under a wide range of jurisdictional circumstances.[3585] The offense can only be committed

---

[3580] § 121(f), P.L. 109-177, 120 Stat. 223, 224 (2006), adding new 18 U.S.C. 2346(b).

[3581] 21 U.S.C. 841-971.

[3582] 21 U.S.C. 841, 844.

[3583] See, e.g., 21 U.S.C. 859 (sale of drugs to a child: twice the normal penalty); 861 (use a child in drug trafficking: twice the normal penalty); 861(f) (sale of drugs to a pregnant woman: twice the normal penalty).

[3584] 18 U.S.C. 2339A, 2339B.

[3585] § 122, P.L. 109-177, 120 Stat. 225 (2006), adding new 21 U.S.C. 960A(b) ("There is jurisdiction over an offense under this section if — (1) the prohibited drug activity or the terrorist offense is in violation of the criminal laws of the United States; (2) the offense, the prohibited drug activity, or the terrorist offense occurs in or affects interstate for foreign commerce; (3) an offender provides anything of pecuniary value for a terrorist offense that causes or is designed to cause death or serious bodily injury to a national of the United States while that national is outside the United States, or substantial damage to the property of a legal entity organized under the laws of the United States (including any of its States, districts, commonwealths, territories, or possessions) while that property outside of the United States; (4) the offense or the prohibited drug activity occurs in whole or in part outside of the United States including on the high seas),

with the knowledge of the terrorist misconduct of its beneficiaries. Violators face imprisonment for not less than twice the minimum penalty for drug trafficking under 21 U.S.C. 841(b)(1) nor more than life, and period of supervised release of not less than five years.[3586] The Act also expressly prohibits attempts and conspiracies to violate the new section. It may be that 21 U.S.C. 963 would have produced the same result in the absence of an express provision, since it punishes attempts and conspiracies to commit any offense defined in the Controlled Substances Act. It may also be that in conjunction, section 963 and the new section outlaw conspiracies to attempt a substantive violation of the new section.

Interference With the Operation of an Aircraft

It is a federal crime to destroy an aircraft or its facilities under various circumstances giving rise to federal jurisdiction or to attempt, or conspire to do so, 18 U.S.C. 32. Violations are punishable by imprisonment for not more than 20 years. It is likewise a federal crime to interfere with a member of a flight crew in the performance of their duties; this too is punishable by imprisonment for not more than 20 years (or imprisonment for any term of years or for life in the case of assault with a dangerous weapon), 49 U.S.C. 46504.

Section 123 of the Act amends 18 U.S.C. 32 to make it a federal crime to interfere or disable the operator of an aircraft or aircraft facility with reckless disregard for human safety or with the intent to endanger, subject to the same sanctions that apply to other violations of the section. By operation of section 32, the new prohibition extends to attempts and conspiracies to engage in such conduct, 18 U.S.C. 32(a)(7)(redesignated 18 U.S.C. 32(a)(8)).

Investigation of Political Activities

FISA bars the use of various information collection techniques in the course of a foreign intelligence investigation, if the investigation is based solely on the exercise of First Amendment protected rights, 50 U.S.C. 1805(a)(3)(A), 1824(a)(1)(A), 1942(a)(1).

Section 124 of the Act expresses the sense of Congress that the federal government should not conduct criminal investigations of Americans based solely on their membership in non-violent political organizations or their participation in other lawful political activity.

---

and a perpetrator of the offense or the prohibited drug activity is a national of the United States or a legal entity organized under the laws of the United States (including any of its States, districts, commonwealths, territories, or possessions); or (5) after the conduct required for the offense occurs an offender is brought into or found in the United States, even if the conduct required for the offense occurs outside the United States.") In cases where neither the support, the drug offense, nor the terrorism have any connection to the U.S. other than the later presences of the offender here, paragraph 960A(b)(5) may exceed Congress's legislative reach unless the benefit of a treaty obligation can be claimed.

[3586] § 122, P.L. 109-177, 120 Stat. 225 (2006), adding new 21 U.S.C. 960A.

Immunity for Fire Equipment Donors

Section 125 grants immunity from civil liability to the donors (other than manufacturers) of fire equipment to volunteer fire organizations.

Federal Data Mining Report

Section 126 directs the Attorney General to submit a report to Congress within a year after the date of the Act's enactment, concerning the Department of Justice's use or development of "pattern-based" data mining technologies. While the Act provides a definition of "data-mining,"[3587] it does not define "pattern-based."[3588]

Title II: Terrorist Death Penalty Enhancement Act of 2005

Title II of the Act makes several adjustments in federal death penalty law, which concern air piracy cases arising before 1994, a redundant procedural mechanism in federal capital drug cases, supervised release for terrorism offenses, and a transfer of the law governing the appointment of counsel in capital cases.

Pre-1994 Capital Air Piracy Cases

In the late 1960s and early 1970s, the U.S. Supreme Court held unconstitutional the imposition of capital punishment under the procedures then employed by the

---

[3587] § 126, P.L. 109-177, 120 Stat. 228 (2006).

[3588] The want of definition may be significant because the terms are not hermetically sealed legal concepts, see, e.g., Safeguarding Privacy in the Fight Against Terrorism, Report of the Technology and Privacy Advisory Committee, 45 (March 2004)("data mining includes 'pattern-based' searches . . . These [might] involve developing models of what terrorist behavior might look like and then examining databases for similar patterns. This is similar to commercial data mining techniques — businesses develop a pattern of attributes or behaviors that their good customers have in common, and then search databases to find people meeting those patterns — but potentially far more powerful given the range of data to which the government has access and the capacity of data mining to eliminate the need to aggregate data before searching them. As we use the term, data mining may also include 'subject-based' searches, which look for information about a specific individual or links to known terrorist suspects. This has long been a basic tool of criminal investigators everywhere: start with known suspects and, with proper authorization (in many cases, a warrant or a subpoena), look for information about them and the people with whom they interact. However, the power of data mining technology and the range of data to which the government has access have contributed to blurring the line between subject- and pattern-based searches. The broader the search criteria, and the more people other than actual terrorist who will be identified by those criteria, the more pattern-like these searches become. Even when a subject-based search starts with a known suspect, it can be transformed into a pattern-based search as investigators target individuals for investigation solely because of their connection with the suspect. The more tenuous the connection, the more like a pattern-based search it becomes. Searches that lack specific focus on identified suspects do pose greater risk for U.S. persons and should be subject to greater scrutiny and accountability").

federal government and most of the states.[3589] In 1974, Congress established a revised procedure for imposition of the death penalty in certain air piracy cases.[3590] In 1994, when Congress made the procedural adjustments necessary to revive the death penalty as a sentencing option for other federal capital offenses, it replaced the air piracy procedures with those of the new regime.[3591] At least one court, however, held that the new procedures could not be applied retroactively to air piracy cases occurring after the 1974 fix but before the 1994 legislation, in the absence of an explicit statutory provision.[3592]

Section 211 of the Act adds an explicit provision to the end of the 1994 legislation.[3593] The amendment provides for the application of the existing federal capital punishment procedures, 18 U.S.C. ch.228, in addition to consideration of the mitigating and aggravating factors in place prior to the 1994 revival.[3594] Section 211 also provides for severance should any of the 1994 factors be found constitutionally invalid, and includes a definition of "especially heinous, cruel, or depraved" used as an aggravating factor in section 46503, to avoid the vagueness problems that might otherwise attend the use of such an aggravating factor.[3595]

The conference report accompanying H.R. 3199 notes that the changes apply to a relative small group of individuals responsible for murders committed during the course of hijackings in the mid 1980's who would otherwise be eligible for parole within 10 years of sentencing and could not be effectively sentenced to more than 30 years in prison.[3596]

[3589] Furman v. Georgia, 408 U.S. 238 (1972).

[3590] P.L. 93-366, 88 Stat. 409 (1974), 49 U.S.C. 1473 (1976 ed.)

[3591] P.L. 103-322, 108 Stat. 1796, 1970 (1994), 18 U.S.C. 3591-3598.

[3592] United States v. Safarini, 257 F.Supp.2d 191, 202-3 (D.D.C. 2003).

[3593] § 211(a), P.L. 109-177, 120 Stat. 230 (2006), adding subsection 60003(c) to P.L. 103-322, 108 Stat.1970 (1994).

[3594] P.L. 103-272, 108 Stat. 1242 (1994). Because the 1994 legislation was enacted almost immediately after recodification of title 49, 49 U.S.C. 46503 never appeared in the official United States Code or any of its supplements. The predecessor to 49 U.S.C. 46503 as repealed in the 1994 capital punishment revival statute appears in 49 U.S.C. App. 1473 (1988 ed.).

[3595] See, e.g., Maynard v. Cartwright, 486 U.S. 356, 359-61 (1988).

[3596] H.Rept. 109-333, at 101 (2005) ("This provision is particularly important for several reasons. In the absence of a death penalty that could be implemented for pre-FDPA hijacking offenses resulting in death that also occurred before the effective date of the Sentencing Guidelines on November 1, 1987, the maximum penalty available would be life imprisonment. Under the pre-Sentencing Guidelines structure, even prisoners sentenced to life imprisonment were eligible for a parole hearing after serving only ten years. While there is a split in the Circuit Courts of Appeals as to whether a sentencing judge can impose a sentence that could avert the 10-year parole

Life Time Supervised Release Regardless of Risks

Prior to the Act, a federal court could have imposed a sentence of supervised release, to be served upon release from prison, of any term of years or life if the defendant has been convicted of a federal crime of terrorism (18 U.S.C. 2332b(g)(5)(B)) involving the foreseeable risk of physical injury of another, 18 U.S.C. 3583(j).[3597] Section 212 of the Act amends section 3583(j) to eliminate the

---

hearing requirement, the current position of the Bureau of Prisons is that a prisoner is eligible for a parole hearing after serving ten years of a life sentence. Even if parole is denied on that first occasion, such prisoners are eligible to have regularly scheduled parole hearings every two years thereafter. Moreover, in addition to parole eligibility after ten years, the old sentencing and parole laws incorporated a presumption that even persons sentenced to life imprisonment would be released after no more than 30 years. In the context of the individuals responsible for the hijacking incidents described above, most of the perpetrators were no older than in their twenties when they committed their crimes. The imposition of a pre-Guidelines sentence of life imprisonment for these defendants means that many, if not all of them, could be expect to be released from prison well within their lifetime. Given the gravity of these offenses, coupled with the longstanding Congressional intent to have a death penalty available for the offense of air piracy resulting in death, such a result would be at odds with the clear directive of Congress.")

[3597] The federal crimes of terrorism are violations of: 18 U.S.C. 32 (destruction of aircraft or aircraft facilities), 37 (violence at international airports), 81 (arson within special maritime and territorial jurisdiction), 175 or 175b (biological weapons), 175c (variola virus), 229 (chemical weapons), subsection (a), (b), (c), or (d) of section 351 (congressional, cabinet, and Supreme Court assassination and kidnaping), 831 (nuclear materials), 842(m) or (n) (plastic explosives), 844(f)(2) or (3) (arson and bombing of Government property risking or causing death), 844(I) (arson and bombing of property used in interstate commerce), 930(c) (killing or attempted killing during an attack on a Federal facility with a dangerous weapon), 956(a)(1) (conspiracy to murder, kidnap, or maim persons abroad), 1030(a)(1) (protection of computers), 1030(a)(5)(A)(I) resulting in damage as defined in 1030(a)(5)(B) (ii) through (v) (protection of computers), 1114 (killing or attempted killing of officers and employees of the United States), 1116 (murder or manslaughter of foreign officials, official guests, or internationally protected persons), 1203 (hostage taking), 1361 (government property or contracts), 1362 (destruction of communication lines, stations, or systems), 1366(a) (destruction of an energy facility), 1751(a), (b), (c), or (d) (Presidential and Presidential staff assassination and kidnaping), 1992 (train wrecking), 1993 (terrorist attacks and other acts of violence against mass transportation systems), 2155 (destruction of national defense materials, premises, or utilities), 2156 (national defense material, premises, or utilities), 2280 (violence against maritime navigation), 2281 (violence against maritime fixed platforms), 2332 (certain homicides and other violence against United States nationals occurring outside of the United States), 2332a (use of weapons of mass destruction), 2332b (acts of terrorism transcending national boundaries), 2332f (bombing of public places and facilities), 2332g (missile systems designed to destroy aircraft), 2332h (radiological dispersal devices), 2339 (harboring terrorists), 2339A (providing material support to terrorists), 2339B (providing material support to terrorist organizations), 2339C (financing of terrorism), 2340A (torture); 42 U.S.C. 2122 (prohibitions governing atomic weapons), 2284 (sabotage of nuclear facilities or fuel); 49 U.S.C. 46502 (aircraft piracy), the second sentence of 46504 (assault on a flight crew with a dangerous weapon), 46505(b)(3) or (c) (explosive or incendiary devices, or endangerment of human life by means of weapons, on aircraft), 46506 if homicide or attempted homicide is involved (application of certain criminal laws to acts on aircraft), and 60123 (b) (destruction of interstate gas or hazardous liquid pipeline facility). Section 112 of the Act adds 18

requirement that the defendant be convicted of a crime involving a foreseeable risk of injury; conviction of any federal crime of terrorism is sufficient.

Capital Procedures in Drug Cases

Prior to the Act, federal law provided two sets of death penalty procedures for capital drug cases, the procedures applicable in federal capital cases generally, 18 U.S.C. 3591-3598, and the procedures specifically applicable in federal capital drug cases, 21 U.S.C. 848. The two procedures are virtually identical according to United States v. Matthews, 246 F.Supp.2d 137, 141 (N.D.N.Y. 2002). Section 221 of the Act eliminates the specific drug case procedures so that only the general procedures apply in such cases. According to the conference report accompanying H.R. 3199, this "eliminates duplicative death procedures under title 21 of the United States code, and consolidates procedures governing all Federal death penalty prosecutions in existing title 18 of the United States Code, thereby eliminating confusing requirements that trial courts provide two separate sets of jury instructions."[3598]

Appointment of Counsel in Capital Cases

Prior to the Act, the federal capital drug provisions housed provisions for the appointment of counsel to assist indigents facing federal capital charges and indigent federal and state death row inmates during federal habeas proceedings, 21 U.S.C. 848(q)(4)-(10). Section 222 of the Act transfers these provisions to title 18.[3599]

Title III: Reducing Crime and Terrorism at America's Seaports Act of 2005

Title III of the Act, among other things, creates more severe criminal penalties concerning criminal and terrorist activities committed at U.S. seaports or aboard vessels.

Seaport Entry by False Pretenses

The Maritime Transportation Security Act requires the submission to the Department of Homeland Security of vessel and facility security plans that include provisions for establishing and controlling secure areas, 46 U.S.C. 70103(c). It also calls for issuance of transportation security cards in order to regulate access to secure areas, 46 U.S.C. 70105. It contains no specific provisions regarding trespassing upon security areas, but the Coast Guard and Maritime

---

U.S.C. 2339D(foreign military training) and 21 U.S.C. 1010A (narco-terrorism) to the list, 18 U.S.C. 2332b(g)(5)(B) as amended by the Act.

[3598] H.Rept. 109-333, at 102 (2005).

[3599] § 222, P.L. 109-177, 120 Stat. 231 (2006), adding new 18 U.S.C. 3599.

Transportation Act amended its provisions in a manner that suggests the application of state criminal laws as well as criminal sanctions found in the Deepwater Port Act, 33 U.S.C. 1514 (imprisonment for not more than one year); the Ports and Waterways Safety Act, 33 U.S.C. 1232 (imprisonment for not more than 10 years); and the act of June 15, 1917, 50 U.S.C. 192 (imprisonment for not more than 10 years).[3600]

As a general matter, it is a federal crime to use fraud or false pretenses to enter federal property, a vessel or aircraft of the United States, or the secured area in an airport, 18 U.S.C. 1036. The offense is punishable by imprisonment for not more than five years if committed with the intent to commit a felony and imprisonment for not more six months in other cases. The same maximum penalty applies to making a false statement to federal officials or in any matter within the jurisdiction of a federal agency or department, 18 U.S.C. 1001. Possession of phony government identification to defraud the U.S. is a one-year felony, absent further aggravating circumstances under which the sanctions are increased, 18 U.S.C. 1028 (a)(4), (b)(6). Moreover, except to the extent covered by 18 U.S.C. 1036 or 18 U.S.C. 1863 (trespassing in the national forests), unlawful entry to property (federal or otherwise) with the intent to commit a second crime is punishable under the laws of the state in which it occurs, cf., 18 U.S.C. 13.

Section 302 of the Act expands 18 U.S.C. 1036 to cover seaports and increases the penalty for violations with respect to any of the protected areas committed with the intent to commit a felony, from imprisonment for not more than five years to imprisonment for not more than 10 years, amended 18 U.S.C. 1036.[3601] The section also provides a definition of "seaport."[3602]

[3600] 46 U.S.C. 70119 expressly authorizes state and local law enforcement officers to make arrests for violations of these Acts, and notes that the authority is in addition and should not be construed to limit any other authority they may possess.

[3601] "(a)Whoever, by any fraud or false pretense, enters or attempts to enter — (1) any real property belonging in whole or in part to, or leased by, the United States; (2) any vessel or aircraft belonging in whole or in part to, or leased by, the United States; (3) any secured or restricted area of any seaport, designated as secure in an approved security plan, as required under section 70103 of title 46, United States Code, and the rules and regulations promulgated under that section; or (4) any secure area of any airport, shall be punished as provided in subsection (b) of this section. "(b) The punishment for an offense under subsection (a) of this section is — (1) a fine under this title or imprisonment for not more than [5 years] 10 years, or both, if the offense is committed with the intent to commit a felony; or (2) a fine under this title or imprisonment for not more than 6 months, or both, in any other case," 18 U.S.C. 1036(a),(b) as amended by the Act (changes are in italics - deletions in bold).

[3602] "As used in this title, the term 'seaport' means all piers, wharves, docks, and similar structures, adjacent to any waters subject to the jurisdiction of the United States, to which a vessel may be secured, including areas of land, water, or land and water under and in immediate proximity to such structures, buildings on or contiguous to such structures, and the equipment and materials on such structures or in such buildings," new 18 U.S.C. 26 as added by the Act. The

The conference report accompanying H.R. 3199 quotes the Interagency Commission report and describes the problems the amendments are designed to address:

> *According to the Report of the Interagency Commission … '[c]ontrol of access to the seaport or sensitive areas within the seaport is often lacking.' Such unauthorized access is especially problematic, because inappropriate controls may result in the theft of cargo and more dangerously, undetected admission of terrorists. In addition to establishing appropriate physical, procedural, and personnel security for seaports, it is important that U.S. criminal law adequately reflect the seriousness of the offense.*[3603]

However, critics might point out that the section does not deal with all "unauthorized access," only access accomplished by fraud. And, they argue, even if the seriousness of such unauthorized access to seaport restricted areas with criminal intent might warrant imprisonment for up to 10 years, there is nothing in conference or Commission reports to explain the necessity for the comparable penalty increase for the other forms of trespassing upon the other areas covered under section 1036.

Obstructing Maritime Inspections

Various federal laws prohibit the failure to heave to or otherwise obstruct specific maritime inspections under various circumstances.[3604]

Section 303 of the Act establishes a new, general federal crime that outlaws, in the case of vessel subject to the jurisdiction of the United States, the failure to heave to, or to forcibly interfere with the boarding of the vessel by federal law enforcement or resist arrest, or to provide boarding federal law enforcement officers with false information concerning the vessel's cargo, origin, destination, registration, ownership, nationality or crew.[3605] The crime is punishable by imprisonment for not more than five years.

---

term "seaport" does not appear to have been used in any other section of title 18; elsewhere in federal law the term "port" is more commonly used, see, e.g., 6 U.S.C. 468 (Coast Guard's homeland security mission), 18 U.S.C. 2199(stowaways), perhaps to make clear that ports such as those on Great Lakes are covered notwithstanding the fact they may not ordinarily be thought of as "seaports."

[3603] H.Rept. 109-333, at 103 (2005).

[3604] See, e.g., 16 U.S.C. 2435, 2438 (enforcement of the Antarctic Marine Living Resources Convention); 16 U.S.C. 5505, 5508 (high seas fishing compliance).

[3605] § 303(a), P.L. 109-177, 120 Stat. 233, 234, adding new 18 U.S.C. 2237.

Interference with Maritime Commerce

Federal law prohibits violence against maritime navigation, 18 U.S.C. 2280, burning or bombing vessels, 18 U.S.C. 2275, burning or bombing property used in or whose use affects interstate or foreign commerce, 18 U.S.C. 844(I), destruction of property within the special maritime and territorial jurisdiction of the United States, 18 U.S.C. 1363. None of them are punishable by life imprisonment unless death results from their commission.[3606]

Section 304 of the Act creates two new federal crimes. The first makes it a federal crime punishable by imprisonment for any term of years or for life (or the death penalty if death results) to place a dangerous substance or device in the navigable waters of the United States with the intent to damage a vessel or its cargo or to interfere with maritime commerce.[3607]

The second of section 304's provisions makes it a federal crime punishable by imprisonment for not more than 20 years to tamper with any navigational aid maintained by the Coast Guard or St. Lawrence Seaway Development Corporation in manner likely to endanger navigation, new 18 U.S.C. 2282B as added by the Act. Opponents may find the sanctions a bit stiff, but in the words of the conference report, "the Coast Guard maintains over 50,000 navigational aids on more than 25,000 miles of waterways. These aids ... are inviting targets for terrorists."[3608] There may also be some question why the new section is necessary given that section 306 of the Act provides, "Whoever knowingly ... damages, destroys, or disables ... any aid to navigation ... shall be ... imprisoned not more than 20 years," new 18 U.S.C. 2291(a)(3) as added by the Act; see also, new 18 U.S.C. 2291(a)(4) as added by section 306 of the Act ("Whoever knowingly interferes by force or violence with the operation of ... any aid to navigation ..., if such action is likely to endanger the safety of any vessel in navigation").

Transporting Dangerous Materials or Terrorists

Section 305 of the Act establishes two other federal terrorism-related transportation offenses, one for transporting dangerous materials and the other for transporting terrorists.

[3606] For example, section 2280, which among other things, "prohibits destroy[ing] a ship or caus[ing] damage to a ship or to its cargo which is likely to endanger the safe navigation of that ship" or attempting or conspiring to do so is punishable by imprisonment for not more than 20 years or if death results by death or imprisonment for life or any term of years, 18 U.S.C. 2280(a)(1)(C),(H).

[3607] § 304, P.L. 109-177, 120 Stat. 235, adding new 18 U.S.C. 2282A

[3608] H.Rept. 109-333, at 103 (2005).

Transporting Dangerous Materials

It is a federal crime to possess biological agents, chemical weapons, atomic weapons, and nuclear material, each punishable by imprisonment for any term of years or for life.[3609] And although the penalties vary, it is likewise a federal crime to commit any federal crime of terrorism.[3610] Morever, it is a federal crime to provide material support, including transportation, for commission of various terrorist crimes or for the benefit of a designated terrorist organization, 18 U.S.C. 2339A, 2339B, or to transport explosives in interstate or foreign commerce with the knowledge they are intended to be used in injure an individual or damage property, 18 U.S.C. 844(d). Most of these offenses condemn attempts and conspiracies to commit them, and accomplices and coconspirators incur comparable liability in any event.[3611]

Section 305 of the Act establishes a new federal offense which prohibits transporting explosives, biological agents, chemical weapons, radioactive or nuclear material knowing it is intended for use to commit a federal crime of terrorism — aboard a vessel in the United States, in waters subject to U.S. jurisdiction, on the high seas, or aboard a vessel of the United States.[3612] The crime is punishable by imprisonment for any term of years or for life and may be punishable by death if death results from commission of the offense.

Transporting Terrorists

While it is a crime to harbor a terrorist, 18 U.S.C. 2339, or to provide material support, including transportation, for the commission of a terrorist offense or for the benefit of a foreign designated terrorist organization, 18 U.S.C. 2339A, 2339B, such offenses are only punishable by imprisonment for not more than 15 years. The same perceived defect may appear to some in the penalties for aiding and abetting commission of the various federal crimes of terrorism and in the penalties available for committing many of them.[3613]

[3609] 18 U.S.C. 175, 229, 831; 42 U.S.C. 2272.

[3610] Each crime designated in 18 U.S.C. 2332b(g)(5)(B) carries its own penalty.

[3611] 18 U.S.C. 2; United States v. Pinkerton, 328 U.S. 640, 647-48 (1946).

[3612] §305(a), P.L. 109-177, 120 Stat. 236 (2006), adding new 18 U.S.C. 2283.

[3613] For example, destruction of aircraft or violence at international airports in violation of 18 U.S.C. 32 and 73 respectively are punishable by imprisonment for not more than 20 years, unless a death results; and the same penalties apply to computer fraud and abuse violations considered federal crimes of terrorism, 18 U.S.C. 1030(a)(5), (c)(4). Aiding and abetting carries the same penalties as the underlying offense, 18 U.S.C. 2.

Section 305 creates a new federal offense, 18 U.S.C. 2284, punishable by imprisonment for any term of years or for life for transporting an individual knowing he intends to commit, or is fleeing from the commission of, a federal crime of terrorism. Unlike the new 18 U.S.C. 2282A(c), created in section 304, neither of the section 305 offenses have an explicit exception for official activities. Of course, even though facially the new section 2284 forbids transporting terrorists for purposes of extradition or prisoner transfer, it would never likely be read or applied to prevent or punish such activity.

Interference With Maritime Navigation

Chapter 111 of title 18 of the United States Code relates to shipping and by and large outlaws violence in various forms committed against vessels within U.S. jurisdiction.[3614] Other sections of the Code proscribe the use of fire, explosives or violence with sufficient breath of protect shipping under some circumstances. For example, one section condemns the use fire or explosives against property used in (or used in an activity affecting) interstate or foreign commerce, 18 U.S.C. 844(I). Another prohibits destruction of property within the maritime jurisdiction of the Untied States, 18 U.S.C. 1363, and a third, arson within the maritime jurisdiction, 18 U.S.C. 81. Hoaxes relating to violations of chapter 111 are punishable by imprisonment for not more than five years (not more than 20 years if serious injury results and if death results, by imprisonment for any term of years or for life or by death), 18 U.S.C. 1038.

Section 306 of the Act enacts a new chapter 111A supplementing chapter 111 as well as section 1038 and consists of four sections. Of the four sections, two are substantive, proscribing hoaxes and the destruction of vessels or maritime facilities, new 18 U.S.C. 2291, 2292; and two procedural, one providing the jurisdictional base for the substantive offenses, new 18 U.S.C. 2290, and the other barring prosecution of certain misdemeanor or labor violations, new 18 U.S.C. 2993.

According to the conference report accompanying H.R. 3199, "this section harmonizes the somewhat outdated maritime provisions with the existing criminal sanctions for destruction or interference with an aircraft or aircraft facilities in 18 U.S.C. 32, 34, and 35."[3615] It is not surprising, therefore, that the new destruction offense mirrors the substantive provisions for the destruction of

---

[3614] The offenses include 18 U.S.C. 2271 (conspiracy to destroy vessels), 2272 (destruction of vessel by owner); 2273 (destruction of vessel by nonowner); 2274 (destruction or misuse of vessel by person in charge); 2275 (firing or tampering with vessel), 2276 (breaking and entering a vessel); 2277 (explosives or dangerous weapons aboard vessels); 2278 (explosives on vessels carrying steerage passengers); 2279 (boarding vessels before arrival); 2280 (violence against maritime navigation); and 2281 (violence against maritime fixed platforms).

[3615] H.Rept. 109-333, at 104 (2005).

aircraft and their facilities, 18 U.S.C. 32,[3616] although it differs from the aircraft prohibition in several respects. First, it has exceptions for lawful repair and salvage operations and for the lawful transportation of hazardous waste, new 18 U.S.C. 2291(b). Second, in the manner of 18 U.S.C. 1993 (attacks on mass transit), it increases the penalty for violations involving attacks on conveyances carrying certain hazardous materials to life imprisonment, new 18 U.S.C. 2291(c). Third, it tightens the "death results" sentencing escalator so that a sentence of death or imprisonment for life or any term of years is only warranted if the offender intended to cause the resulting death, new 18 U.S.C. 2291(d).

In addition to these, the substantive prohibitions of the new section 2291 differ from the otherwise comparable prohibitions of 18 U.S.C. 2280 (concerning violence against maritime navigation) in two major respects. The proscriptions in section 2280 and those of section 32 generally require that the prohibited damage adversely impact on safe operation;[3617] new section 2291 is less likely to feature a comparable demand.

[3616] "Whoever knowingly — (1) sets fire to, damages, destroys, disables, or wrecks any vessel; (2) places or causes to be placed a destructive device or substance, as defined in section 31(a)(3), or explosive, as defined in section 844(j) in, upon, or near, or otherwise makes or causes to be made unworkable or unusable or hazardous to work or use, any vessel, or any part or other materials used or intended to be used in connection with the operation of a vessel; (3) sets fire to, damages, destroys, disables or places a destructive device or substance in, upon, or near, any maritime facility, including any aid to navigation, lock, canal, or vessel traffic service facility or equipment; (4) interferes by force or violence with the operation of any maritime facility, including any aid to navigation, lock, canal, or vessel traffic service facility or equipment, if such action is likely to endanger the safety of any vessel in navigation; (5) sets fire to, damages, destroys, or disables or places a destructive device or substance in, upon, or near, any appliance, structure, property, machine, or apparatus, or any facility or other material used, or intended to be used, in connection with the operation, maintenance, loading, unloading or storage of any vessel or any cargo carried or intended to be carried on any vessel; (6) performs an act of violence against or incapacitates any individual on any vessel, if such act of violence or incapacitation is likely to endanger the safety of the vessel or those on board; (7) performs an act of violence against a person that causes or is likely to cause serious bodily injury, as defined in section 1365(h)(3), in, upon, or near, any appliance, structure, property, machine, or apparatus, or any facility or other material used, or intended to be used, in connection with the operation, maintenance, loading, unloading or storage of any vessel or any cargo carried or intended to be carried on any vessel; (8) communicates information, knowing the information to be false and under circumstances in which such information may reasonably be believed, thereby endangering the safety of any vessel in navigation; or (9) attempts or conspires to do anything prohibited under paragraphs (1) through (8) of this subsection, shall be fined under this title or imprisoned not more than 20 years, or both," 18 U.S.C. 2291(a) as added by the Act. Section 2291 carries a 20 year maximum sanction for violations. The other sections cited in the report refer to the death penalty (18 U.S.C. 34) and hoax (18 U.S.C. 35) provisions relating to violations of 18 U.S.C. 32.

[3617] "A person who unlawfully and intentionally — (A) seizes or exercises control over a ship by force or threat thereof or any other form of intimidation; (B) performs an act of violence against a person on board a ship if that act is likely to endanger the safe navigation of that ship; (C) destroys a ship or causes damage to a ship or to its cargo which is likely to endanger the safe navigation of that ship; (D) places or causes to be placed on a ship, by any means whatsoever, a

On the other hand, because it is treaty-based, section 2280 enjoys a broader jurisdictional base than new section 2290 is able to provide for new section 2291. By virtue of new section 2290, a violation of new section 2291 is only a federal crime if it is committed within the United States, or the offender or victim is a U.S. national, or the vessel is a U.S. vessel, or a U.S. national is aboard the vessel involved. In the case of subsection 32(b) or section 2280, there need be no more connection to the United States than that the offender is subsequently found or brought here, 18 U.S.C. 32(b), 2280(b)(1)(c). Like section 2280, however, new section 2291 is subject to exceptions for misdemeanor offenses and labor disputes.[3618]

New section 2292 creates a hoax offense in the image of 18 U.S.C. 35 which relates to hoaxes in an aircraft context. It sets a basic civil penalty of not more than $5000 for hoaxes involving violations of the new section 2291 or of chapter 111, the existing shipping chapter.[3619] If the misconduct is committed "knowingly, intentionally, maliciously, or with reckless disregard for the safety of human life," it is punishable by imprisonment for not more than five years.[3620] The Act also requires that in both instances, jurisdiction over the offense is governed by the jurisdiction of the offense that is the subject to the hoax.[3621]

---

device or substance which is likely to destroy that ship, or cause damage to that ship or its cargo which endangers or is likely to endanger the safe navigation of that ship; (E) destroys or seriously damages maritime navigational facilities or seriously interferes with their operation, if such act is likely to endanger the safe navigation of a ship; (F) communicates information, knowing the information to be false and under circumstances in which such information may reasonably be believed, thereby endangering the safe navigation of a ship; (G) injures or kills any person in connection with the commission or the attempted commission of any of the offenses set forth in subparagraphs (A) through (F); or (H) attempts or conspires to do any act prohibited under subparagraphs (A) through (G), shall be fined under this title, imprisoned not more than 20 years, or both; and if the death of any person results from conduct prohibited by this paragraph, shall be punished by death or imprisoned for any term of years or for life,"18 U.S.C. 2280(a)(1).

[3618] "It is a bar to prosecution under this chapter if — (1) if the conduct in question occurred within the United States in relation to a labor dispute, and such conduct is prohibited as a felony under the law of the State in which it was committed; or (2) such conduct is prohibited as a misdemeanor, and not a felony, under the law of the State in which it was committed," new 18 U.S.C. 2293(a) as added by § 306 of the Act, 120 Stat. 239 (2006).

[3619] "Whoever imparts or conveys or causes to be imparted or conveyed false information, knowing the information to be false, concerning an attempt or alleged attempt being made or to be made , to do any act that would be a crime prohibited by this chapter or by chapter 111 of this title, shall be subject to a civil penalty of not more than $5,000, which shall be recoverable in a civil action brought in the name of the United States," new 18 U.S.C. 2292(a) as added by § 306 of the Act, 120 Stat. 239 (2006).

[3620] § 306, P.L. 109-177, 120 Stat. 239 (2006), adding new 18 U.S.C. 2292(b).

[3621] § 306, P.L. 109-177, 120 Stat. 239 (2006), adding new 18 U.S.C. 2292(c).

In the case of hoaxes involving violations of chapter 111, the new section affords the government an alternative ground for prosecution to that offered by 18 U.S.C. 1038.

Theft From Maritime Commerce

Section 307 of the Act expands or clarifies the application of various criminal provisions particularly in the case of maritime commerce.

Theft From Interstate Commerce

Federal law prohibits theft from shipments traveling in interstate or foreign commerce; violations are punishable by imprisonment for not more than 10 years (not more than one year if the value of the property stolen is $1000 or less), 18 U.S.C. 659.

Section 307 increases the penalty for theft of property valued at $1000 or less to imprisonment for not more than three years, 18 U.S.C. 659 as amended by the Act. It also makes it clear that theft from trailers, cargo containers, freight stations, and warehouses are covered, and that the theft of goods awaiting transshipment is also covered, 18 U.S.C. 659 as amended by the Act.

Interstate or Foreign Transportation of Stolen Vessels

Interstate or foreign transportation of a stolen vehicle or aircraft is punishable by imprisonment for not more than 10 years, 18 U.S.C. 2312; receipt of a stolen vehicle or aircraft that has been transported in interstate or foreign commerce carries the same penalty, 18 U.S.C. 2313.

Section 307 expands the coverage of federal law to cover the interstate or foreign transportation of a stolen vessel and receipt of a stolen vessel that has been transported in interstate or overseas, 18 U.S.C. 2311 as amended by the Act. The United States Sentencing Commission is to review the sentencing guidelines application to violations of 18 U.S.C. 659 and 2311. The Attorney General is to see that cargo theft information is included in the Uniform Crime Reports and to report annually to Congress on law enforcement activities relating to theft from interstate or foreign shipments in violations of 18 U.S.C. 659.

Stowaways

Stowing away on a vessel or an aircraft is a federal crime; offenders are subject to imprisonment for not more than one year, 18 U.S.C. 2199. Section 308 of the Act increases the penalty for stowing away from imprisonment for not more than one year to not more than five years (not more than 20 years if the offense is committed with the intent to inflict serious injury upon another or if serious injury to another results; or if death results, by death or imprisonment for any term of years or for life), 18 U.S.C. 2199 as amended by the Act. The "death

results" capital punishment provision of the Act is only triggered if the offender intended to cause a death, 18 U.S.C. 2199(3) as amended by the Act.

Port Security Bribery

Bribery of a federal official is punishable by imprisonment for not more than 15 years, 18 U.S.C. 201; many federal crimes of terrorism carry maximum penalties of imprisonment for not more than 20 years or more.[3622] Those who aid and abet or conspire for the commission of such crimes are subject to sanctions.[3623]

Section 309 of the Act makes it a federal crime to bribe any individual (private or public) with respect to various activities within any secure or restricted area or seaport — with the intent to commit international or domestic terrorism (as defined in 18 U.S.C. 2331). Offenders face imprisonment for not more than 15 years, new 18 U.S.C. 226 as added by the Act.

Smuggling Goods Into the United States

Section 310 increases the sentence of imprisonment for smuggling into the United States from not more than five years to not more than 20 years, 18 U.S.C. 545 as amended by the Act.

Smuggling Goods From the United States

The penalty for smuggling goods into a foreign country by the owners, operators, or crew of a U.S. vessel is imprisonment for not more than five years, 18 U.S.C. 546. Other penalties apply for smuggling or unlawfully exporting specific goods or materials out of the U.S. or into other countries.[3624]

Section 311 of the Act creates a new federal crime which outlaws smuggling goods out of the United States; offenders face imprisonment for not more than 10 years, new 18 U.S.C. 554 as added by the Act. Once smuggling from the U.S. is made a federal offense, corresponding changes in federal forfeiture and custom laws become a possibility.

Federal law proscribes laundering the proceeds of various federal crimes (predicate offenses), 18 U.S.C. 1956, 1957. Smuggling goods into the U.S. in violation of 18 U.S.C. 545 is a money laundering predicate offense, 18 U.S.C.

[3622] See, e.g., 18 U.S.C. 32 (destruction of aircraft, 20 years), 81 (arson, 25 years), 2332a (weapons of mass destruction, life imprisonment).

[3623] 18 U.S.C. 2; United States v. Pinkerton, 340 U.S. 640 (1946).

[3624] See, e.g., 31 U.S.C. 5332 (bulk cash), 21 U.S.C. 953 (controlled substances), 18 U.S.C. 553 (stolen motor vehicles).

1956(c)(7)(D). The proceeds involved in financial transactions in violation of the money laundering statutes are generally subject to confiscation, 18 U.S.C. 981(a)(1)(A). Section 311 adds the new overseas smuggling crime, 18 U.S.C. 554, to the money laundering predicate offense list, 18 U.S.C. 1956(c)(7)(D) as amended by the Act.

Federal law calls for the confiscation of goods smuggled into the United States and of the conveyances used to smuggle them in, 19 U.S.C. 1595a. Section 311 calls for the confiscation of goods smuggled out of the U.S. and of any property used to facilitate the smuggling, new 19 U.S.C. 1595a(d) as added by the Act.

It is a federal crime to remove property from the custody of the Customs Service. Section 311 increases the penalty for violation of this crime to imprisonment for not more than 10 years, 18 U.S.C. 549 as amended by the Act.

Title IV: Combating Terrorism Financing Act of 2005

Title IV of the Act strengthens penalties for money laundering, particularly related to financing terrorism, and makes changes to forfeiture authority. There is also a provision that might be construed to permit pre-trial asset freezes in certain civil forfeiture cases made part of the property owner's criminal trial.

International Emergency Economic Powers Act Penalties

The International Emergency Economic Powers Act (IEEPA), 50 U.S.C. 1701-1707, grants the President the power to impose economic restrictions "to deal with unusual and extraordinary [external] threats to the national security, foreign policy, or economy of the United States," 50 U.S.C. 1701(a). The authority has been invoked among other instances to block Iranian assets, Exec. Order No. 12170, 44 Fed.Reg. 65729 (Nov. 1979); to prohibit trade and certain other transactions with Libya, Exec. Order No. 12543, 51 Fed.Reg. 875 (Jan. 7, 1986); to impose economic sanctions on countries found to be contributing to the proliferation of weapons of mass destruction, Exec. Order No. 12938, 59 Fed. Reg. 59099 (Nov. 14, 1994); to block the assets and prohibit financial transactions with significant narcotics traffickers, 60 Fed.Reg. 54579 (Oct. 21, 1995); and to block the property and prohibit transactions with persons who commit, threaten to commit, or support terrorism, Exec. Order No. 13224, 66 Fed.Reg. 49079 (Sept. 23, 2001).

The Act increases the imprisonment and civil penalty for violations of presidential orders or related regulations issued under IEEPA, including but not limited to those that bar financial dealings with designated terrorists and terrorist groups. Violations are now punishable by a civil penalty of not more

than $50,000 (previously $10,000) and by imprisonment for not more than 20 years (previously 10 years).[3625]

Terrorist Money Laundering

RICO

The federal Racketeer Influenced and Corrupt Organizations (RICO) law imposes severe penalties (up to 20 years imprisonment) for acquiring or operating an enterprise through the commission of a pattern of other crimes (predicate offenses), 18 U.S.C. 1961-1965. One federal money laundering statute prohibits, among other things, using the funds generated by the commission of a predicate offense in a financial transaction designed to conceal the origin of the funds or promote further predicate offenses, 18 U.S.C. 1956. A second statute condemns financial transactions involving more than $10,000 derived from a predicate offense, 18 U.S.C. 1957. Crimes designated RICO predicate offenses automatically qualify as money laundering predicate offenses, 18 U.S.C. 1956(c)(7)(A), 1957(f)(3). Property associated with either a RICO or money laundering violation is subject to confiscation, but RICO forfeiture requires conviction of the property owner, 18 U.S.C. 1963, money laundering forfeiture does not, 18 U.S.C. 1956, 1957, 981.

It is a federal crime to operate a business that transmits money overseas either directly or indirectly, without a license, or for a licensed business to either fail to comply with applicable Treasury Department regulations or to transmit funds that it knows will be used for, or were generated by, criminal activities, 18 U.S.C. 1960.

The Act adds 18 U.S.C. 1960 (illegal money transmissions) to the RICO predicate offense list and consequently to the money laundering predicate offense list, 18 U.S.C. 1961(1) as amended by the Act. The House-passed version of the Reauthorization Act also added 8 U.S.C. 1324a (employing aliens) to the RICO list; however, this provision was not included in the conference bill and consequently is not part of the Act as enacted.

Direct Money Laundering Predicates

Section 403(b) of the Act states, "Section 1956(c)(7)(D) of title 18, United States Code, is amended by striking 'or any felony violation of the Foreign Corrupt Practices Act' and inserting 'any felony violation of the Foreign Corrupt Practices Act.'" However, this grammatical change relating to the Foreign Corrupt Practices Act (dropping the "or" before the reference) is redundant. The Intelligence Reform and Terrorism Prevention Act already made this grammatical fix, 118 Stat. 3774 (2004).

[3625] §402, P.L. 109-177, 120 Stat. 243 (2006), amending 50 U.S.C. 1705.

Investigative Jurisdiction

The Act makes conforming amendments to 18 U.S.C. 1956(e), 1957(e) concerning the money laundering investigative jurisdiction of various components of the Department of Homeland Security.[3626] Procedures for coordination, to avoid duplication of efforts, and because investigative agencies share in the distribution of forfeited property to the extent of their participation in the investigation that led to confiscation, may prove necessary in implementing these provisions, 18 U.S.C. 981(d), (e); 19 U.S.C. 1616a.

Forfeiture for Foreign Crimes

The property of individuals and entities that prepare for or commit acts of international terrorism against the United States or against Americans is subject to federal confiscation, 18 U.S.C. 981(a)(1)(G). Criminal forfeiture is confiscation that occurs upon conviction for a crime for which forfeiture is a consequence, e.g., 18 U.S.C. 1963 (RICO). Civil forfeiture is confiscation accomplished through a civil proceeding conducted against the "offending" property based on its relation to a crime for which forfeiture is a consequence, e.g., 18 U.S.C. 981. Criminal forfeiture is punitive; civil forfeiture is remedial, Calderon-Toledo v. Pearson Yacht Leasing, 416 U.S. 663, 683-88 (1974). A convicted defendant may be required to surrender substitute assets if the property subject to criminal forfeiture is located overseas or otherwise beyond the reach of the court, 18 U.S.C. 853(p). Civil forfeiture ordinarily requires court jurisdiction over the property, but when forfeitable property is held overseas in a financial institution that has a correspondent account in this country the federal government may institute and maintain civil forfeiture proceedings against the funds in the interbank account here, 18 U.S.C. 9871(k).

Article III, section 2 of the United States Constitution declares in part that, "no attainder of treason shall work corruption of blood, or forfeiture of estate except during the life of the person attainted," U.S.Const. Art.III, §3, cl.2. Forfeiture of estate is the confiscation of property simply because it is the property of the

---

[3626] "Violations of this section may be investigated by such components of the Department of Justice as the Attorney General may direct, and by such components of the Department of the Treasury as the Secretary of the Treasury may direct, as appropriate and, with respect to offenses over which the Department of Homeland Security has jurisdiction, by such components of the Department of Homeland Security as the Secretary of Homeland Security may direct, and, with respect to offenses over which the United States Postal Service has jurisdiction, by the Postal Service. Such authority of the Secretary of the Treasury, the Secretary of Homeland Security, and the Postal Service shall be exercised in accordance with an agreement which shall be entered into by the Secretary of the Treasury, the Secretary of Homeland Security, the Postal Service, and the Attorney General. Violations of this section involving offenses described in paragraph (c)(7)(E) may be investigated by such components of the Department of Justice as the Attorney General may direct, and the National Enforcement Investigations Center of the Environmental Protection Agency,"18 U.S.C. 1956(e) as amended by the Act (language added by the Act in italics); the Act amends 18 U.S.C. 1957(e) with similar language.

defendant, without any other connection to the crime for which gives rise to the forfeiture. The constitutional provision applies only in cases of treason, but due process would seem likely to carry the ban to forfeiture of estate incurred as a result of other crimes, particularly lesser crimes.[3627] The assumption may be hypothetical because with a single Civil War exception, until very recently federal law only called for the forfeiture of property that had some nexus to the confiscation-triggering crime beyond mere ownership by the defendant.[3628] Subparagraph 981(a)(1)(G) calls for the confiscation the property of individuals and entities that engage in acts of terrorism against the United States or Americans, 18 U.S.C. 981(a)(1)(G)(i), and under separate clauses any property derived from or used to facilitate such misconduct, 18 U.S.C. 981(a)(1)(G)(ii),(iii). As yet, there no reported cases involving 18 U.S.C. 981(a)(1)(G)(i).

Section 404 of the Act authorizes the federal government to confiscate under civil forfeiture procedures all property of any individual or entity planning or committing an act of international terrorism against a foreign nation or international organization without any further required connection of the property to the terrorist activity other than ownership. The section contemplates forfeiture of property located both here and abroad, since it refers to "all assets, foreign or domestic," but with respect to property located outside of the United States, it requires an act in furtherance of the terrorism to have "occurred within the jurisdiction of the United States."[3629] It is unclear whether the jurisdiction referred to is the subject matter jurisdiction or territorial jurisdiction of the United States or either or both. The due process shadow of Article III, section 3, clause 2 may limit the reach of the proposal to property with some nexus other than ownership to the terrorist act.

Money Laundering Through "Hawalas"

Money laundering in violation of 18 U.S.C. 1956 may take either of two forms (1) engaging in a prohibited financial transaction involving the proceeds of a

---

[3627] United States v. Grande, 620 F.2d 1026,1038 (4th Cir. 1980)("We would agree. . . that if §1963 revives forfeiture of estate as that concept was expressed in the Constitution it is almost certainly invalid because of the irrationality of a ruling that forfeiture of estate cannot be imposed for treason but can be imposed for a pattern of lesser crimes").

[3628] Under the Confiscation Act all the property of Confederate army and naval officers was forfeited, 12 Stat. 589 (1862), but owing to the constitutional reservations of President Lincoln, the forfeiture statute was followed by another declaring that confiscation would only apply during the life time of a member of the Confederate armed forces, 12 Stat. 627 (1862). The Supreme Court read the two together and as a matter statutory construction held that a life estate in the property of the former Confederate naval officer at issue was all that was subject to confiscation, Bigelow v. Forest, 76 U.S. 339, 350 (1869).

[3629] § 404(3), P.L. 109-177, 120 Stat. 244 (2006), adding new subsection 18 U.S.C. 981(a)(1)(G)(iv).

predicate offense, 18 U.S.C. 1956(a)(1), or (2) internationally transporting, transmitting, or transferring the proceeds of a predicate offense, 18 U.S.C. 1956(a)(2). Section 405 of the Act extends the financial transaction offense to include related, parallel transactions and transmissions.[3630]

As the conference report accompanying H.R. 3199 explains, the amendment addresses a feature of the often informal networks called "hawalas," for transfer money overseas:

> *Alternative remittance systems are utilized by terrorists to move and launder large amounts of money around the globe quickly and secretly. These remittance systems, also referred to as "hawala" networks, are used throughout the world, including the Middle East, Europe, North American and South Asia. These systems are desirable to criminals and non-criminals alike because of the anonymity, low cost, efficiency, and access to underdeveloped regions. The United States has taken steps to combat the "hawala" networks by requiring all money transmitters, informal or form, to register as money service businesses.*
>
> *Under current Federal law, a financial transaction constitutes a money laundering offense only if the funds involved in the transaction represent the proceeds of some criminal offense. . . There is some uncertainty, however, as to whether the "proceeds element" is satisfied with regard to each transaction in a money laundering scheme that involves two or more transactions conducted in parallel, only one of which directly makes use of the proceeds from unlawful activity. For example, consider the following transaction: A sends drug proceeds to B, who deposits the money in Bank Account 1. Simultaneously or subsequently, B takes an equal amount of money from Bank Account 2 and sends it to A, or to a person designated by A. The first transaction from A to B clearly satisfies the proceeds element of the money laundering statute, but there is some question as to whether the second transaction — the one that involves only funds withdrawn form Bank Account 2 does so as well. The question has become increasingly important because such parallel transactions are the*

[3630] "For purposes of this paragraph, a financial transaction shall be considered to be one involving the proceeds of specified unlawful activity if it is party of a set of parallel or dependent transactions, any one of which involves the proceeds of specified unlawful activity, and all of which are part of a single plan or arrangement," 18 U.S.C. 1956(a)(1) as amended by § 405, P.L. 109-177, 120 Stat. 244 (2006).

technique used to launder money through the Black Market Peso Exchange and "hawala" network.[3631]

Technical Amendments

Section 406 of the Act corrects a number of typographical and grammatical errors in existing law including changing the reference in section 322 of the USA PATRIOT Act, 115 Stat. 315 (2001), from 18 U.S.C. 2466(b) to 28 U.S.C. 2466(b); changing the phrase "foreign bank" to "foreign financial institution" in 18 U.S.C. 981(k)(relating to forfeiture and interbank accounts); correcting a reference to the Intelligence Reform and Terrorism Prevention Act in 31 U.S.C. 5318(n)(4)(A); capitalizing a reference in the Intelligence Reform and Terrorism Prevention Act (amending 18 U.S.C. 2339C rather than 18 U.S.C. 2339c); and codifying the forfeiture procedure passed as section 316 of the USA PATRIOT Act, 115 Stat. 309 (2001), new 18 U.S.C. 987.

Civil Forfeiture Pre-trial Freezes and Restraining Orders

Federal law permits pre-trial restraining orders to freeze property sought in criminal forfeiture cases, 21 U.S.C. 853(e), and pre-trial restraining orders or the appointment of receivers or conservators in civil forfeiture cases, 18 U.S.C. 983(j). In money laundering civil penalty and forfeiture cases, federal law also permits restraining orders and the appointment of receivers under somewhat different, less demanding procedures with respect to the property of foreign parties held in this country, 18 U.S.C. 1956(b). Section 406 of the Act removes the requirement that the property be that of a foreign party, by amending 18 U.S.C. 1956(b)(3),(4).

Conspiracy Penalties

It is a federal crime to destroy or attempt to destroy commercial motor vehicles or their facilities, 18 U.S.C. 33. Offenders face imprisonment for not more than 20 years. It is also a federal crime to cause or to attempt to cause more than $100,000 worth of damage to an energy facility, 18 U.S.C. 1366. Again, offenders face imprisonment for not more than 20 years. As a general rule, conspiracy to commit these or any other federal crime is punishable by imprisonment for not more than five years, 18 U.S.C. 371, and conspirators are liable for the underlying offense and any other offense committed by any of co-conspirators in the foreseeable furtherance of the criminal scheme, United States v. Pinkerton, 340 U.S. 640 (1946).

For several federal crimes, instead of the general five-year penalty for conspiracy, section 811 of the USA PATRIOT Act used the maximum penalty for the

---

[3631] H.Rept. 109-333, at 107 (2005).

underlying offense as the maximum penalty for conspiracy to commit the underlying offense, 115 Stat. 381-82 (2001). Section 406(c) of the Act allows for the same penalty scheme for conspiracies to violate 18 U.S.C. 33 (destruction of motor vehicles) and 18 U.S.C. 1366 (damage an energy facility).

Laundering the Proceeds of Foreign Terrorist Training

Federal law prohibits laundering the proceeds of various predicate offenses, 18 U.S.C. 1956; in addition to other criminal penalties, property associated with such laundering is subject to confiscation, 18 U.S.C. 981(a)(1)(A). Receipt of military training from a foreign terrorist organization is also a federal crime, 18 U.S.C. 2339D. Section 112 of the Act makes 18 U.S.C. 2339D a federal crime of terrorism under 18 U.S.C. 2332b(g)(5)(B). Federal crimes of terrorism are RICO predicate offenses by definition, 18 U.S.C. 1961(1)(G). RICO predicate offenses are by definition money laundering predicate offenses, 18 U.S.C. 1956(c)(7)(A). Section 409 of the Act makes 18 U.S.C. 2339D a money laundering predicate offense directly, 18 U.S.C. 1956(c)(7)(D). It is not clear why the duplication was thought necessary.

Uniform Procedures for Criminal Forfeitures

The Act contains an amendment to 28 U.S.C. 2461(c), for which there is no explanation in the conference report accompanying H.R. 3199. Nor does the amendment appear in either of the two versions of H.R. 3199 sent to conference. Nor does the amendment appear to have been included in other legislative proposals and thus has not heretofore been the beneficiary of examination in committee or on the floor. The change is captioned "uniform procedures for criminal forfeitures," but it is not facially apparent precisely how the procedures for various criminal forfeitures are disparate or how the amendment makes them more uniform. Part of the difficulty flows from the fact that both section 2461(c) and the Act's amendment are somewhat cryptic. Nevertheless, it seems crafted to make a default procedure into an exclusive procedure.

In its original form, 28 U.S.C. 2461(c) states:

> *If a forfeiture of property is authorized in connection with a violation of an Act of Congress, and any person is charged in an indictment or information with such violation but no specific statutory provision is made for criminal forfeiture upon conviction, the Government may include the forfeiture in the indictment or information in accordance with the Federal Rules of Criminal Procedure, and upon conviction, the court shall order the forfeiture of the property in accordance with the procedures set forth in section 413 of the Controlled Substances Act (21 U.S.C. 853), other than subsection (d) of that section.*

The Act amends section 2461(c) to read:

> *If a person is charged in a criminal case with a violation of an Act of Congress for which the civil or criminal forfeiture of property is authorized, the Government may include notice of the forfeiture in the indictment or information pursuant to the Federal Rules of Criminal Procedure. If the defendant is convicted of the offense giving rise to the forfeiture, the court shall order the forfeiture of the property as part of the sentence in the criminal case pursuant to the Federal Rules of Criminal Procedure and section 3554 of title 18, United States Code. The procedures in section 413 of the Controlled Substances Act (21 U.S.C. 853) apply to all stages of a criminal forfeiture proceeding, except that subsection (d) of such section applies only in cases in which the defendant is convicted of a violation of such Act.*

A casual reading of the original section 2461(c) might suggest that it only applies in the case of a criminal forfeiture statute which fails to indicate what procedure should be used to accomplish confiscation. In fact, section 2461(c) originally allowed confiscation under its criminal forfeiture procedures where civil forfeiture was authorized by statute but criminal forfeiture otherwise was not.[3632] On its face, however, it did not allow the government to merge every civil forfeiture with the criminal prosecution of the property owner. In its original form, section 2461(c) was only available if there was no other criminal forfeiture counterpart for the civil forfeiture.[3633] Under the Act, the distinction no longer exists.

Moreover, since section 2461(c) speaks of treating civil forfeitures as criminal forfeitures after conviction, some courts have held that pre-trial freeze orders available in other criminal forfeiture cases may not be invoked in the case of a

---

[3632] United States v. Razmilovic, 419 F.3d 134,136 (2d Cir. 2005)("Section 2461(c) thus authorizes criminal forfeiture as a punishment for any act for which civil forfeiture is authorized, and allows the government to combine criminal conviction and criminal forfeiture as a consolidated proceeding").

[3633] 18 U.S.C. 2461(c)("If a forfeiture of property is authorized in connection with a violation of an act of Congress, ..an act. but no specific statutory provision is made for criminal forfeiture upon conviction . . ."); United States v. Causey, 309 F.Supp.2d 917, 920 (S.D. Tex. 2004)("Section 981 [relating to civil forfeiture] forms the basis for criminal forfeiture through the application of 28 U.S.C. 2461(c), which allows criminal forfeiture to be sought anytime there is a civil forfeiture provision but no corresponding criminal forfeiture statute"); United States v. Schlesinger, 396 F.Supp.2d 267, 275 (E.D.N.Y. 2005) ("Constructing the statute in this manner makes §2461(c) a broad 'gap filler' that applies whenever civil forfeiture is permitted. In sum, when there is no provision for criminal forfeiture, the government may use a civil forfeiture provision if it includes such allegation in the indictment. In instances where there is a specific criminal forfeiture provision — that specific provision and the procedures that it sets forth — and not the civil forfeiture provision will apply").

section 2461(c) "gap filler."[3634] It is unclear whether the Act is intended to change this result as well. On the one hand, the language of conviction still remains. On the other hand, the description of the role of 21 U.S.C. 853 (which authorizes pre-trial restraining orders) may signal a different result. The statutory language prior to amendment is fairly clear, the procedures of section 853 come into play after conviction: "upon conviction, the court shall order the forfeiture of the property in accordance with the procedures set forth in section 413 of the Controlled Substances Act (21 U.S.C. 853)," 28 U.S.C. 2461(c). The statement in the Act is less conclusive: "The procedures in section 413 of the Controlled Substances Act (21 U.S.C. 853) apply to all stages of a criminal forfeiture proceeding." This change in language suggests that a change in construction may have been intended.

Title V: Miscellaneous Provisions

Title V of the Act contains miscellaneous provisions added in conference and not previously included in either the House or Senate version of H.R. 3199, some of which — like the habeas amendments in the case of state death row inmates, or the adjustments in the role of the Office of Intelligence Policy and Review in the FISA process — may be of special interest.

Justice Department Residency Requirements

United States Attorneys and Assistant United States Attorneys must live within the district for which they are appointed, except in the case of the District of Columbia and the Southern and Eastern Districts of New York, 28 U.S.C. 545. The Attorney supervises and directs litigation in which the United States has an interest, 28 U.S.C. 516-519. He enjoys the authority to marshal, move, and direct the officers, employees, or agencies of the Department of Justice to this end, 28 U.S.C. 509, 510, 547. Section 501 of the Act allows the Attorney General to waive the residency requirement with respect to U.S. Attorneys or Assistant U.S. Attorneys who have been assigned additional duties outside the districts for which they were appointed.[3635] The conference report accompanying H.R. 3199 notes that the amendment will allow Justice Department personnel to be assigned to Iraq, but does not explain why the authority is made retroactive to February 1, 2005.[3636]

Appointment of U.S. Attorneys

[3634] United States v. Razmilovic, 419 F.3d 134,137 (2d Cir. 2005). Note that in some civil forfeiture cases, the government is entitled to a pre-trial freeze order, 18 U.S.C. 983(j).

[3635] § 501, P.L. 109-177, 120 Stat. 246 (2006), amending 28 U.S.C. 545(a).

[3636] H.Rept. 109-333 at 109 (2005).

The Attorney General has the authority to temporarily fill vacancies in the office of United States Attorney, 28 U.S.C. 546. Prior to the Act, if a replacement had not been confirmed and appointed within 120 days, the district court was authorized to make a temporary appointment. The Act repeals the authority of the court and permits the Attorney General's temporary designee to serve until the vacancy is filled by confirmation and appointment.[3637]

Presidential Succession: Homeland Security Secretary

The heads of the various federal departments come within the line of presidential succession, 3 U.S.C. 19(d)(1). Section 503 of the Act adds the Secretary of the Department of Homeland Security to the list following the Secretary of Veterans Affairs.

Confirmation of the Director of BATFE

Prior to the Act, the Attorney General had the responsibility of appointing the Director the Bureau of Alcohol, Tobacco, Firearms and Explosives (BATFE). Section 504 of the Act removes this power from the Attorney General, and vests the appointment in the President with the advice and consent of the Senate, amending section 1111(a)(2) of the Homeland Security Act of 2002, P. L. 107-296, 116 Stat. 2135 (2002).

Qualifications for U.S. Marshals

The President appoints the marshal in each federal judicial district with the advice and consent of the Senate, 28 U.S.C. 561. There are no statutory qualifications. The Act describes a fairly demanding set of minimum qualifications that each marshal "should have,"[3638] which the conference report characterizes as clarifications.[3639] Some may consider this an intrusion upon the constitutional prerogatives of the President. The Constitution does confer upon him the power to nominate and, with the advice and consent of the Senate, to appoint officers of the United States, U.S. Const. art. II, §2. It might be thought

---

[3637] § 502, P.L. 109-177, 120 Stat. 246 (2006), amending 28 U.S.C. 546(c).

[3638] "Each marshal appointed under this section should have — (1) a minimum of 4 years of command-level law enforcement management duties, including personnel, budget, and accountable property issues, in a police department, sheriff's office or Federal law enforcement agency; (2) experience in coordinating with other law enforcement agencies, particularly at the State and local level; (3) college-level academic experience; and (4) experience in or with county, State, and Federal court systems or experience with protection of court personnel, jurors, and witnesses," 28 U.S.C. 561(I) as amended by the Act.

[3639] H.Rept. 109-333 at 109 (2005)("Section 505 of the conference report is a new section. This section clarifies the qualifications individuals should have before joining the United States Marshals").

that to impose minimum qualifications for appointment impermissibly limits the President's power to nominate. But with few exceptions, the offices in question are creatures of statute. They exist by exercise of Congress's constitutional authority "to make all laws necessary and proper for carrying into execution" the constitutional powers of the Congress, the President or Government of the United States, U.S. Const. art. I, §8, cl. 18. The imposition of minimum qualifications is consistent with long practice as to which the Supreme Court has observed:

> *Article II expressly and by implication withholds from Congress power to determine who shall appoint and who shall remove except as to inferior offices. To Congress under its legislative power is given the establishment of offices, the determination of their functions and jurisdiction, the prescribing of reasonable and relevant qualifications and rules of eligibility of appointees, and the fixing of the term for which they are to be appointed, and their compensation — all except as otherwise provided by the Constitution.*[3640]

The terminology used in section 505 of the Act leaves some doubt whether it is intended to require or merely encourage the nomination of candidates exhibiting the statutory qualifications ("each marshal appointed under this section should have ..."). Perhaps more intriguing is why the conferees deemed this particular office and not others appropriate for such treatment. The office has existed since the dawn of the Republic, 1 Stat. 87 (1789), without a statement of required or preferred qualifications. Arguably comparable or more significant offices within the Department of Justice face no similar provisions. No such provisions attend the appointment of U.S. Attorneys, 28 U.S.C. 541; the Director the Federal Bureau of Investigation, 28 U.S.C. 532; the Director of the Marshals Service, 28 U.S.C. 561; or even the Attorney General himself, 28 U.S.C. 503. Even when the Act puts its hand anew to the appointment of an arguably comparable position — the appointment of the Director of BATFE, supra — it says nothing of minimum

---

[3640] Myers v. United States, 272 U.S. 52, 129 (1926)(emphasis added). See also, Corwin, Tenure of Office and the Removal Power Under the Constitution, 27 COLUMBIA LAW REVIEW 353, 391 (1927)("From the first Congress has exercised its power under the 'necessary and proper' clause to fix the qualifications of officers, not only in respect to inferior offices but also in respect to superior offices, and this notwithstanding that in so doing it has obviously restricted the President's power of nomination"); 2 ROTUNDA & NOWAK, TREATISE ON CONSTITUTIONAL LAW: SUBSTANCE AND PROCEDURE 35 (3d ed. 1999)("Congress can limit the President's power to nominate by imposing qualifications that the appointee for the office must possess"); Eldred v. Ashcroft, 537 U.S. 186, 213 (2003)("This Court has repeatedly laid down the principle that a contemporaneous legislative exposition of the Constitution when the founders of our Government and framers of our Constitution were actively participating in public affairs, acquiesced in for a long term of years, fixes the construction to be given the Constitution's provisions"). Justice Brandeis in Myers footnotes literally hundreds of instances dating from the First Congress wherein Congress set minimum qualifications for various public office holders, 272 U.S. at 265 n.35 -274 n.56.

qualifications. Of course, the requirements seem relevant and it is difficult to argue that any federal office should not be filled with the most highly qualified individual possible.

New National Security Division of the DOJ and new Assistant Attorney General

Section 506 of the Act creates a new National Security Division within the Department of Justice (DOJ), headed by a new Assistant Attorney General, comprising prosecutors from the DOJ's Criminal Division's Counterespionage and Counterterrorism sections and attorneys from the DOJ's Office of Intelligence Policy and Review, the office that is responsible for reviewing wiretapping operations under FISA.

Background

The presidential Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction recommended that "[t]he Department of Justice's primary national security elements — the Office of Intelligence Policy and Review, and the Counterterrorism and Counterespionage sections [of the Criminal Division] — should be placed under a new Assistant Attorney General for National Security."[3641] The Commission felt the then-existing organizational scheme might be awkward and that perhaps the system would benefit from a check on Office of Intelligence Policy and Review's rejection of FISA applications as insufficient.[3642]

[3641] The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, Report to the President of the United States, 471-73 (Mar. 31, 2005), available on Jan. 6, 2006 at, [http://www.wmd.gov/report/wmd_report.pdf].

[3642] "The Justice Department's three primary national security components are located in different divisions, with no individual below the Deputy Attorney General who can supervise all three. The Office of Intelligence Policy and Review (OIPR) is responsible for FISA requests, representing the Department of Justice on intelligence-related committees, and advising the Attorney General on 'all matters relating to the national security activities.' It is independent of any division and reports directly to the Deputy Attorney General. In contrast, both the Counterterrorism and Counterespionage sections are located in the Criminal Division, but they each report to two different Deputy Assistant Attorney Generals. If there is method to this madness, neither we, nor any other official with whom we spoke, could identify it. "There is reason to believe that the this awkward (and outdated) organizational scheme has created problems between the Justice Department and the Intelligence Community. In our classified report we describe one such problem that cannot be discussed in our unclassified report. "We believe that bringing the Office of Intelligence Policy and Review closer to its operational counterparts like the Counterespionage and Counterterrorism sections would give the office better insight into actual intelligence practices and make it better attuned to operational needs. Attorneys in the Counterterrorism and Counterespionage sections routinely work alongside FBI agents and other intelligence officers. By contrast, OIPR is largely viewed within the Department as an 'assembly line operation not requiring any special grounding in the facts of a particular matter.' OIPR's job is to process and adjudicate FISA requests — not to follow a case from start to completion. One of the advantages of placing all three national security components under a single Assistant Attorney General is that they will see themselves as acting in concert to serve a

Critics might suggest that curtailing the independence of the Office of Intelligence Policy and Review (OIPR) with an eye to less rigorous examination of FISA applications is likely to have an adverse impact. They might argue that adding another layer of review to the FISA application process can only bring further delays to a process the Administration has continuously sought to streamline. In the same vein, should the judges of the FISA Court conclude that the OIPR has been shackled and ceased to function as an independent gatekeeper for the Court, they might examine applications more closely and feel compelled to modify or reject a greater number; further contributing to delay, or so it might be said. On the other hand, both the Act and the USA PATRIOT Act vest oversight on the exercise of sensitive investigative authority in senior officials in order to guard against abuse.

Be that as it may, the President notified various administration officials that he concurred in the Commission's recommendation.[3643] Section 441 of the Intelligence Authorization Act for Fiscal Year 2006, S. 1803, as reported by the Senate Select Committee on Intelligence, contained similar provisions.[3644]

The Act makes the following provisions for the new Assistant Attorney General:

- Assistant Attorney General (AAG) is to be designated by the President and presented to the Senate for its advice and consent, adding new section 28 U.S.C. 507A(a); cf., H.Rept. 109-142 at 31;
- AAG serves as head of the DOJ National Security Division, as primary DOJ liaison with DNI, and performs other duties as assigned, new 28 U.S.C. 507A(b);
- the Attorney General is to consult with the DNI before recommending a nominee to be AAG, adding new subsection 50 U.S.C. 403-6(c)(2)(C);
- the Attorney General may authorize the AAG to perform the Attorney General's FISA-related duties, amending 50 U.S.C. 1801(g);

---

common mission. "The Bellows Report [Final Report of the Attorney General's Review Team on the Handling of the Los Alamos National Laboratory Investigation] identifies a further reason to have a single individual below the Deputy Attorney General to supervise the OIRP: the need to have a single individual who is knowledgeable about FISA to review FISA applications that are rejected by OIPR. Id. at pp.767-768. The lack of such an individual in the Wen Ho Lee investigation caused serious problems. An Assistant Attorney General for National Security would fit the bill perfectly,"Id. at 472, 482 n.94 (the last paragraph quoted above appears as footnote 94 in the Report).

[3643] S.Rept. 109-142, at 31 (2005)("The President endorsed this recommendation in a June 29, 2005, memorandum for the Vice President, Secretary of State, Secretary of Defense, Attorney General, Secretary of Homeland Security, Director of OMB, DNI, Assistant to the President for National Security Affairs, and Assistant to the President for Homeland Security and Counterterrorism").

[3644] See generally, H.Rept. 109-333, at 109 (2005); H.Rept. 109-142, at 31-33 (2005).

- AAG may approve application for a communications interception (wiretap) order under the Electronic Communications Privacy Act (Title III), amending 18 U.S.C. 2516(1);
- the Attorney General may authorize the AAG to approve admission into the witness protection program, amending 18 U.S.C. 3521(d)(3);
- AAG must provide briefings for the DOJ officials or their designee of Division cases involving classified information, amending 18 U.S.C. App. III 9A(a);
- AAG replaces OIPR for purposes of advising the Attorney General on the development of espionage charging documents and related matters, amending 28 U.S.C. 519 note;
- the Attorney General may authorize the AAG to approve certain undercover operations, amending 28 U.S.C. 533 note;
- AAG joins those whom the Attorney General consult concerning a state application of emergency law enforcement assistance, amending 42 U.S.C. 10502(2)(L);
- the National Security Division headed by the AAG consists of the OIPR, the counterterrorism and counterespionage sections, and any other entities the Attorney General designates, adding new section 28 U.S.C. 509A;
- Division employees are barred from engaging in political management or political campaigns, amending 5 U.S.C. 7323(b)(3);
- subject to a rule change by the Senate, the Senate Select Committee on Intelligence enjoys 20 day sequential referral of AAG nominees, amending section 17 of S.Res. 94-400 of the Standing Rules of the Senate, Senate Manual §94 (2002).

Habeas Corpus in State Capital Cases

Federal law provides expedited habeas corpus procedures in the case of state death row inmates in those states that qualify for application of the procedures and have opted to take advantage of them, 28 U.S.C. ch. 154. As the Supreme Court stated, "Chapter 154 will apply in capital cases only if the State meets certain conditions. A state must establish 'a mechanism for the appointment, compensation, and payment of reasonable litigation expenses of competent counsel' in state postconviction proceedings, and 'must provide standards of competency for the appointment of such counsel,'" Calderon v. Ashmus, 523 U.S. 740, 743 (1998). Thus far apparently, few if any states have sought and been found qualified to opt in.[3645]

[3645] At least for a short period of time Arizona was qualified to opt in, cf., Spears v. Stewart, 283 F.3d 992, 996 (9th Cir. 2002)(denying rehearing en banc)("The three judge panel . . . determined that although (a) the question whether Arizona had opted-in to the short-fuse habeas scheme provided in Chapter 154. . . was entirely irrelevant to the outcome of the case before it; (b) the linchpin provision for the procedures by which Arizona had once sought to opt-in under Chapter 154 had already been repealed by the state; (c) the state did not even comply with its own

Critics implied that the states have been unable to take advantage of the expedited capital procedures only because the courts have a personal stake in the outcome. The solution, they contend, is the amendment found in section 507 of the Act,[3646] which allows the Attorney General to determine whether a state qualifies, permits the determination to have retroactive effect, and allows review by the federal appellate court least likely to have an interest in the outcome, the U.S. Court of Appeals for the D.C. Circuit.[3647] Opponents of the proposal raised separation of powers issues and questioned whether the chief federal prosecutor or the courts are more likely to make an even handed determination of whether the procedures for providing capital defendants with qualified defense counsel are adequate.[3648]

---

procedures in the case before the panel; (d) Arizona was unquestionably not in compliance with Chapter 154 at the time the appeal was heard; (e) in fact, the state had never at any time effectively complied with its short-lived procedures; and (f) no other state in the nation has ever been held to have successfully opted-in under Chapter 154, the panel would seize this opportunity to issue an advisory opinion stating that the no-longer-existent Arizona procedures were in compliance with Chapter 154's requirements")(citing, Ashmus v. Woodford, 202 F.3d 1160, 1160 (9th Cir. 2000)(California has not opted-in); Harris v. Bowersox, 184 F.3d 744, 7848 (8th Cir. 1999)(Missouri has not opted-in); Duvall v. Reynolds, 139 F.3d 768, 776 (10th Cir. 1998)(Oklahoma has not opted-in); Hill v. Butterworth, 941 F.Supp. 1129, 1146-147 (N.D.Fla. 1996), vac'd on other grounds, 147 F.3d 1333 (11th Cir. 1998)(Florida has not opted-in); Mata v. Johnson, 99 F.3d 1261, 1267 (5th Cir. 1996), vac'd on other grounds, 105 F.3d 209 (5th Cir. 1997)(Texas has not opted-in); Austin v. Bell, 126 F.3d 843, 846 n.3 (6th Cir. 1997)(Tennessee has not opted-in); Holloway v. Horn, 161 F.Supp.2d 452, 478 n.11 (E.D.Pa. 2001), rev'd on other grounds, 355 f.3d 707 (3d Cir. 2004)(Pennsylvania has not opted- in); Smith v. Anderson, 104 F.Supp. 2d 773, 786 (S.D.Ohio 2000)(Ohio has not opted-in); Oken v. Nuth, 30 F.Supp.2d 877, 879 (D.Md. 1998)(Maryland has not opted-in); Tillman v. Cook, 25 F.Supp.2d 1245, 1253 (D.Utah 1998)(Utah has not opted-in); Weeks v. Angelone,4 F.Suppl2d 467, 506 n.4 (E.D.Va. 1998)(Virginia has not opted-in); Ryan v. Hopkins, 1996 WL 539220, at *3-4 (D.Neb. 1969)(Nebraska has not opted-in)). Related cases include, Grayson v. Epps, 338 F.Supp.2d 699, 700-704 (S.D. Miss. 2004)(Mississippi has not opted-in); Keel v. French, 162 F.3d 263, 267 n.1 (4th Cir. 1998)(North Carolina has not opted-in); High v. Head, 209 F.3d 1257, 1262 n.4 (11th Cir. 2000)(Georgia does not claim to have opted-in); Allen v. Lee, 366 F.3d 319, 353 (4th Cir. 2004)(Luttig, J. dissenting)(noting that the Fourth Circuit has adopted by rule the section 2266 time lines).

[3646] § 507, P.L. 109-177, 120 Stat. 250 (2006), amending 28 U.S.C. 2261(b), 2265.

[3647] See 151 CONG. REC. S5540, 5541 (daily ed. May 19, 2005) (statement of Sen. Kyl)("The SPA [Streamlined Procedures Act] also expands and improves the special expedited habeas procedures authorized in chapter 154 of the United States Code. The procedures are available to States that establish a system for providing high-quality legal representation to capital defendants. Chapter 154 sets strict time limits on Federal court action and places limits claims. Currently, however, the court that decides whether a State is eligible for chapter 154 is the same court that would be subject to its time limits. Unsurprisingly, these courts have proven resistant to chapter 154. The SPA would place the eligibility decision in the hands of a neutral party — the U.S. Attorney General, with review of his decision in the D.C. Circuit, which does not hear habeas appeals.")

[3648] "[T]he SPA intimates that courts can't objectively evaluate whether states meet the 'opt-in' provisions detailed in the AEDPA because their dockets are implicated in the timelines created by

Under the Act, states would opt-in or would have opted-in as of the date, past or present, upon which the Attorney General determines they established or have established qualifying assistance of counsel mechanism. Opting-in to the expedited procedures of chapter 154 only applies, however, to instances in which "counsel was appointed pursuant to that mechanism [for the death row habeas petitioner], petitioner validly waived counsel, petitioner retained counsel, or petitioner was found not to be indigent."[3649] The standards of qualifying mechanism remain the same except that the Act drops that portion of subsection 2261(d) which bars an attorney from serving as habeas counsel if he represented the prisoner during the state appellate process, amending 28 U.S.C. 2261(d).

The Act establishes a de novo standard of review for the Attorney General's determination before the D.C. Circuit, new 28 U.S.C. 2265(c)(3). It also extends the expedited time deadline for U.S. district court action on a habeas petition from a state death row inmate from 6 to 15 months (180 days to 450 days)(although the 60 days permitted the court for decision following completion of all pleadings, hearings, and submission of briefs remains the same), new 28 U.S.C. 2266(b).

In *McFarland v. Scott*, 512 U.S. 849, 859 (1994), the Supreme Court held that federal district courts might stay the execution of a state death row inmate upon the filing of a petition for the appointment of counsel but prior to the filing of a federal habeas petition in order to allow for the assistance of counsel in the filing the petition.

In an amendment described as overruling McFarland, H.Rept. 109-333, at 109 (2005), the Act amends federal law to permit a stay in such cases of no longer than 90 days after the appointment of counsel or the withdrawal or denial of a request for the appointment of counsel, new 28 U.S.C. 2251(b) as added by section 507(f) of the Act.

---

opt-in status. The legislation attempts to resolve this by empowering the chief prosecutor in the United States, the Attorney General, to make these decisions. Giving federal prosecutors control over even part of the federal judiciary's docket and decisionmaking authority would have serious implications for the separation of powers necessary for fair administration of criminal justice," Habeas Corpus Proceedings and Issues of Actual Innocence: Hearings Before the Senate Comm. on the Judiciary, 109th Cong., 1st sess. (2005) (testimony of Bryan Stevenson, Executive Director of Equal Justice Initiative of Alabama, available on Jan. 6, 2006, at [http://judiciary.senate.gov/print_ testimony.cfm?id=1569&wit_id=4458].

[3649] 28 U.S.C. 2261(b)(2) as amended by the Act.

Title VI: Secret Service Authorization and Technical Modification Act of 2005

The Secret Service provisions of the Act were added to H.R. 3199 during conference. They have several intriguing aspects although the constitutional reach of two provisions may be somewhat limited.

Protection of the President and Certain Other Federal Officials

Under 18 U.S.C. 1752, it is a federal crime:

(1) to willfully and knowingly trespass in areas designated as temporary offices or residences for (or as restricted areas in places visited by or to be visited by) those under Secret Service protection, 18 U.S.C. 1752(a)(1);
(2) to engage in disorderly conduct in or near such areas or places with the intent to and result of impeding or disrupting the orderly conduct of governmental business or functions there, 18 U.S.C. 1752(a)(2);
(3) to willfully and knowingly block passage to and from such areas or places, 18 U.S.C. 1752(a)(3);
(4) to willfully and knowingly commit an act of violence in such area or place, 18 U.S.C. 1752(a)(4); or
(5) to attempt of conspire to do so, 18 U.S.C. 1752(a),(b).

Obstructing Secret Service officers in the performance of their protective duties is also a federal crime and is punishable by imprisonment for not more than one year and/or a fine of not more than $1,000, 18 U.S.C. 3056(d).

Section 602 of the Act increases the penalties for violation of 18 U.S.C. 1752 from imprisonment for not more than six months to imprisonment for not more than one year; unless the offense results in significant bodily injury[3650] or the offender uses or carries a deadly or dangerous weapon during and in relation to the offense, in which case the offense is punishable by imprisonment for not more than 10 years, 18 U.S.C. 1752(b) as amended by the Act. As a general rule applicable here, crimes punishable by imprisonment for not more than six months are subject as an alternative to a fine of not more than $5,000; crimes punishable by imprisonment for not more than one year by a fine of not more than $100,000 as an alternative; crimes punishable by imprisonment for more than one year by a fine of not more than $250,000; and in each case organizations are subject to maximum fines that are twice the amount to which an individual might be fined, 18 U.S.C. 3571, 3559.

[3650] "'Significant bodily injury' means bodily injury which involves a risk of death, significant physical pain, protracted and obvious disfigurement, or a protracted loss or impairment of the function of a bodily member, organ, or mental or sensory faculty," 18 U.S.C. 2118(e)(3), 1752(b)(1)(B) as amended by the Act.

The Act also amends section 1752 to provide a uniform scienter element (willfully and knowingly) for each of the offenses prescribed there.

Special Events of National Significance

Section 602 of the Act also creates a new federal crime relating to misconduct concerning "special events of national significance." It amends 18 U.S.C. 1752 to make it a federal crime "willfully and knowingly to enter or remain in any posted, cordoned off, or otherwise restricted area of a building or grounds so restricted in conjunction with an event designated as a special event of national significance," 18 U.S.C. 1752(a)(2) as amended. The Act provides no definition of "special event of national significance." Nor is the term defined elsewhere in federal law, although it is used in 18 U.S.C. 3056, which authorizes the Secret Service to participate in the coordination of security arrangements for such activities.[3651] The conference report accompanying H.R. 3199 explains that the provisions relate to misconduct at events at which individuals under Secret Service protection are not attendees and by implication are not anticipated to be attendees.[3652] This may raise questions about the constitutional basis upon which the other criminal prohibitions in section 1752 rely.

Congress and the federal government enjoy only those powers which the Constitution provides; all other powers are reserved to the states and to the people, U.S. Const. Amends. X, IX. The Constitution does not vest primary authority to enact and enforce criminal law in the federal government. The Constitution does grant Congress explicit legislative authority in three instances — treason, piracy and offenses against the law of nations, U.S.Const. Art.III, §3; Art.I, §8, cl.10. And it vests Congress with other more general powers which may be exercised through the enactment of related criminal laws, such as the power to regulate commerce or to enact laws for the District of Columbia, U.S.Const. Art.I, §8, cls.3, 17. Nevertheless, "[e]very law enacted by Congress must be based on

---

[3651] "(1) When directed by the President, the United States Secret Service is authorized to participate, under the direction of the Secretary of Homeland Security, in the planning, coordination, and implementation of security operations at special events of national significance, as determined by the President. "(2) At the end of each fiscal year, the President through such agency or office as the President may designate, shall report to the Congress — (A) what events, if any, were designated special events of national significance for security purposes under paragraph (1); and (B) the criteria and information used in making each designation," 18 U.S.C. 3056(e).

[3652] H.Rept. 109-333, at 110 (2005)("Section 602 of the conference report is a new section. 18 U.S.C. 1752 authorizes the Secret Service to charge individuals who breach established security perimeters or engage in other disruptive or potentially dangerous conduct at National Special Security Events (NSSEs) if a Secret Service protectee is attending [or will be attending] the designated event. Section 602 of the conference report expands 18 U.S.C. 1752 to criminalize such security breaches at NSSEs that occur when the Secret Service protectee is not in attendance [and will not be in attendance]")(language in brackets added to demonstrate the reach of section 1752 prior to the Act, and the breadth of the Act's amendment).

one or more of its powers enumerated in the Constitution," United States v. Morrison, 529 U.S. 598, 607 (2000). It is not clear which of Congress's enumerated powers individually or in concert supports under all circumstances the creation of a trespassing offense relating to "restricted areas" temporarily cordoned off or established for a "special event of national significance."

Of course, the protection of such events under many circumstances may fall within one or more of Congress's enumerated powers. For instance, Congress may enact a trespassing law protecting special events held in the District of Columbia by virtue of its power to enact laws for the District, U.S. Const. Art.I, §8, cl.17. Even here, however, the First Amendment may impose impediments when in a particular case the governmental interest in the special event is minimal and significant access restrictions are imposed on use of the streets or other public areas to prevent peaceful protest demonstrations.[3653] Subject to some considerations, events which have an impact on interstate or foreign commerce seem to fall within Congress's power to regulate such commerce, U.S. Const. Art.I, §8, cl. 3.

Interpretative regulations that limit the amendment's application to areas within the scope of Congress's legislative authority and consistent with the demands of the First Amendment offer the prospect of passing constitutional muster. Although the bill repeals the subsection of 1752 which in amended form might authorize curative implementing regulations, such regulatory authority is likely implicit.[3654]

Use of False Credentials to National Special Security Events

Questions as to the breadth of the exercise of Congress's legislative authority might also be raised about section 603 of the Act, which brings special event tickets and credentials within the folds of the statute that outlaws misuse of governmentally issued identification documents, 18 U.S.C. 1028. The structure

[3653] Boos v. Barry, 485 U.S. 312, 318 (1988)("public streets and sidewalk" are "traditional public fora that time out of mind, have been used for purposes of assembly, communicating thoughts between citizens, and discussing public questions. In such places, which occupy a special position in terms of First Amendment protection, the government's ability to restrict expressive activity is very limited")(internal quotation marks and citations omitted).

[3654] "The Secretary of the Treasury is authorized — (1) to designate by regulations the buildings and grounds which constitute the temporary residences of the President or other person protected by the Secret Service and the temporary offices of the President and his staff or of any other person protected by the Secret Service, and (2) to prescribe regulations governing ingress or egress to such buildings and grounds and to posted, cordoned off, or otherwise restricted areas where the President or other person protected by the Secret Service is or will be temporarily visiting," 18 U.S.C. 1752(d). The authority vested in the Secretary of the Treasury passed to the Secretary of Homeland Security when the Secret Service was transferred to that Department, 6 U.S.C. 381. Of course, a conforming amendment to subsection 1752(d) would be required to implement the expanded "special event" area coverage.

of section 1028 makes the point more obviously than might otherwise be the case. In its form prior to the Act, section 1028 prohibited eight particular varieties of unauthorized possession or trafficking in identification documents[3655] when committed under one of three jurisdictional circumstances: the documents are issued or purport to be issued by a federal entity, the documents are used to defraud the United States, or the offense involves transportation in, or affects, interstate or foreign commerce, 18 U.S.C. 1028(a), (c).

The Act makes three changes in the scheme. First, it amends one of the eight prohibition subsections, that which outlaws unlawful possession of U.S. documents or facsimiles thereof, when committed under one of three jurisdictional circumstances. The change adds the documents of special event sponsors to the protected class, if the one jurisdictional predicates is satisfied.[3656] Second, it amends the definition of "identification document" to include special events documents,[3657] so that each of the other eight prohibition subsections

---

[3655] "Whoever, in a circumstance described in subsection (c) of this section — (1) knowingly and without lawful authority produces an identification document, authentication feature, or a false identification document; (2) knowingly transfers an identification document, authentication feature, or a false identification document knowing that such document was stolen or produced without lawful authority; (3) knowingly possesses with intent to use unlawfully or transfer unlawfully five or more identification documents (other than those issued lawfully for the use of the possessor), authentication feature, or false identification documents; (4) knowingly possesses an identification document (other than one issued lawfully for the use of the possessor), authentication feature, or a false identification document, with the intent such document or feature be used to defraud the United States; (5) knowingly produces, transfers, or possesses a document-making implement or authentication feature with the intent such document-making implement or authentication feature will be used in the production of a false identification document or another document-making implement or authentication feature which will be so used; (6) knowingly possesses an identification document or authentication feature that is or appears to be an identification document or authentication feature of the United States which is stolen or produced without lawful authority knowing that such document or feature was stolen or produced without such authority; (7) knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law; or (8) knowingly traffics in false authentication features for use in false identification documents, document-making implements, or means of identification; shall be punished as provided in subsection (b) of this section " 18 U.S.C. 1028(a).

[3656] "Whoever, in a circumstance described in subsection (c) of this section. . . knowingly possesses an identification document or authentication feature that is or appears to be an identification document or authentication feature of the United States or a sponsoring entity of an event designated as a special event of national significance which is stolen or produced without lawful authority knowing that such document was stolen or produced without such authority. . shall be punished as provided in subsection (b) of this section," 18 U.S.C. 1028(a)(6)(amendment in italics).

[3657] "In this section . . . the term 'identification document' means a document made or issued by or under the authority of the United States Government, a State, political subdivision of a State, a sponsoring entity of an event designated as a special event of national significance a foreign government, political subdivision of a foreign government, an international governmental or an

applies as long as one of the three jurisdictional predicates is satisfied. Third, it amends one of the jurisdictional predicates, that which is based on issuance by a federal agency. It treats sponsors of special events as federal agencies within the jurisdictional subsection of section 1028(c).[3658]

It is this third amendment that raises the issue. There is no doubt that Congress has the constitutional power to enact legislation prohibiting possession or trafficking in special event identification documents, if the third jurisdictional predicate is satisfied, i.e., the offense involves transportation in, or affects, interstate or foreign commerce.[3659] Nor is there any dispute Congress enjoys such authority, if the second jurisdiction predicate is satisfied, i.e., the offense involves defrauding the United States.[3660] There may be some question, however, as to the extent to which Congress may prohibit unlawful possession or trafficking in special event identification documents predicated solely upon the fact they were issued by a special event sponsor. "National significance" is not a term that by itself conjures up reference to any of Congress's constitutionally enumerated powers, although the commerce clause might provide an arguably adequate foundation, particularly if regulations confined enforcement to events with an obvious impact on interstate or foreign commerce. Of course, legislation that cannot be traced to one or more of Congress's enumerated powers lies beyond its reach, United States v. Morrison, 529 U.S. 598, 607 (2000).

---

international quasi-governmental organization which, when completed with information concerning a particular individual, is of a type intended or commonly accepted for the purpose of identification of individuals," 18 U.S.C. 1028(d)(3)(amendment in italics).

[3658] "The circumstance referred to in subsection (a) of this section is that — (1) the identification document, authentication feature, or false identification document is or appears to be issued by or under the authority of the United States or a sponsoring entity of an event designated as a special event of national significance or the document-making implement is designed or suited for making such an identification document, authentication feature, or false identification document," 18 U.S.C. 1028(c)(1)(amendment in italics)

[3659] "[M]odern Commerce Clause jurisprudence has identified three broad categories of activity that Congress may regulate under its commerce power. First, Congress may regulate the use of the channels of interstate commerce. Second, Congress is empowered to regulate and protect the instrumentalities of interstate commerce, or persons or things in interstate commerce, even though the threat may come only from intrastate activities. Finally, Congress' commerce authority includes the power to regulate those activities having a substantial relation to interstate commerce, i.e., those activities that substantially affect interstate commerce," United States v. Morrison, 529 U.S. 598, 608-609 (2000)(internal quotation marks and citations omitted); United States v. Lopez, 514 U.S. 549, 558-59 (1995).

[3660] "Congress has authority under the Spending Clause to appropriate federal moneys to promote the general welfare, and it has corresponding authority under the Necessary and Proper Clause, to see to it that taxpayer dollars appropriated under that power are in fact spent for the general welfare, and not frittered away in graft or on projects undermined when funds are siphoned off or corrupt public officers are derelict about demanding value for dollars," Sabri v. United States, 541 U.S. 600, 605 (2004).

Forensic and Investigative Support of Missing and Exploited Children Cases

The PROTECT Act[3661] authorizes "officers and agents of the Secret Service" to provide state and local authorities and the National Center for Missing Exploited Children with investigative and forensic services in missing and exploited children cases, 18 U.S.C. 3056(f). Within the Secret Service, officers and agents conduct investigations, but employees provide forensic services. Section 604 of the Act changes "officers and agents of the Secret Service" to simply "the Secret Service" to reflect this reality.

Secret Service Uniformed Division

The Act amends and transfers the organic authority for the Secret Service Uniformed Division. The conference report's explanation is terse:

> *Section 605 of the conference report is a new section. This section places all authorities of the Uniformed Division, which are currently authorized under title 3, in a newly created 18 U.S.C. §3056A, following the core authorizing statute of the Secret Service (18 U.S.C. §3056), thereby organizing the Uniformed Division under title 18 of the United States Code with other Federal law enforcement agencies.*[3662]

What makes the statement interesting is that the organic authority for most federal law enforcement agencies is not found in title 18. For example, the FBI and the Marshals Service provisions appear not in title 18 but in title 28, 28 U.S.C. 531-540, 561-569; the Inspectors General Offices in appendices to title 5, 5 U.S.C. App. III; the Coast Guard in title 14, 14 U.S.C. chs.1-25; the Customs Service in title 19, 19 U.S.C. 2071-2083.

What is also somewhat intriguing is what is not said. There is no further explanation of the additions, modifications, deletions or apparent duplications associated with the transfer. Existing law lists a series of protective duties the Uniformed Division is authorized to perform, 3 U.S.C. 202. Although it is more geographically specific, it essentially reflects a similar list of some of the duties of the Secret Service as a whole found in 18 U.S.C. 3056.[3663] The Act adds four protective duties to the list: protection of former presidents and their spouses, protection of presidential and vice presidential candidates, protection of visiting

---

[3661] P.L. 108-21, 117 Stat. 650 (2003).

[3662] H.Rept. 109-333, at 111 (2005).

[3663] For example, while both 3 U.S.C. 202 and 18 U.S.C. 3056 authorize protection of the President, Vice President and their families, section 202 authorizes the Uniformed Division to protect the White House, any building housing presidential offices, the Treasury building and certain foreign diplomatic missions located outside of the District of Columbia, 3 U.S.C. 202.

heads of state, and security for special events of nation significance, new 18 U.S.C. 3056A(a)(10)-(13) as added by the Act. All but the special event provisions are already part of the general Secret Service authority under section 3056 (18 U.S.C. 3056(a)(3),(7), (5)). The Act also explicitly authorizes members of the Division to carry firearms, make arrests under certain situations, and perform other duties authorized by law, 18 U.S.C. 3056A(b)(1) as added by the Act — authority they are likely to already enjoy by operation of section 3056, 18 U.S.C. 3056(c)(1)(B), (C), (F), or by virtue of the fact they are vested with "powers similar to those of members of the Metropolitan Police of the District of Columbia," 3 U.S.C. 202.

Section 605(b) of the Act specifically permits the Secretary of Homeland Security to contract out protection of foreign missions and foreign officials outside of the District of Columbia, amending 18 U.S.C. 3056(d).

The Act also repeals 3 U.S.C. 203 (relating to personnel, appointment and vacancies), 204 (relating to grades, salaries, and transfers), 206 (relating to privileges of civil-service appointees), 207 (relating to participation in police and firemen's relief fund),[3664] and 208(b)(relating to authorization of appropriations).

Secret Service as a Distinct Entity

Section 607 of the Act statutorily declares the Secret Service a distinct entity within the Department of Homeland Security, reporting directly to the Secretary, adding new subsection 18 U.S.C. 3056(g).

Exemptions from the Federal Advisory Committee Act

Major presidential and vice presidential candidates are entitled to Secret Service protection, 18 U.S.C. 3056(a)(7). The Secretary of Homeland Security identifies who qualifies as a "major" candidate and therefore is entitled to protection after consulting with an advisory committee consisting of House Speaker and minority leader, the Senate majority and minority leader and fifth member whom they select, id. The Secret Service's electronic crime task forces consist of federal and state law enforcement members as well as representatives from academia and industry who share information concerning computer security and abuse, 18 U.S.C. 3056 note.

The Federal Advisory Commission Act imposes notice, open meeting, record keeping, and reporting requirements on groups classified as federal advisory committees, 5 U.S.C. App. II. Advisory committees are committees, task forces,

[3664] However, section 606 of the Act, 120 Stat. 256 (2006), states that the changes do "not affect the retirement benefits of current employees or annuitants that existed on the day before the effective date of this Act."

and other groups established by the statute, the President, or an executive agency "in the interest of obtaining advice and recommendations for" the President or federal agencies, 5 U.S.C. App. II 3(2). No group consisting entirely of officers or employees of the United States is considered an advisory committee for purposes of the act, id.

It is not clear that either the candidates protection committee or the electronic crimes task forces would be considered advisory committees for purposes of the advisory act. Even if the committee were not exempt because it consists entirely of federal "officers or employees," it seems highly unlikely that it is the type of committee envisioned by Congress when it enacted the act.[3665] As for the task forces, it is not clear that their function is to provide advice and recommendations for agency action. In any event, section 608 of the Act exempts electronic crimes task forces and the candidates protection advisory committee from provisions of the Federal Advisory Committee Act, amending 18 U.S.C. 3056 note, 3056(a)(7).

Title VII: Combat Methamphetamine Epidemic Act of 2005

Title VII of the Act contains subtitles concerning regulation of domestic and international commerce in three methamphetamine (meth) precursor chemicals: ephedrine, pseudoephedrine, and phenylpropanolamine (EPP); increased penalties for methamphetamine offenses; expanded environmentally-related regulations; and adjusted grant programs.[3666] In many of its particulars, Title VII resembles H.R. 3889, the Methamphetamine Epidemic Elimination Act, as amended by the House Committees on Energy and Commerce and on the Judiciary, H.Rept. 109-299 (pts. 1 & 2)(2005).[3667]

Domestic Regulation of Precursor Chemicals

Sales Regulation of "Scheduled Listed Chemicals"

The first part of Title VII addresses the fact that certain cold and allergy medicines — widely and lawfully used for medicinal purposes and readily available in news stands, convenience stores, grocery stores, and drugstores — when collected in bulk can be used to manufacture methamphetamine. At the

---

[3665] Public Citizen v. Department of Justice, 491 U.S. 440, 451-67(1989)(holding the act inapplicable to American Bar Association committee whose advice the Department sought regarding the qualifications of candidates for judicial appointment).

[3666] Related CRS Reports include CRS Report RS22325, Methamphetamine: Legislation and Issues in the 109th Congress, by Celinda Franco, and CRS Report RS22177, The Legal Regulation of Sales of Over-the-Counter Cold Medication, by Jody Feder.

[3667] In many respects, it is also compatible with S. 103 as reported by the Senate Committee on the Judiciary without written report.

federal level, the Food and Drug Administration (FDA) regulates the commercial drug market to ensure the public of safe and effective medicinal products pursuant to the Federal Food Drug and Cosmetic Act, 21 U.S.C. 301-397. The Attorney General through the Drug Enforcement Administration regulates the commercial drug market with respect to drugs with a potential for addiction and abuse, pursuant to the Controlled Substances Act, 21 U.S.C. 801- 904, and the Controlled Substances Import and Export Act, 21 U.S.C. 951-971.

The degree of regulatory scrutiny afforded a particular drug classified as a controlled substance and sometimes certain of the chemicals essential for its production (precursor chemicals, also known as "list chemicals") depends upon the drug's potential for abuse weighed against its possible beneficial uses.[3668] Those who lawfully import, export, produce, prescribe, sell or otherwise dispense drugs classified as controlled substances must be registered, 21 U.S.C. 958, 822. In the case of controlled substances susceptible to abuse and therefore criminal diversion and for certain of their precursor chemicals, the Attorney General may impose production and import/export quotas, security demands, inventory control measures, and extensive registration, record keeping and inspection requirements, 21 U.S.C. 821-830, 954-71. A wide range of civil and criminal sanctions, some of them quite severe, may be imposed for violation of the Controlled Substances Act, the Controlled Substances Import and Export Act, or of the regulations promulgated for their implementation, 21 U.S.C. 841-863, 959-967.[3669]

Prior to the Act, the Controlled Substances Act, in a dizzying array of criss-crossing exceptions and definitions, permitted the over-the-counter sale, without regulatory complications, of cold remedies containing ephedrine, pseudoephedrine or phenylpropanolamine (EPP) — methamphetamine precursors — in packages containing less than 3 grams of EPP base (and in amounts not in excess of 9 grams of pseudoephedrine or phenylpropanolamine base per transaction).[3670] Title VII eliminates the criss-crossing[3671] and replaces it

---

[3668] For example, the so-called "schedule I controlled substances" are those drugs that have "high potential for abuse," that have "no currently accepted medical use in treatment in the United States," and for which there are no "accepted safety for use . . . under medical supervision," 21 U.S.C. 812(b)(1).

[3669] See generally, CRS Report 97-141, Drug Smuggling, Drug Dealing and Drug Abuse: Background and Overview of the Sanctions Under the Federal Controlled Substances Act and Related Statutes, by Charles Doyle.

[3670] All three chemicals are defined as "list I chemicals," 21 U.S.C. 802(34)(C),(I),(K). List I and List II chemicals are defined as "listed chemicals," 21 U.S.C. 802(33). Several of the act's regulatory provisions apply to "regulated transactions" described as including the distribution, receipt, sale, import or export of listed chemicals, 21 U.S.C. 802(39)(A). Regulated transactions, however, do not include transactions involving FDA approved drugs, 21 U.S.C. 802(39)(A)(iv), unless the drug contains EPP (except "ordinary over-the-counter products" defined as products

with a new regulatory scheme for "scheduled listed chemical products," i.e., EPP products,[3672] which:

- limits drugstore, convenience store, grocery store, news stand, lunch wagon (mobile retailer), and other retail sales of EPP products to 3.6 grams of EEP base per customer per day (down from 9 grams per transaction), 21 U.S.C. 830(d), 802(46), 802(47);
- limits mobile retail sales to 7.5 grams of EPP base per customer per month, 21 U.S.C. 830(e)(1)(A);
- insists that EPP products be displayed "behind the counter" (locked up in the case of mobile retailers), 21 U.S.C. 830(e)(1)(A);
- (other than for sales involving 60 milligrams or less of pseudoephedrine) requires sellers to maintain a logbook (for at least two years) recording for every purchase, the time and date of sale, the name and quantity of the product sold, and name and address of the purchaser, 21 U.S.C. 830(e)(1)(A);
- (other than for sales involving 60 milligrams or less of pseudoephedrine) demands that purchasers present a government-issued photo identification, sign the logbook for the sale noting their name and address, and the date and time of the sale, 21 U.S.C. 830(e)(1)(A);
- provides that the logbook must include a warning that false statements are punishable under 18 U.S.C. 1001 with a term of imprisonment of not more than five years and/or a fine of not more than $250,000 (not more than $500,000 for organizations), 21 U.S.C. 830(e)(1)(A), 830(e)(1)(D);
- states that sellers must provide, document, and certify training of their employees on the EPP product statutory and regulatory requirements, 21 U.S.C. 830(e)(1)(A), (B);
- directs the Attorney General to promulgate regulations to protect the privacy of the logbook entries (except for access for federal, state and local law enforcement officials), 21 U.S.C. 830(e)(1)(C);
- affords sellers civil immunity for good faith disclosure of logbook information to law enforcement officials (unless the disclosure constitutes

---

containing not more than 3 grams of an EPP base and unless in liquid form are packaged in blister packs where feasible, 21 U.S.C. 802(45)), 21 U.S.C. 802(39)(iv)(I)(aa), or unless the drug is one the Attorney General has determined is subject to diversion, 21 U.S.C. 802(39)(iv)(I)(bb), and the drug is one with a EPP base in amounts in excess of a threshold established by the Attorney General (except that the threshold for pseudoephedrine and phenylpropanolamine products may be no more than 9 grams of base per transaction and in packages containing no more than 3 grams of base), 21 U.S.C. 802(39)(iv)(II).

[3671] Section 711 of the Act replaces 20 U.S.C. 802(45); section 712 replaces 20 U.S.C. 802(39)(iv).

[3672] The bill defines a "scheduled listed chemicals product" as one "that contains ephedrine, pseudoephedrine, or phenylpropanolamine" and "may be marketed or distributed lawfully in the United States under the Federal, Food Drug, and Cosmetic Act as a nonprescription drug," new 21 U.S.C. 802(45) as added by the Act.

gross negligence or intentional, wanton, or willful misconduct), 21 U.S.C. 830(e)(1)(E);
- requires sellers take measures against possible employee theft or diversion and preempts any state law which precludes them asking prospective employees about past EPP or controlled substance convictions, 21 U.S.C. 830(e)(1)(G);
- sets September 30, 2006 as the effective date for the regulatory scheme (but the 3.6 gram limit on sales would become effective 30 days after enactment).

Federal law imposes monthly reporting requirements on mail order sales of EPP products, 21 U.S.C. 830(b)(3). Under the Act, those subject to the reporting requirement must confirm the identity of their customers under procedures established by the Attorney General, and sales are limited to 7.5 grams of EPP base per customer per month.[3673] If the Attorney General determines that an EPP product cannot be used to produce methamphetamine, he may waive the 3.6 gram limit on retail sales and 7.5 gram limits on mail order and mobile retail sales.[3674]

Sellers who knowingly violate the mail order regulations, or knowingly or recklessly violate the sales regulations, or unlawfully disclose or refuse to disclose EPP logbook sales information, or continue to sell after being prohibited from doing so as a result of past violations, are subject to imprisonment for not more than one year, and/or a fine of not more than $100,000 (not more than $200,000 for organizations), and to a civil penalty of not more than $25,000, 21 U.S.C. 842 as amended by section 711(f) of the Act. During the 30 days after enactment but before the new purchase limits become effective, knowing or intentional retail purchases more than 9 grams of EPP base (7.5 grams in the case of mail order purchases) are punishable by imprisonment for not more than one year and/or a fine of not less than $1,000 nor more than $100,000 (not more than $200,000 for an organization), 21 U.S.C. 844(a) as amended by section 711(e)(1) of the Act.

Authority to Establish Production Quotas

The Controlled Substances Act allows the Attorney General to assess the total annual requirements for various controlled substances and to impose manufacturing quotas accordingly, 21 U.S.C. 826. Section 713 of the Act extends that authority to reach EPP production. For violations, manufacturers face imprisonment for not more than one year, and/or a fine of not more than $100,000 (not more than $200,000 for organizations), and to a civil penalty of not more than $25,000.

[3673] § 711(c)(1), P.L. 109-177, 120 Stat. 261 (2006), adding 21 U.S.C. 830(e)(2).

[3674] § 711(d), P.L. 109-177, 120 Stat. 261, 262 (2006), adding 21 U.S.C. 830(e)(3).

Imports/Exports

The Attorney General enjoys broad general authority to regulate controlled substances imported and exported for legitimate purposes, 21 U.S.C. 952, 953 (neither section mentions listed chemicals). Importers and exporters of list I chemicals (which includes EPP), however, must register with the Attorney General, 21 U.S.C. 958. And they must notify the Attorney General 15 days in advance of any anticipated shipment of listed chemicals to or from the U.S. involving anyone other than a regular source or customer, 21 U.S.C. 971.

Section 715 of the Act expands the statutory statement of the Attorney General's authority to regulate controlled substance imports to include EPP, amending 21 U.S.C. 952. Moreover, it provides implicit statutory confirmation of the Attorney General's authority to set import quotas for EPP by authorizing him to increase the quantity of chemicals importer's registration permits him to bring into the country, new subsection 21 U.S.C. 952(d) as added by the Act. Here and its other adjustments concerning imports and exports, the Act instructs the Attorney General to confer with the U.S. Trade Representative in order to ensure continued compliance with our international trade obligations.

International Regulation of Precursors

Foreign Distribution Chains

The Act also affords the Attorney General renewed notification when the listed chemical transaction, for which approval was initially sought and granted, "falls through," and the importer or exporter substitutes a new subsequent purchaser, 21 U.S.C. 971 as amended.[3675] The Attorney General may require EPP importers to include "chain of distribution" information in their notices that traces the distribution trial from foreign manufacturers to the importer, new subsection 21 U.S.C. 971(h) as added by section 721 of the Act. The Attorney General may seek further information from foreign participants in the chain and refuse to approve transactions involving uncooperative participants, 21 U.S.C. 971(h)(2), (h)(3). Failure to comply with these expanded notice requirements or the bills' EPP import registration and quota provisions is punishable by imprisonment for not more than 10 years and /or a fine of not more than $250,000 (not more than $500,000 for organizations), 21 U.S.C. 960(d)(6) as amended by section 717 of the Act.

[3675] H.Rept. 109-333 (2005)("A problem can arise, however, when the sale that the importer or exporter originally planned falls through. When this happens the importer or exporter must quickly find a new buyer for the chemicals on what is called the "spot marker" — wholesale market. Sellers are often under pressure to find a buyer in a short amount of time, meaning that they may be tempted to entertain bids from companies without a strong record of preventing diversion. More importantly, the Department of Justice has no opportunity to review such transactions in advance and suspend them if there is a danger of diversion to illegal drug production").

Foreign Assistance to Source Countries

The Foreign Assistance Act calls for an annual report on the drug trafficking and related money laundering activities taking place in countries receiving assistance, 22 U.S.C. 2291h. Major illicit drug-producing and drug-transit countries are subject to a procedure featuring presidential certification of cooperative corrective efforts, 22 U.S.C. 2291j. The Act amends the reporting and certification requirements to cover the five largest EPP exporting and the five largest EPP importing countries with the highest rates of diversion, 22 U.S.C. 2291h, 2291j as amended by section 722 of the Act.[3676] It also directs the Secretary of State in consultation with the Attorney General to report to Congress on a plan to deal with the diversion. Section 723 of the Act further instructs the Secretary to take diplomatic action to prevent methamphetamine smuggling from Mexico into the United States and to report to Congress on results of the efforts; the first such report is due not later than one year after the Act's enactment, and every year thereafter.

Enhanced Criminal Penalties for Meth Production and Trafficking

Smuggling Using Commuter Lanes

Unlawful possession of methamphetamine is punishable by imprisonment for terms ranging from not more than 20 years to imprisonment for life depending upon the amount involved and the offender's criminal record, 21 U.S.C. 841(b), 848. Unlawful possession of EPP is punishable by imprisonment for terms ranging from not more than five years to imprisonment for life depending upon the amount involved and the offender's criminal record, 21 U.S.C. 841(c), 848. Similar penalties follow smuggling methamphetamine or EPP, 21 U.S.C. 960, 848. Section 731 of the Act establishes a consecutive term of imprisonment of not more than 15 years to be added to the otherwise applicable sentence when the methamphetamine or EPP offense is committed in connection with quick entry border procedures.

Manufacturing Controlled Substances on Federal Property

The fines for controlled substance offenses that involve cultivation of a controlled substance on federal property are not more than $500,000 individuals and $1 million for organizations, 21 U.S.C. 841(b)(5). The Act establishes the same fine levels for manufacturing a controlled substance on federal property, 21 U.S.C. 841(b)(5) as amended by section 732 of the Act.[3677]

[3676] Similar provisions appear in the House-passed Foreign Relations Authorization Act, Fiscal Years 2006 and 2007 (H.R. 2601)(§1007).

[3677] The change confirms existing law since for purposes of the Controlled Substances Act, "manufacturing" includes "cultivating," 21 U.S.C. 802(15), (22).

Increased Penalties for Drug Kingpins

The Controlled Substances Act punishes major drug traffickers (those guilty of continuing criminal enterprise offenses sometimes known as "drug kingpins"), 21 U.S.C. 848. Drug kingpins, whose offenses involve 300 or more times the amount of controlled substance necessary to trigger the sentencing provisions of 21 U.S.C. 841(b)(1)(B) or whose offenses generate more than $10 million in gross receipts a year, face sentences of mandatory life imprisonment. In the case of a drug kingpin trafficking in methamphetamine, section 733 of the Act lowers the thresholds to 200 or more times the trigger amounts or $5 million in gross receipts a year, new subsection 21 U.S.C. 848(s) as added by the Act.

Cooking or Dealing Near Children

The Controlled Substances Act doubles the otherwise applicable penalties for the distribution or manufacture of controlled substances near schools, playgrounds, video arcades and other similarly designated places likely to be frequented by children, 21 U.S.C. 860. Section 734 of the Act adds a penalty of imprisonment for not more than 20 years to the otherwise applicable penalties for distributing, possessing with the intent to distribute, or manufacturing methamphetamine anywhere where a child under 18 years of age is in fact present or resides, new section 21 U.S.C. 860a as added by the Act.

Reports to the Sentencing Commission

The United States Sentencing Commission establishes and amends federal sentencing guidelines, which must be considered when federal courts impose sentence in a criminal case, 28 U.S.C. 994; 18 U.S.C. 3553; United States v. Booker, 543 U.S. 220, 245 (2005). Every federal judicial district must provide the Commission with detailed reports on each criminal sentence imposed by the district's judges, 28 U.S.C. 994(w). Section 735 of the Act authorizes the Commission to establish the format for such reports and emphasizes the need for a written statement of reasons for the sentence imposed including the reasons for any departure from the sentence advised the by the guidelines, 28 U.S.C. 994(w) as amended by the Act.

Reports to Congress

Section 736 of the Act requires the Attorney General to report twice a year — to the Judiciary Committees; the House Energy and Commerce Committee; the Senate Commerce, Science and Transportation Committee; the House Government Reform Committee; and the Senate Caucus on International Narcotics Control — on the Drug Enforcement Administration's and the Federal Bureau of Investigation's allocation of resources to the investigation and prosecution of methamphetamine offenses.

<u>Enhanced Environmental Regulation of Methamphetamine Byproducts</u>

Transportation of Hazardous Materials

Under the Hazardous Material Transportation Act, the Secretary of Transportation enjoys regulatory authority over the transportation of certain explosive, toxic or otherwise hazardous material, 49 U.S.C. 5103. Section 741 of the Act instructs the Secretary to report every two years to the House Committee on Transportation and Infrastructure and to the Senate Committee on Commerce, Science, and Transportation on whether he has designated as hazardous materials for purposes of the act, all methamphetamine production by-products, 49 U.S.C. 5103(d) as added by the Act.

Solid Waste Disposal

Under the Solid Waste Disposal Act, the Administrator of the Environmental Protection Agency identifies and lists toxic, flammable, corrosive and otherwise hazardous waste, 42 U.S.C. 6921. Section 742 of the Act requires the EPA Administrator to report within two years of enactment, to the House Committee on Energy and Commerce and the Senate Committee on Environment and Public Works, on the information received from law enforcement agencies and others identifying the by-products of illicit methamphetamine product and on which of such by-products the Administrator considers hazardous waste for purposes of the act, new subsection 42 U.S.C. 6921(j) as added by the Act.

Restitution for Methamphetamine Possession

The Act amends the provision under which offenders convicted of violations of the Controlled Substances Act or the Controlled Substances Import and Export Act involving the manufacture of amphetamine or methamphetamine may be ordered to pay restitution and to reimburse governmental entities for cleanup costs, to specifically include restitution and reimbursement in the case of offenses involving simple possession or possession with intent to distribute, 21 U.S.C. 853(q) as amended by section 743 of the Act.[3678] This change was prompted by United States v. Lachowski, 405 F.3d 696, 700 (8th Cir. 2005), which had held that the "offenses involving the manufacture of amphetamine or methamphetamine" upon which a restitution or reimbursement order might be based did not include unlawful possession with intent to distribute methamphetamine. The conferees felt that Lachowski "undermined the ability of the Federal government to seek cleanup costs from methamphetamine traffickers

---

[3678] "The court, when sentencing a defendant convicted of an offense under this subchapter or subchapter II of this chapter involving the manufacture, the possession, or the possession with the intent to distribute, of amphetamine or methamphetamine, shall — (1) order restitution as provided in sections 3612 and 3664 of Title 18; (2) order the defendant to reimburse the United States, the State or local government concerned, or both the United States and the State or local government concerned for the costs incurred by the United States or the State or local government concerned, as the case may be, for the cleanup associated with the manufacture of amphetamine or methamphetamine by the defendant, or on premises or in property that the defendant owns, resides, or does business in; and (3) order restitution to any person injured as a result of the offense as provided in section 3663A of Title 18," 21 U.S.C. 853(q)(amendments in italics).

who are convicted only of methamphetamine possession — even when the methamphetamine lab in question was on the defendant's own property."[3679]

Drug Courts and Grant Programs

Improvements to the DOJ Drug Court Program

The Attorney General may make grants to state, local and tribal governments for the operation of drug courts, 42 U.S.C. 3797u. The Act instructs the Attorney General to prescribe guidelines or regulations to ensure that such programs feature mandatory drug testing and mandatory graduated sanctions for test failures, new subsection 42 U.S.C. 3797u(c) as added by section 751 of the Act, and authorizes appropriations for FY2006 of $70 million, new subsection 42 U.S.C. 3793(25)(A)(v)[inadvertently cited in the Act as 42 U.S.C. 2591(25)(A)(v)] as added by section 752 of the Act. The Attorney General is also directed to study the feasibility of a drug court program for low-level, non-violent federal offenders and to report on the results by June 30, 2006.

Grant Programs

The Act also creates three methamphetamine-related grant programs. One, provided by section 754 of the Act, addresses public safety as well as methamphetamine manufacturing, trafficking and use in "hot spots." Appropriations of $99 million for each of the next five fiscal years (2006-2010) are authorized for grants to the states under the program. The second, section 755 of the Act, authorizes appropriations of $20 million for fiscal years 2006 and 2007 in order to provide grants to the states for programs for drug-endangered children. The third program (services relating to methamphetamine use by pregnant and parenting women offenders), section 756 of the Act, is available to state, local, and tribal governments and supported an authorization of such appropriations as are necessary.

[3679] H.Rept. 109-333, at 116 (2005).

Subchapter I: Electronic Surveillance (50 U.S.C. §§ 1801-1812)

And

Subchapter II: Physical Searches (50 U.S.C. §§ 1821-1829)

The Foreign Intelligence Surveillance Act: An Overview of the Statutory Framework and U.S. Foreign Intelligence Surveillance Court and U.S. Foreign Intelligence Surveillance Court of Review Decisions, RL30465 (February 15, 2007)

ELIZABETH B. BAZAN, CONGRESSIONAL RESEARCH SERV., THE FOREIGN INTELLIGENCE SURVEILLANCE ACT: AN OVERVIEW OF THE STATUTORY FRAMEWORK AND U.S. FOREIGN INTELLIGENCE SURVEILLANCE COURT AND U.S. FOREIGN INTELLIGENCE SURVEILLANCE COURT OF REVIEW DECISIONS (2007), *available at* http://www.intelligencelaw.com/library/secondary/crs/pdf/RL30465_2-15-2007.pdf.

Order Code RL30465

Updated February 15, 2007

Elizabeth B. Bazan
Legislative Attorney
American Law Division

Summary

The Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. § 1801 et seq., as passed in 1978, provided a statutory framework for the use of electronic surveillance in the context of foreign intelligence gathering. In so doing, Congress sought to strike a delicate balance between national security interests and personal privacy rights. Subsequent legislation expanded federal laws dealing with foreign intelligence gathering to address physical searches, pen registers and trap and trace devices, and access to certain business records. The USA PATRIOT Act of 2001, P.L. 107-56, made significant changes to some of these provisions. Further amendments were included in the Intelligence Authorization Act for Fiscal Year 2002, P.L. 107-108, and the Homeland Security Act of 2002, P.L. 107-296, the Intelligence Reform and Terrorism Prevention Act, P.L. 108-458, the

USA PATRIOT Improvement and Reauthorization Act of 2005, P.L. 109-177, and the USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006, P.L. 109178. In addressing international terrorism or espionage, the same factual situation may be the focus of both criminal investigations and foreign intelligence collection efforts. Some of the changes in FISA under these public laws are intended, in part, to facilitate information sharing between law enforcement and intelligence elements. In its Final Report, the 9/11 Commission noted that the removal of the pre-9/11 "wall" between intelligence and law enforcement "has opened up new opportunities for cooperative action within the FBI."

On May 17, 2002, the U.S. Foreign Intelligence Surveillance Court (FISC) issued a memorandum opinion and order written by the then Presiding Judge of the court, and concurred in by all of the other judges then on the court. The unclassified opinion and order were provided to the Senate Judiciary Committee in response to a letter from Senator Leahy, Senator Grassley, and Senator Specter, who released them to the public on August 22, 2002. In its decision, the FISC considered a motion by the U.S. Department of Justice "to vacate the minimization and 'wall' procedures in all cases now or ever before the Court, including this Court's adoption of the Attorney General's July 1995 intelligence sharing procedures, which are not consistent with new intelligence sharing procedures submitted for approval with this motion." The FISC granted the Department's motion, but modified part of what it saw as proposed minimization procedures. This decision was not appealed directly, but the Department of Justice did seek review of an FISC order granting as modified an application for electronic surveillance of an agent of a foreign power and for an FISC order renewing that surveillance, both subject to restrictions based on the May 17 memorandum opinion and order by the FISC. The U.S. Foreign Intelligence Surveillance Court of Review reversed and remanded the FISC orders on November 18, 2002. This report will examine the detailed statutory structure provided by FISA and related provisions of E.O. 12333, and will discuss the decisions of the U.S. Foreign Intelligence Surveillance Court and the U.S. Foreign Intelligence Surveillance Court of Review. It will be updated as subsequent changes require.

Introduction

On October 26, 2001, President George W. Bush signed P.L. 107-56, the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act or the USA PATRIOT Act. Among its provisions are a number which impacted or amended the Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. § 1801 *et seq*., an act which provides a statutory structure for the use of electronic surveillance, physical searches, pen registers, trap and trace devices, and orders requiring production of tangible things within the United States to gather foreign intelligence information or to assist in specified types of investigations.

The changes made to FISA by P.L. 107-56 were far reaching. For example, the law expanded the number of United States district court judges on the Foreign Intelligence Surveillance Court and provided for roving or multipoint electronic surveillance authority under FISA. It amended FISA provisions with respect to pen registers and trap and trace devices, and substantially expanded the reach of the business records provisions to provide a mechanism for production of any tangible thing pursuant to a FISA court order. The amended language changed the certification demanded of a federal officer applying for a FISA order for electronic surveillance or a physical search from requiring a certification that the purpose of the surveillance or physical search is to obtain foreign intelligence information to requiring certification that *a significant purpose* of the surveillance or search is to obtain foreign intelligence information. As implemented, this has made it possible for FISA to be used where the primary purpose of the investigation is criminal investigation, so long as a significant foreign intelligence purpose is also present. FISA, as amended, also affords a private right of action to persons aggrieved by inappropriate use or disclosure of information gathered in or derived from a FISA surveillance or physical search or through the use of a pen register or trap and trace device. Of the amendments made by the USA PATRIOT Act, all but the section which increased the number of judges on the Foreign Intelligence Surveillance Court were set by that Act to sunset on December 31, 2005. P.L. 109-160 and P.L. 109-170 extended the sunset of certain FISA provisions, among others, to February 3, 2006, and March 10, 2006, respectively. The USA PATRIOT Improvement and Reauthorization Act of 2005, P.L. 109-177, replaced the sunset provisions of P.L. 107-56, as amended, with new provisions extending the application of the affected amendments to December 31, 2009. Amendments to FISA were also made by the Intelligence Authorization Act for Fiscal Year 2003, P.L. 107-108; the Homeland Security Act of 2002, P.L. 107-296; and the Intelligence Reform and Terrorism Protection Act of 2004, P.L. 108-458.

In the 109th Congress, two measures, the USA PATRIOT Improvement and Reauthorization Act of 2005, P.L. 109-177, and the USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006, P.L. 109-178, made significant changes to FISA. P.L. 109-177 extended the duration of FISA electronic surveillance, physical searches, and pen register and trap and trace devices. It also added requirements to applications for production of certain sensitive types of records, and expanded the requirements for applications for FISA orders for production of tangible things and for orders authorizing such production. This Act created a new petition review pool within the U.S. Foreign Intelligence Surveillance Court (FISC) to address challenges to such production orders or to related nondisclosure orders, and established a detailed procedure for review of such orders. Further, it directed the Inspector General of the U.S. Department of Justice to perform a comprehensive audit of the effectiveness and use, including improper or illegal use, of the investigative authority under title V of FISA, 50 U.S.C. § 1861 et seq., for fiscal years 2002-2006. The measure modified the requirements for multipoint electronic surveillance under FISA. It also expanded congressional oversight of FISA electronic surveillance, physical searches, and

use of pen registers and trap and trace devices. P.L. 109-178 amends the procedures for judicial review of production and nondisclosure orders under 50 U.S.C. § 1861.

On May 17, 2002, the U.S. Foreign Intelligence Surveillance Court issued an opinion and order[3680] written by the then Presiding Judge of the court, U.S. District Judge Royce C. Lamberth. All of the other judges then on the FISC concurred in the order. The opinion was provided by the current Presiding Judge of the FISC, U.S. District Judge Colleen Kollar-Kotelly, to the Senate Judiciary Committee in response to a July 31 letter from Senator Leahy, Senator Grassley and Senator Specter.[3681] On August 22, 2002, the unclassified opinion was released to the public by Senator Leahy, Senator Grassley and Senator Specter.

In the memorandum opinion and order, the FISC considered a motion by the U.S. Department of Justice "to vacate the minimization and 'wall' procedures in all cases now or ever before the Court, including this Court's adoption of the Attorney General's July 1995 intelligence sharing procedures, which are not consistent with new intelligence sharing procedures submitted for approval with this motion."[3682] In its memorandum and accompanying order, the FISC granted the Department of Justice's motion, but modified the second and third paragraphs of section II.B of the proposed minimization procedures.[3683]

The FISC's May 17th memorandum opinion and order were not appealed directly. However, the Justice Department sought review in the U.S. Foreign Intelligence Court of Review (Court of Review) of an FISC order authorizing electronic surveillance of an agent of a foreign power, subject to restrictions flowing from the May 17th decision, and of an FISC order renewing that surveillance subject to the same restrictions. The Court of Review reversed and remanded the FISC orders.[3684] This opinion, the first issued by the U.S. Foreign Intelligence

---

[3680] In re All Matters Submitted to the Foreign Intelligence Surveillance Court, 218 F. Supp. 2d 611(U.S. Foreign Intell. Surveil. Ct. 2002) (hereinafter FISC op.).

[3681] See, Statement of Sen. Patrick Leahy, Chairman, Committee on the Judiciary, "The USA PATRIOT Act in Practice: Shedding Light on the FISA Process" (Sept. 10, 2002), [http://leahy.senate.gov/press/200209/091002.html]; "Courts," National Journal's Technology Daily (August 22, 2002, PM Edition); "Secret Court Rebuffs Ashcroft; Justice Dept. Chided on Misinformation," by Dan Eggen and Susan Schmidt, Washington Post, p. A1 (August 23, 2002).

[3682] FISC op., 218 F. Supp. 2d at 613.

[3683] *Id.* at 624-27.

[3684] In re Sealed Case, 310 F.3d 717 (U.S. Foreign Intell. Surveil. Ct. Rev. 2002) (hereinafter Court of Review op.). The Foreign Intelligence Surveillance Act, P.L. 95-511, as amended (hereinafter FISA), Title I, § 103, 50 U.S.C. § 1803, created both the U.S. Foreign Intelligence Surveillance Court and the U.S. Foreign Intelligence Surveillance Court of Review. As originally constituted the FISC was made up of 7 U.S. district court judges publicly designated by the Chief Justice of the

SurveillanceCourt of Review since its creation in 1978, was also released to the public. This report will provide background on the Foreign Intelligence Surveillance Act, discuss its statutory framework, and review these two decisions.

Background

Investigations for the purpose of gathering foreign intelligence give rise to a tension between the Government's legitimate national security interests and the protection of privacy interests.[3685] The stage was set for legislation to address these competing concerns in part by Supreme Court decisions on related issues. In Katz v. United States, 389 U.S. 347 (1967), the Court held that the protections of the Fourth Amendment extended to circumstances involving electronic surveillance of oral communications without physical intrusion.[3686] The Katz Court stated, however, that its holding did not extend to cases involving national security.[3687] In United States v. United States District Court, 407 U.S. 297 (1972) (the Keith case), the Court regarded Katz as "implicitly recogniz[ing] that the broad and unsuspected governmental incursions into conversational privacy which electronic surveillance entails necessitate the application of Fourth Amendment safeguards."[3688] Mr. Justice Powell, writing for the Keith Court, framed the matter before the Court as follows:

> *The issue before us is an important one for the people of our country and their Government. It involves the delicate question of the President's power, acting through the Attorney General, to authorize electronic surveillance in internal security matters without prior judicial approval. Successive Presidents for more than one-quarter of a century have authorized such surveillance in varying degrees, without guidance from the Congress or a definitive decision of this Court. This case brings the issue here for the first time. Its resolution is a matter of national concern,*

United States. As amended by the USAPATRIOT Act, P.L. 107-56, § 208, the membership in the FISC was expanded to 11 members, at least 3 of whom must live within a 20 mile radius of the District of Columbia. The U.S. Foreign Intelligence Surveillance Court of Review is made up of 3 U.S. district court or U.S. court of appeals judges publicly designated by the Chief Justice. Subsection 1803(e)(1), as added by Sec. 106(f)(1) of the USA PATRIOT Improvement and Reauthorization Act of 2005, P.L. 109-177, creates a petition review pool of FISC judges to address petitions filed under § 501(f) of FISA, 50 U.S.C. § 1861(f), to challenge production orders or related nondisclosure orders.

[3685] The Fourth Amendment to the United States Constitution states:
The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

[3686] Katz v. United States, 389 U.S. 347, 353 (1967).

[3687] *Id.*, at 359, n. 23.

[3688] United States v. United States District Court, 407 U.S. 297, 313-14 (1972).

> *requiring sensitivity both to the Government's right to protect itself from unlawful subversion and attack and to the citizen's right to be secure in his privacy against unreasonable Government intrusion.*[3689]

The Court held that, in the case of intelligence gathering involving domestic security surveillance, prior judicial approval was required to satisfy the Fourth Amendment.[3690] Justice Powell emphasized that the case before it "require[d] no judgment on the scope of the President's surveillance power with respect to the activities of foreign powers, within or without the country."[3691] The Court expressed no opinion as to "the issues which may be involved with respect to activities of foreign powers or their agents."[3692] However, the guidance which the Court provided in Keith with respect to national security surveillance in a domestic context to some degree presaged the approach Congress was to take in foreign intelligence surveillance. The *Keith* Court observed in part:

> *...We recognize that domestic surveillance may involve different policy and practical considerations from the surveillance of "ordinary crime." The gathering of security intelligence is often long range and involves the interrelation of various sources and types of information. The exact targets of such surveillance may be more difficult to identify than in surveillance operations against many types of crime specified in Title III [of the Omnibus Crime Control and Safe Streets Act, 18 U.S.C. § 2510 et seq.]. Often, too, the emphasis of domestic intelligence gathering is on the prevention of unlawful activity or the enhancement of the Government's preparedness for some possible future crisis or emergency. Thus, the focus of domestic surveillance may be less precise than that directed against more conventional types of*

[3689] 407 U.S. at 299.

[3690] *Id.*, at 391-321. Justice Powell also observed that,

> National security cases ... often reflect a convergence of First and Fourth Amendment values not present in cases of "ordinary" crime. Though the investigative duty of the executive may be stronger in such cases, so also is there greater jeopardy to constitutionally protected speech. "Historically the struggle for freedom of speech and press in England was bound up with the issue of the scope of the search and seizure power," Marcus v. Search Warrant, 367 U.S. 717, 724 (1961).... Fourth Amendment protections become the more necessary when the targets of official surveillance may be those suspected of unorthodoxy in their political beliefs. The danger to political dissent is acute where the Government attempts to act under so vague a concept as the power to protect "domestic security." ....

[3691] *Id.*, at 308.

[3692] *Id.*, at 321-22.

> *crimes. Given these potential distinctions between Title III criminal surveillances and those involving domestic security, Congress may wish to consider protective standards for the latter which differ from those already prescribed for specified crimes in Title III. Different standards may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens. For the warrant application may vary according to the governmental interest to be enforced and the nature of citizen rights deserving protection.... It may be that Congress, for example, would judge that the application and affidavit showing probable cause need not follow the exact requirements of § 2518 but should allege other circumstances more appropriate to domestic security cases; that the request for prior court authorization could, in sensitive cases, be made to any member of a specially designated court...; and that the time and reporting requirements need not be so strict as those in § 2518. The above paragraph does not, of course, attempt to guide the congressional judgment but rather to delineate the present scope of our own opinion. We do not attempt to detail the precise standards for domestic security warrants any more than our decision in Katz sought to set the refined requirements for the specified criminal surveillances which now constitute Title III. We do hold, however, that prior judicial approval is required for the type of domestic surveillance involved in this case and that such approval may be made in accordance with such reasonable standards as the Congress may prescribe.*[3693]

Court of appeals decisions following *Keith* met more squarely the issue of warrantless electronic surveillance in the context of foreign intelligence gathering. In *United States v. Brown*, 484 F.2d 418 (5th Cir. 1973), *cert. denied*, 415 U.S. 960 (1974), the Fifth Circuit upheld the legality of a warrantless wiretap authorized by the Attorney General for foreign intelligence purposes where the conversation of Brown, an American citizen, was incidentally overheard. The Third Circuit in *United States v. Butenko*, 494 F.2d 593 (3rd Cir. 1974), *cert. denied sub nom*, *Ivanov v. United States*, 419 U.S. 881 (1974), concluded that warrantless electronic surveillance was lawful, violating neither Section 605 of the Communications Act nor the Fourth Amendment, if its primary purpose was to gather foreign intelligence information. In its plurality decision in *Zweibon v. Mitchell*, 516 F.2d 594, 613-14 (D.C. Cir. 1975), *cert. denied*, 425 U.S. 944 (1976), the District of Columbia Circuit took a somewhat different view in a case involving a warrantless wiretap of a domestic organization that was not an agent of a foreign power or working in collaboration with a foreign power. Finding that

---

[3693] 407 U.S. at 323-24.

a warrant was required in such circumstances, the plurality also noted that "an analysis of the policies implicated by foreign security surveillance indicates that, absent exigent circumstances, all warrantless electronic surveillance is unreasonable and therefore unconstitutional."

With the passage of the Foreign Intelligence Surveillance Act (FISA), P.L. 95511, Title I, October 25, 1978, 92 Stat. 1796, codified as amended at 50 U.S.C. § 1801 et seq., Congress sought to strike a delicate balance between these interests when the gathering of foreign intelligence involved the use of electronic surveillance.[3694] Collection of foreign intelligence information through electronic surveillance is now governed by FISA and E.O. 12333.[3695] This report will examine the provisions of FISA which deal with electronic surveillance in the foreign intelligence context, as well as those applicable to physical searches, the use of pen registers and trap and trace devices under FISA, and access to business records and other tangible things for foreign intelligence purposes. As the provisions of E.O. 12333 to some extent set the broader context within which FISA operates, we will briefly examine its pertinent provisions first.

Executive Order 12333

Executive Order 12333, 46 Fed. Reg. 59,941 (December 4, 1981), as amended,[3696] 50 U.S.C. § 401 note, deals with "United States Intelligence Activities." Under Section 2.3 of E.O. 12333, the agencies within the Intelligence Community are to "collect, retain or disseminate information concerning United States persons only in accordance with procedures established by the head of the agency concerned and approved by the Attorney General, consistent with the authorities provided by Part 1 of this Order...." Among the types of information that can be collected, retained or disseminated under this section are:

(a) Information that is publicly available or collected with the consent of the person concerned;

[3694] For an examination of the legislative history of P.L. 95-511, see S.Rept. 95-604, Senate Committee on the Judiciary, Parts I and II (Nov. 15, 22, 1977); S.Rept. 95-701, Senate Select Committee on Intelligence (March 14, 1978); H.Rept. 95-1283, House Permanent Select Committee on Intelligence (June 8, 1978); H. Conf. Rept. 95-1720 (Oct. 5, 1978); Senate Reports and House Conference Report are reprinted in 1978 U.S. Code Cong. & Admin. News 3904.

[3695] Physical searches for foreign intelligence information are governed by 50 U.S.C. § 1821 et seq., while the use of pen registers and trap and trace devices in connection with foreign intelligence investigations is addressed in 50 U.S.C. § 1841 et seq. Access to certain business records and other tangible things for foreign intelligence or international terrorism investigative purposes is covered by 50 U.S.C. § 1861 et seq.

[3696] E.O. 12333 was amended by E.O. 13284, 68 Fed. Reg. 4,075 (Jan. 23, 2003), entitled "Amendment of Executive Orders, and Other Actions, in Connection with the Establishment of the Department of Homeland Security" ; and E.O. 13355, 69 Fed. Reg. 53,593 (Aug. 27, 2004), entitled "Strengthened Management of the Intelligence Community".

(b) Information constituting foreign intelligence or counterintelligence, including such information concerning corporations or other commercial organizations. Collection within the United States of foreign intelligence not otherwise obtainable shall be undertaken by the FBI or, when significant foreign intelligence is sought, by other authorized agencies of the Intelligence Community, provided that no foreign intelligence collection by such agencies may be undertaken for the purpose of acquiring information concerning the domestic activities of United States persons;
(c) Information obtained in the course of a lawful foreign intelligence, counterintelligence, international narcotics or international terrorism investigation;
(d) Information needed to protect the safety of any persons or organizations, including those who are targets, victims or hostages of international terrorist organizations;
(e) Information needed to protect foreign intelligence or counterintelligence sources or methods from unauthorized disclosure. Collection within the United States shall be undertaken by the FBI except that other agencies of the Intelligence Community may also collect such information concerning present or former employees, present or former intelligence agency contractors or their present or former employees, or applicants for any such employment or contracting;
(f) Information concerning persons who are reasonably believed to be potential sources or contacts for the purpose of determining their suitability or credibility;
(g) Information arising out of a lawful personnel, physical or communications security investigation;
(h) ...
(i) Incidentally obtained information that may indicate involvement in activities that may violate federal, state, local or foreign laws; and
(j) Information necessary for administrative purposes.

In addition, agencies within the Intelligence Community may disseminate information, other than information derived from signals intelligence, to each appropriate agency within the Intelligence Community for purposes of allowing the recipient agency to determine whether the information is relevant to its responsibilities and can be retained by it.

In discussing collections techniques, Section 2.4 of E.O. 12333 indicates that agencies within the Intelligence Community are to use

> *the least intrusive collection techniques feasible within the United States or directed against United States persons abroad. Agencies are not authorized to use such techniques as electronic surveillance, unconsented physical search, mail surveillance, physical surveillance, or monitoring devices unless they are in accordance with procedures established by the head of the agency*

concerned and approved by the Attorney General. Such procedures shall protect constitutional and other legal rights and limit use of such information to lawful governmental purposes....

Section 2.5 of the Executive Order 12333 states that:

The Attorney General hereby is delegated the power to approve the use for intelligence purposes, within the United States or against a United States person abroad, of any technique for which a warrant would be required if undertaken for law enforcement purposes, provided that such techniques shall not be undertaken unless the Attorney General has determined in each case that there is probable cause to believe that the technique is directed against a foreign power or an agent of a foreign power. Electronic surveillance, as defined in the Foreign Intelligence Surveillance Act of 1978 [section 1801 et seq. of this title], shall be conducted in accordance with that Act, as well as this Order.

The Foreign Intelligence Surveillance Act

The Statutory Framework

The Foreign Intelligence Surveillance Act (FISA), P.L. 95-511, Title I, October 25, 1978, 92 Stat. 1796, codified at 50 U.S.C. § 1801 et seq., as amended, provides a framework for the use of electronic surveillance[3697] and physical searches[3698] to

---

[3697] 50 U.S.C. § 1801(f)(2) defines "electronic surveillance" to mean:
(1) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes;
(2) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any person thereto, if such acquisition occurs in the United States, but does not include the acquisition of those communications of computer trespassers that would be permissible under section 2511(2)(i) of Title 18;
(3) the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States; or
(4) the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes. The italicized portion of Subsection 1801(f)(2) was added by Sec. 1003 of P.L. 107-56.

[3698] A "physical search" is defined under section 301(5) of FISA, 50 U.S.C. § 1821(5), to mean: any physical intrusion within the United States into premises or property (including examination of the interior of property by technical means) that is intended to result in seizure, reproduction, inspection, or alteration of information, material, or property, under circumstances in which a

obtain foreign intelligence information.[3699] It also provides a statutory structure for the installation and use of pen registers and trap and trace devices[3700] and for

---

person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, but does not include (A) "electronic surveillance", as defined in section 1801(f) of this title [50 U.S.C.], or (B) the acquisition by the United States Government of foreign intelligence information from international or foreign communications, or foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic communications system, utilizing a means other than electronic surveillance as defined in [50 U.S.C. § 1801(f)].

[3699] "Foreign intelligence information" is defined in 50 U.S.C. § 1801(e) to mean:
(1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against —
(A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
(B) sabotage or international terrorism by a foreign power or an agent of a foreign power;
(C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or
(2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to —
(A) the national defense or the security of the United States; or
(B) the conduct of the foreign affairs of the United States.

"International terrorism" is defined in 50 U.S.C. § 1801(c) to mean activities that:
(1) involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or any State;
(2) appear to be intended —
(A) to intimidate or coerce a civilian population;
(B) to influence the policy of a government by intimidation or coercion; or
(C) to affect the conduct of a government by assassination or kidnapping; and
(3) occur totally outside the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum.

"Sabotage" is defined in 50 U.S.C. § 1801(d) to mean "activities that involve a violation of chapter 105 of Title 18, or that would involve such a violation if committed against the United States."

[3700] Pen registers and trap and trace devices are addressed in title IV of FISA, 50 U.S.C. § 1841 et seq. Subsection 401(2) of FISA, 50 U.S.C. § 1841(2) defines "pen register" and "trap and trace device" by cross-reference to 18 U.S.C. § 3127. Under 18 U.S.C. § 3127(3), "pen register" is defined to mean: a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication, but such term does not include any device or process used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device or process used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business.

The term "trap and trace device" is defined under 18 U.S.C. § 3127(4) to mean: "a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication."

---

orders requiring production of tangible things for use in federal investigations to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities.[3701] Such an investigation of a United States person may not be conducted solely on the basis of activities protected by the First Amendment to the Constitution.[3702] This measure seeks to strike a balance between national security needs in the context of foreign intelligence gathering and privacy rights.

Creation of the U.S. Foreign Intelligence Surveillance Court and the U.S. Foreign Intelligence Court of Review.

FISA establishes two special courts, the U.S. Foreign Intelligence Surveillance Court (FISC) and the U.S. Foreign Intelligence Surveillance Court of Review (Court of Review), comprised of federal judges to address applications for court orders authorizing such electronic surveillance, physical searches, installation

---

[3701] 50 U.S.C. § 1861. In addition to the provisions dealing with electronic surveillance, physical searches and pen registers and trap and trace devices, FISA includes a section which, subject to subsection 1861(a)(3), permits the Director of the FBI or his designee (whose rank may be no lower than an Assistant Special Agent in Charge) to apply for an order requiring "production of any tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities...." 50 U.S.C. § 1861(a)(1). Where such an investigation is of a United States person, it may not be conducted "solely upon the basis of activities protected by the first amendment to the Constitution." *Id.* Subsection 1861(a)(3) was added by P.L. 109-177. It provides that, in the case of an application for an order requiring the production of library circulation records, library patron lists, book sales records, book customer lists, firearms sales records, tax return records, educational records, or medical records containing information that would identify a person, the Director of the Federal Bureau of Investigation may delegate the authority to make such application to either the Deputy Director of the Federal Bureau of Investigation or the Executive Assistant Director for National Security (or any successor position). The Deputy Director or the Executive Assistant Director are prohibited from further delegation of such authority. Although this section is entitled "access to certain business records for foreign intelligence and international terrorism investigations," it encompasses substantially more than just business records. The current language of 50 U.S.C. §§ 1861 and 1862 (which deals with congressional oversight of all such requests for production of tangible things under § 1861) was added by the USA PATRIOT Act, and amended by P.L. 107-108. It replaced former 50 U.S.C. §§ 1861-1863, added by P.L. 105-272, title VI, § 602, 112 Stat. 2411 (Oct. 20, 1998), which defined various terms, provided for applications for orders for access to certain limited types of business records (relating to records in the possession of common carriers, physical storage facilities, public accommodation facilities, and vehicle rental facilities) for foreign intelligence and international terrorism investigations, and provided for congressional oversight of such records requests. For more information on title V of FISA, 50 U.S.C. §§ 1861-1862, see the section of this report entitled "Access to certain business records and other tangible things for foreign intelligence purposes," *infra*.

[3702] Section 402(a)(1) of FISA, 50 U.S.C. § 1842(a)(1); Section 501(a)(1) and (a)(2)(B) of FISA, 50 U.S.C. § 1861(a)(1) and (a)(2)(B).

and use of pen registers and trap and trace devices, and production of tangible things.[3703]

Under 50 U.S.C. § 1803(a),[3704] the Chief Justice of the United States must publicly designate eleven U.S. district court judges from seven of the United States judicial circuits, of whom no fewer than three must reside within 20 miles of the District of Columbia. These eleven judges constitute the U.S. Foreign Intelligence Surveillance Court (FISC), which has jurisdiction over applications for and orders approving electronic surveillance,[3705] physical searches,[3706] pen registers or trap and trace devices[3707] or orders for production of tangible things[3708] anywhere within the United States under FISA. If an application for electronic surveillance[3709] or a physical search[3710] under this Act is denied by one judge of this court, it may not then be considered by another judge on the court. If a judge denies such an application, he or she must immediately provide a written statement for the record of the reason(s) for this decision.[3711]

The Chief Justice also publicly designates the three U.S. district court or U.S. court of appeals judges who together make up the U.S. Foreign Intelligence Surveillance Court of Review (Court of Review).[3712] This court has jurisdiction to review any denial of an order under FISA.[3713] If the United States appeals an FISC denial of an application, the record from the FISC must be transmitted under seal to the Court of Review established.

[3703] For a more detailed discussion of the FISC and the Court of Review, see CRS Report RL33833, The U.S. Foreign Intelligence Surveillance Court and the U.S. Foreign Intelligence Surveillance Court of Review: An Overview, by Elizabeth B. Bazan.

[3704] When FISA was enacted in 1978, the FISC was made up of seven judges; Section 208 of P.L. 107-56 increased that number to eleven.

[3705] Cf., 50 U.S.C. § 1802(b).

[3706] 50 U.S.C. § 1822(c).

[3707] 50 U.S.C. § 1842(b) and (d).

[3708] 50 U.S.C. § 1861(b) and (c).

[3709] 50 U.S.C. § 1803(a).

[3710] 50 U.S.C. § 1822(c).

[3711] 50 U.S.C. §§ 1803(a), 1822(c).

[3712] 50 U.S.C. § 1803(b).

[3713] 50 U.S.C. §§ 1803(b); see also, 50 U.S.C. §§ 1822(d), 1861(f)(3).

If the Court of Review determines that an application was properly denied, again a written statement of the reason(s) for the court's decision must be provided for the record. The United States may petition for a writ of certiorari to the United States Supreme Court for review of that decision.[3714] All proceedings under FISA must be conducted expeditiously, and the record of all proceedings including applications and orders granted, must be maintained under security measures established by the Chief Justice in consultation with the Attorney General and the Director of National Intelligence.[3715]

Three FISC judges who reside within 20 miles of the District of Columbia, or, if all of such judges are unavailable, other judges of the FISC designated by the presiding judge of such court, comprise a petition review pool which has jurisdiction to review petitions filed pursuant to 50 U.S.C. § 1861(f)(1) challenging production orders and non-disclosure orders.[3716]

The judges of the FISC and the Court of Review serve for seven year terms and may not be redesignated.[3717] The FISC and the Court of Review may establish rules and procedures, and may take such actions, as are reasonably necessary to administer their responsibilities under FISA.[3718] The FISC has established the FOREIGN INTELLIGENCE SURVEILLANCE COURT RULES OF PROCEDURE, and PROCEDURES FOR REVIEW OF PETITIONS FILED PURSUANT TO SECTION 501(F) OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED have also been adopted.[3719]

[3714] 50 U.S.C. § 1803(b); see also, 50 U.S.C. §§ 1822(d), 1861(f)(3).

[3715] 50 U.S.C. § 1803(c).

[3716] 50 U.S.C. § 1803(e), added by Subsection 106(f)(1) of P.L. 109-177. Under 50 U.S.C. § 1803(e)(2), the FISC was required to adopt and, consistent with the protection of national security, to publish procedures for the review of petitions filed pursuant to 50 U.S.C. § 1861(f)(1) by the panel established under Subsection 1803(e)(1). Subsection 1803(e)(2) further directed that such procedures provide that review of a petition shall be conducted in camera and also provide for the designation of an acting presiding judge. Under Rule 8(a) of the PROCEDURES FOR REVIEW OF PETITIONS FILED PURSUANT TO SECTION 501(F) OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED, Clerk of the Court notifies the Presiding Judge of the FISC when a petition is received. If the Presiding Judge is unavailable, the local FISC judge, other than the Presiding Judge, who has the greatest seniority on the FISC is notified by the Clerk of the Court. If no local judge is available, the Clerk of the Court notifies the most senior FISC judge reasonably available. The judge notified is the Acting Presiding Judge for that case.

[3717] 50 U.S.C. § 1803(d).

[3718] 50 U.S.C. § 1803(f)(1), added by P.L. 109-177, Subsection 109(d).

[3719] Both are available at [http://www.uscourts.gov/rules/fisa.html].

Rules of procedure for the Court of Review have not been identified. Any such rules and procedures, and any modifications thereto, must be recorded and transmitted in an unclassified form (although they may include a classified annex) to all of the judges on the FISC; all of the judges on the Court of Review; the Chief Justice of the United States; the Committee on the Judiciary of the Senate and of the House of Representatives; and the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence.[3720]

Electronic surveillance under FISA.

Electronic surveillance under title I of FISA, 50 U.S.C. § 1801 et seq., is generally conducted under an FISC order, unless the surveillance fits within one of three statutory exceptions.[3721]

50 U.S.C. § 1802 — Electronic Surveillance of Certain Foreign Powers Without a Court Order.

The first of these exceptions is electronic surveillance of certain foreign powers without a court order upon Attorney General certification that specific criteria have been met. Under section 101(g) of FISA, 50 U.S.C. § 1801(g), as amended by Subsection 506(a)(5) of P.L. 109-177, the term "Attorney General" is defined to mean "the Attorney General of the United States (or Acting Attorney General), the Deputy Attorney General, or, upon the designation of the Attorney General, the Assistant Attorney General designated as the Assistant Attorney General for National Security under section 507A of title 28, United States Code."[3722]

[3720] 50 U.S.C. § 1803(f)(2), as added by P.L. 109-177, Subsection 109(d).

[3721] These three exceptions are: 50 U.S.C. § 1802 (electronic surveillance of three categories of foreign powers for up to one year without a court order upon Attorney General certification; the three categories, as defined in 50 U.S.C. §§ 1801(a)(1), (2), or (3), cover (1) a foreign government or any component thereof, whether or not recognized by the United States; (2) a faction of a foreign nation or nations, not substantially composed of United States persons; or (3) an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments); 50 U.S.C. § 1805(f) (emergency electronic surveillance upon Attorney General certification for up to 72 hours while an FISC order is being sought); and 50 U.S.C. § 1811 (electronic surveillance for 15 calendar days after a congressional declaration of war).

[3722] Section 507A was added to title 28, U.S.C., by P.L. 109-177, Section 506(a)(1). It provides:
§ 507A. Assistant Attorney General for National Security
(a) Of the Assistant Attorneys General appointed under section 506, one shall serve, upon the designation of the President, as the Assistant Attorney General for National Security.
(b) The Assistant Attorney General for National Security shall —
(1) serve as the head of the National Security Division of the Department of Justice under section 509A of this title;
(2) serve as primary liaison to the Director of National Intelligence for the Department of Justice; and

(3) perform such other duties as the Attorney General may prescribe.

Under 50 U.S.C. § 1802, the President, through the Attorney General, may authorize electronic surveillance to acquire foreign intelligence information for up to one year without a court order if two criteria are satisfied. First, to utilize this authority, the Attorney General must certify in writing under oath that:
(A) the electronic surveillance is solely directed at —
(i) the acquisition of the contents of communications transmitted by means of communications used exclusively between or among foreign powers, as defined in [50 U.S.C. § 1801(a)(1), (2), or (3)]; or
(ii) the acquisition of technical intelligence, other than the spoken communications of individuals, from property or premises under the open and exclusive control of a foreign power, as defined in [50 U.S.C. § 1801(a)(1), (2) or (3)];
(B) there is no substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person is a party; and
(C) the proposed minimization procedures with respect to such surveillance meet the definition of minimization procedures under [50 U.S.C. § 1801(h)];[3723]

[3723] Minimization procedures with respect to electronic surveillance are defined in 50 U.S.C. § 1801(h) to mean:
(1) specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information;
(2) procedures that require that nonpublicly available information, which is not foreign intelligence information, as defined in subsection (e)(1) of this section, shall not be disseminated in a manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to understand foreign intelligence information or assess its importance;
(3) notwithstanding paragraphs (1) and (2), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes; and
(4) notwithstanding paragraphs (1), (2), and (3), with respect to any electronic surveillance approved pursuant to section 1802(a) of this title, procedures that require that no contents of any communication to which a United States person is a party shall be disclosed, disseminated, or used for any purpose or retained for longer than 72 hours unless a court order under section 1805 of this title is obtained or unless the Attorney General determines that the information indicates a threat of death or serious bodily harm to any person.

Sec. 314(a)(1) of H.Rept. 107-328, the conference report on the Intelligence Authorization Act for Fiscal Year 2002 to accompany H.R. 2883, amended 50 U.S.C. § 1801(h)(4) to change to 72 hours what was previously a 24 hour period beyond which the contents of any communication to which a U.S. person is a party may not be retained absent a court order under 50 U.S.C. § 1805 or a finding by the Attorney General that the information indicates a threat of death or serious bodily injury. The conference version of H.R. 2883 received the approbation of both houses of Congress, and was forwarded to the President on December 18, 2001, for his signature. Signed by the President ten days later, it became P.L. 107-108.

"United States person" is defined in 50 U.S.C. § 1801(i) to mean a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 1101(a)(20) of Title 8), an

unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in subsection (a)(1), (2), or (3) of this section.

"Foreign power" is defined in 50 U.S.C. § 1801(a) to mean:
(1) a foreign government or any component thereof, whether or not recognized by the United States;
(2) a faction of a foreign nation or nations, not substantially composed of United States persons;
(3) an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments;
(4) a group engaged in international terrorism or activities in preparation therefor;
(5) a foreign-based political organization, not substantially composed of United States persons; or
(6) an entity that is directed and controlled by a foreign government or governments.

"Agent of a foreign power" is defined in 50 U.S.C. § 1801(b) to mean:
(1) any person other than a United States person, who —
(A) acts in the United States as an officer or employee of a foreign power, or as a member of a foreign power as defined in subsection (a)(4) of this section;
(B) acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of the United States, when the circumstances of such person's presence in the United States indicate that such person may engage in such activities in the United States, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities; or
(C) engages in international terrorism or activities in preparation therefore [sic]; or
(2) any person who —
(A) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States;
(B) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States;
(C) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, or on behalf of a foreign power; or
(D) knowingly enters the United States under a false or fraudulent identity for or on behalf of a foreign power or, while in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power; or
(E) knowingly aids or abets any person in the conduct of activities described in subparagraph (A), (B), or (C) or knowingly conspires with any person to engage in activities described in subparagraph (A), (B), or (C).
The italicized language in 50 U.S.C. § 1801(b)(1)(C) was added to the definition of "agent of a foreign power" in Section 6001 of the Intelligence Reform and Terrorism Prevention Act of 2004, P.L. 108-458. This provision would be "subject to the sunset provision in section 224 of the USA PATRIOT Act of 2001 (Public Law 107-56, 115 Stat. 295), including the exception provided in subsection (b) of such section 224." As amended by P.L. 109-177, Section 103, the sunset provision in Section 224 of P.L. 107-56, would take effect on December 31, 2009, except for any foreign intelligence investigation begun before that date or any criminal offense or potential offense that began or occurred before that date. For a more in depth discussion of this so-called "lone wolf" provision, see CRS Report RS22011, Intelligence Reform and Terrorism Prevention Act of 2004: "Lone Wolf" Amendment to the Foreign Intelligence Surveillance Act, by Elizabeth B. Bazan and Brian T. Yeh.

....

Second, in order for the President, through the Attorney General, to use this authority

> *... the Attorney General [must report] such minimization procedures and any changes thereto to the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence at least thirty days prior to their effective date, unless the Attorney General determines immediate action is required and notifies the committees immediately of such minimization and the reason for their becoming effective immediately.*

Such electronic surveillance must be conducted only in accordance with the Attorney General's certification and minimization procedures adopted by him. A copy of his certification must be transmitted by the Attorney General to the FISC. This certification remains under seal unless an application for a court order for surveillance authority is made under 50 U.S.C. §§ 1801(h)(4) and 1804,[3724] or the certification is necessary to determine the legality of the surveillance under 50 U.S.C. § 1806(f).[3725]

Several other provisions of Intelligence Reform and Terrorism Prevention Act also impacted FISA. Section 1011 of the measure amended Title I of the National Security Act of 1947, 50 U.S.C. § 402 et seq., to strike the previous Sections 102 through 104 of the Act 50 U.S.C. §§ 403, 403-1, 403-3, and 403-4, and insert new Sections 102 through 104A. The new Section 102 created the position of Director of National Intelligence (DNI). Section 102A outlined authorities and responsibilities of the position. Under the new Section 102A(f)(6) of the National Security Act, the DNI was given responsibility "to establish requirements and priorities for foreign intelligence information to be collected under [FISA], and provide assistance to the Attorney General to ensure that information derived from electronic surveillance or physical searches under that act is disseminated so that it may be used efficiently and effectively for foreign intelligence purposes, except that the Director shall have no authority to direct, manage, or undertake electronic surveillance or physical search operations pursuant to that act unless otherwise authorized by statute or Executive order." New Section 102A(f)(8) of the National Security Act, as enacted by P.L. 108-458, Section 1011, provided that, "Nothing in this act shall be construed as affecting the role of the Department of Justice or the Attorney General with respect to applications under the Foreign Intelligence Surveillance Act."

Section 1071(e) of P.L. 108-458, amended FISA to insert "Director of National Intelligence" in lieu of "Director of Central Intelligence" in each place in which it appeared.

Section 6002 created additional semiannual reporting requirements under FISA, which are codified at 50 U.S.C. § 1871. For a more detailed discussion of these reporting requirements, see fn. 165, infra, and accompanying text.

[3724] 50 U.S.C. § 1804 is discussed at pages 17-22 of this report, *infra*.

[3725] 50 U.S.C. § 1802(a)(2) and (a)(3). 50 U.S.C. § 1806 is discussed at fn. 68 and accompanying text, *infra*.

In connection with electronic surveillance so authorized, the Attorney General may direct a specified communications common carrier to furnish all information, facilities, or technical assistance needed for the electronic surveillance to be accomplished in a way that would protect its secrecy and minimize interference with the services provided by the carrier to its customers. 50 U.S.C. § 1802(a)(4)(A). In addition, the Attorney General may direct the specified communications common carrier to maintain any records, under security procedures approved by the Attorney General and the Director of National Intelligence, concerning the surveillance or the assistance provided which the carrier wishes to retain. 50 U.S.C. § 1802(a)(4)(B). Compensation at the prevailing rate must be made to the carrier by the Government for providing such aid.

If the President, by written authorization, empowers the Attorney General to approve applications to the FISC, an application for a court order may be made pursuant to 50 U.S.C. § 1802(b). A judge receiving such an application may grant an order under 50 U.S.C. § 1805 approving electronic surveillance of a foreign power or an agent of a foreign power to obtain foreign intelligence information. There is an exception to this, however. Under 50 U.S.C. § 1802(b), a court does not have jurisdiction to grant an order approving electronic surveillance directed solely as described in 50 U.S.C. § 1802(a)(1)(A) (that is, at acquisition of the contents of communications transmitted bymeans of communications used exclusively between or among foreign powers, or acquisition of technical intelligence, other than the spoken communications of individuals, from property or premises under the open and exclusive control of a foreign power), unless the surveillance may involve the acquisition of communications of a United States person. 50 U.S.C. § 1802(b).

50 U.S.C. § 1804 — Applications for FISC Orders Authorizing Electronic Surveillance.

An application for a court order authorizing electronic surveillance for foreign intelligence purposes may be sought under 50 U.S.C. § 1804. An application for such a court order must be made by a federal officer in writing on oath or affirmation to an FISC judge. The application must be approved by the Attorney General based upon his finding that the criteria and requirements set forth in 50 U.S.C. § 1801 et seq. have been met. Section 1804(a) sets out what must be included in the application:

(1) the identity of the Federal officer making the application;
(2) the authority conferred on the Attorney General by the President of the United States and the approval of the Attorney General to make the application;

(3) the identity, if known, or a description of the specific target of the electronic surveillance;[3726]
(4) a statement of the facts and circumstances relied upon by the applicant to justify his belief that —
(A) the target of the electronic surveillance is a foreign power or an agent of a foreign power; and
(B) each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power;
(5) a statement of the proposed minimization procedures;
(6) a detailed description of the nature of the information sought and the type of communications or activities to be subjected to the surveillance;
(7) a certification or certifications by the Assistant to the President for National Security Affairs or an executive branch official or officials designated by the President from among those executive officers employed in the area of national security or defense and appointed by the President with the advice and consent of the Senate[3727] —
(A) that the certifying official deems the information sought to be foreign intelligence information;
(B) that a significant[3728] purpose of the surveillance is to obtain foreign intelligence information;

[3726] Section 108(a)(1) of P.L. 109-177, added the word "specific" to this subsection.

[3727] Under Section 1-103 of Executive Order 12139, 55 Fed. Reg. 30,311 (May 23, 1979),as amended by Section 1 of E.O. 13383, 70 Fed. Reg. 41,933 (July 15, 2005), the Secretary of State, the Secretary of Defense, the Director of National Intelligence, the Director of the FBI, the Deputy Secretary of State, the Deputy Secretary of Defense, the Director of the Central Intelligence Agency, and the Principal Deputy Director of National Intelligence were designated to make such certifications in support of applications to engage in electronic surveillance for foreign intelligence purposes. Neither these officials nor anyone acting in those capacities may make such certifications unless they are appointed by the President with the advice and consent of the Senate.

[3728] Section 218 of P.L. 107-56 amended the requisite certifications to be made by the Assistant to the President for National Security Affairs, or other designated official (see footnote 25). Heretofore, the certifying official had to certify, among other things, that the purpose of the electronic surveillance under FISA was to obtain foreign intelligence information. Under the new language, the certifying official must certify that a significant purpose of such electronic surveillance is to obtain foreign intelligence information. As interpreted by the Court of Review in In re Sealed Case, 310 F.3d 717, 728-38 (U.S. Foreign Intell. Surveil. Ct. Rev. 2002), this language appears to exclude FISA as a vehicle for authorizing electronic surveillance where the sole purpose of an investigation is criminal prosecution. The government must have a measurable foreign intelligence purpose other than criminal prosecution, even of foreign intelligence crimes, in order to satisfy the "significant purpose" standard. The Court's analysis appears to suggest that the primary purpose of the investigation under FISA may be criminal prosecution, so long as collection of foreign intelligence information is also a significant purpose of the electronic surveillance. This issue was not addressed directly in the opinion of the U.S. Foreign Intelligence Surveillance Court in In re All Matters Submitted to the Foreign Intelligence Surveillance Court, 218 F. Supp. 2d 611(U.S. Foreign Intell. Surveil. Ct. 2002). *Id.*, at 615 n.2. Both opinions are

addressed later in this report in the section entitled "Published Decisions of the FISC and the U.S. Foreign Intelligence Surveillance Court of Review." Past cases considering the constitutional sufficiency of FISA in the context of electronic surveillance have rejected Fourth Amendment challenges and due process challenges under the Fifth Amendment to the use of information gleaned from a FISA electronic surveillance in a subsequent criminal prosecution, because the purpose of the FISA electronic surveillance, both initially and throughout the surveillance, was to secure foreign intelligence information and not primarily oriented towards criminal investigation or prosecution, United States v. Megahey, 553 F. Supp. 1180, 1185-1193 (D.N.Y.), aff'd 729 F.2d 1444 (2d Cir. 1982); United States v. Ott, 827 F.2d 473, 475 (9th Cir. 1987); United States. v Badia, 827 F. 2d 1458, 1464 (11th Cir. 1987). See also, United States v. Johnson, 952 F.2d 565, 572 (1st Cir. 1991), rehearing and cert. denied, 506 U.S. 816 (1991) (holding that, although evidence obtained in FISA electronic surveillance may later be used in a criminal prosecution, criminal investigation may not be the primary purpose of the surveillance, and FISA may not be used as an end-run around the 4th Amendment); United States v. Pelton, 835 F.2d 1067, 1074-76 (4th Cir. 1987), cert. denied, 486 U.S.1010 (1987) (holding that electronic surveillance under FISA passed constitutional muster where primary purpose of surveillance, initially and throughout surveillance, was gathering of foreign intelligence information; also held that an otherwise valid FISA surveillance was not invalidated because later use of the fruits of the surveillance in criminal prosecution could be anticipated. In addition, the court rejected Pelton's challenge to FISA on the ground that allowing any electronic surveillance on less than the traditional probable cause standard — i.e. probable cause to believe the suspect has committed, is committing, or is about to commit a crime for which electronic surveillance is permitted, and that the interception will obtain communications concerning that offense — for issuance of a search warrant was violative of the 4th Amendment, finding FISA's provisions to be reasonable both in relation to the legitimate need of Government for foreign intelligence information and the protected rights of U.S. citizens); United States v. Rahman, 861 F. Supp. 247, 251 (S.D. N.Y. 1994). Cf., United States v. Bin Laden, 2001 U.S. Dist. LEXIS 15484 (S.D. N.Y., October 2, 2001); United States v. Bin Laden, 126 F. Supp. 264, 277-78 (S.D. N.Y. 2000) (adopting foreign intelligence exception to the warrant requirement for searches targeting foreign powers or agents of foreign powers abroad; noting that this "exception to the warrant requirement applies until and unless the primary purpose of the searches stops being foreign intelligence collection.... If foreign intelligence collection is merely a purpose and not the primary purpose of a search, the exception does not apply.") Cf., United States v. Sarkissian, 841 F.2d 959, 964-65 (9th Cir. 1988) (FISA court order authorizing electronic surveillance, which resulted in the discovery of plan to bomb the Honorary Turkish Consulate in Philadelphia, and of the fact that bomb components were being transported by plane from Los Angeles. The FBI identified the likely airlines, flight plans, anticipated time of arrival, and suspected courier. Shortly before the arrival of one of those flights, the investigation focused upon an individual anticipated to be a passenger on a particular flight meeting all of the previously identified criteria. An undercover police officer spotted a man matching the suspected courier's description on that flight. The luggage from that flight was sniffed by a trained dog and x-rayed. A warrantless search was conducted of a suitcase that had been shown by x-ray to contain an unassembled bomb. Defendants unsuccessfully moved to suppress the evidence from the FISA wiretap and the warrantless search. On appeal the court upheld the warrantless suitcase search as supported by exigent circumstances. Defendants contended that the FBI's primary purpose for the surveillance had shifted at the time of the wiretap from an intelligence investigation to a criminal investigation and that court approval for the wiretap therefore should have been sought under Title III of the Omnibus Crime Control and Safe Streets Act, 18 U.S.C. § 2510 et seq., rather than FISA. The court, while noting that in other cases it had stated that "the purpose of [electronic] surveillance" under FISA "must be to secure foreign intelligence information", "not to ferret out criminal activity," declined to decide the issue of whether the standard under FISA required "the purpose" or "the primary purpose" of the surveillance to be gathering of foreign intelligence information. The court stated, "Regardless of whether the test is one of purpose or primary purpose, our review of the government's FISA materials convinces us that it is met in this case.... We refuse to draw too fine a distinction between criminal and

(C) that such information cannot reasonably be obtained by normal investigative techniques;
(D) that designates the type of foreign intelligence information being sought according to the categories described in 1801(e) of this title; and
(E) including a statement of the basis for the certification that —
(i) the information sought is the type of foreign intelligence information designated; and

---

intelligence investigations. "International terrorism ," by definition, requires the investigation of activities that constitute crimes. 50 U.S.C. § 1806(f). That the government may later choose to prosecute is irrelevant. FISA contemplates prosecution based on evidence gathered through surveillance. ... "Surveillances ... need not stop once conclusive evidence of a crime is obtained, but instead may be extended longer where protective measures other than arrest and prosecution are more appropriate." S. Rep. No. 701, 95th Cong., 1st Sess. 11 ....[(1978)]....FISA is meant to take into account "the differences between ordinary criminal investigations to gather evidence of specific crimes and foreign counterintelligence investigations to uncover and monitor clandestine activities ..." *Id.* .... At no point was this case an ordinary criminal investigation."). Cf., United States v. Falvey, 540 F. Supp. 1306 (E.D.N.Y. 1982) (distinguishing United States v. Truong Dinh Hung, 629 F.2d 908, 912-13 (4th Cir. 1980); and United States v. Butenko, 494 F.2d 593, 606 (3d Cir.) (en banc), cert. denied sub nom, Ivanov v. United States, 419 U.S. 881 (1974), which held that, while warrantless electronic surveillance for foreign intelligence purposes was permissible, when the purpose or primary purpose of the surveillance is to obtain evidence of criminal activity, evidence obtained by warrantless electronic surveillance is inadmissible at trial, 540 F. Supp. at 1313; on the theory that the evidence in the case before it was obtained pursuant to a warrant — a lawfully obtained court order under FISA, id. at 1314. The court noted that the "bottom line of Truong is that evidence derived from warrantless foreign intelligence searches will be admissible in a criminal proceeding only so long as the primary purpose of the surveillance is to obtain foreign intelligence information." *Id.* at 1313-14. After noting that Congress, in enacting FISA, "expected that evidence derived from FISA surveillances could then be used in a criminal proceeding," the court concluded that "it was proper for the FISA judge to issue the order in this case because of the on-going nature of the foreign intelligence investigation.... The fact that evidence of criminal activity was thereafter uncovered during the investigation does not render the evidence inadmissible. There is no question in [the court's] mind that the purpose of the surveillance, pursuant to the order, was the acquisition of foreign intelligence information. Accordingly, [the court found] that the FISA procedures on their face satisfy the Fourth Amendment warrant requirement, and that FISA was properly implemented in this case." *Id.* at 1314.). It is worthy of note that none of these decisions were handed down by the U.S. Foreign Intelligence Surveillance Court or the U.S. Foreign Intelligence Surveillance Court of Review. For a discussion of the recent decisions of those two courts regarding the Attorney General's 2002 minimization procedures, please see the discussion in the portion of this report regarding "Recent Decisions of the FISC and the U.S. Foreign Intelligence Surveillance Court of Review," infra. Nor do these decisions of the U.S. district courts and U.S. courts of appeal reflect recent legislative amendments to the FISA statute. However, the FISC, in its decision, did not address potential Fourth Amendment implications, and the U.S. Foreign Intelligence Court of Review, in its decision, appears to imply that some Fourth Amendment issues in the FISA context may be non-justiciable. Alternatively, the language in the Court of Review opinion might mean that the issue has not yet been considered by the courts. Using a balancing test it derived from Keith between foreign intelligence crimes and ordinary crimes, the Court of Review found surveillances under FISA, as amended by the USA PATRIOT Act, to be reasonable and therefore constitutional, while at the same time acknowledging that the constitutional question presented by the case before it — "whether Congress' disapproval of the primary purpose test is consistent with the Fourth Amendment — has no definitive jurisprudential answer." Court of Review op., 301 F.3d at 746.

(ii) such information cannot reasonably be obtained by normal investigative techniques;
(8) a statement of the means by which the surveillance will be effected and a statement whether physical entry is required to effect the surveillance;
(9) a statement of the facts concerning all previous applications that have been made to any judge under this subchapter involving any of the persons, facilities, or places specified in the application, and the action taken on each previous application;
(10) a statement of the period of time for which the electronic surveillance is required to be maintained, and if the nature of the intelligence gathering is such that the approval of the use of electronic surveillance under this subchapter should not automatically terminate when the described type of information has first been obtained, a description of facts supporting the belief that additional information of the same type will be obtained thereafter; and
(11) whenever more that one electronic, mechanical or other surveillance device is to be used with respect to a particular proposed electronic surveillance, the coverage of the devices involved and what minimization procedures apply to information acquired by each device. The application for a court order need not contain the information required in Subsections 1804(6), (7)(E), (8), and (11) above if the target of the electronic surveillance is a foreign power and each of the facilities or places at which surveillance is directed is owned, leased, or exclusively used by that foreign power. However, in those circumstances, the application must indicate whether physical entry is needed to effect the surveillance, and must also contain such information about the surveillance techniques and communications or other information regarding United States persons likely to be obtained as may be necessary to assess the proposed minimization procedures. 50 U.S.C. § 1804(b).

Where an application for electronic surveillance under 50 U.S.C. § 1804(a) involves a target described in 50 U.S.C. § 1801(b)(2),[3729] the Attorney General must personally review the application if requested to do so, in writing, by the Director of the Federal Bureau of Investigation, the Secretary of Defense, the Secretary of State, or the Director of National Intelligence.[3730] The authority to make such a request may not be delegated unless the official involved is disabled or otherwise unavailable.[3731] Each such official must make appropriate arrangements, in advance, to ensure that such a delegation of authority is clearly established in case of disability or other unavailability.[3732] If the Attorney General determines that an application should not be approved, he must give the official

---

[3729] For a list of those covered in 50 U.S.C. § 1801(b)(2), see fn. 44, supra.

[3730] 50 U.S.C. § 1804(e)(1)(A).

[3731] 50 U.S.C. § 1804(e)(1)(B).

[3732] 50 U.S.C. § 1804(e)(1)(C).

requesting the Attorney General's personal review of the application written notice of the determination. Except in cases where the Attorney General is disabled or otherwise unavailable, the responsibility for such a determination may not be delegated. The Attorney General must make advance plans to ensure that the delegation of such responsibility where the Attorney General is disabled or otherwise unavailable is clearly established.[3733] Notice of the Attorney General's determination that an application should not be approved must indicate what modifications, if any, should be made in the application needed to make it meet with the Attorney General's approval.[3734] The official receiving the Attorney General's notice of modifications which would make the application acceptable must modify the application if the official deems such modifications warranted. Except in cases of disability or other unavailability, the responsibility to supervise any such modifications is also a non-delegable responsibility.[3735]

50 U.S.C. § 1805 — Issuance of FISC Order Authorizing Electronic Surveillance.

If a judge makes the findings required under 50 U.S.C. § 1805(a), then he or she must enter an ex parte order as requested or as modified approving the electronic surveillance. The necessary findings must include that:

(1) the President has authorized the Attorney General to approve applications for electronic surveillance for foreign intelligence information;
(2) the application has been made by a Federal officer and approved by the Attorney General;
(3) on the basis of the facts submitted by the applicant there is probable cause to believe that —
(A) the target of the electronic surveillance is a foreign power or an agent of a foreign power: Provided, That no United States person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States; and
(B) each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power;
(4) the proposed minimization procedures meet the definition of minimization procedures under section 1801(h) of this title; and
(5) the application which has been filed contains all statements and certifications required by section 1804 of this title and, if the target is a United States person, the certification or certifications are not clearly erroneous on the basis of the statement made under section 1804(a)(7)(E) of this title and any other information furnished under section 1804(d) of this title. In making a probable

---

[3733] 50 U.S.C. § 1804(e)(2)(A).

[3734] 50 U.S.C. § 1804(e)(2)(B).

[3735] 50 U.S.C. § 1804(e)(2)(C).

cause determination under 50 U.S.C. § 1805(a)(3), the judge may consider past activities of the target as well as facts and circumstances relating to the target's current or future activities.[3736]

Section 1805(c) sets out particular specifications and directions which must be included in an order approving a FISA electronic surveillance:

(1) Specifications. — An order approving an electronic surveillance under this section shall specify
(A) the identity, if known, or a description of the specific target of the electronic surveillance identified or described in the application pursuant to [50 U.S.C. § 1804(a)(3)];
(B) the nature and location of each of the facilities or places at which the electronic surveillance will be directed, if known;[3737]
(C) the type of information sought to be acquired and the type of communications or activities to be subjected to the surveillance;
(D) the means by which the electronic surveillance will be effected and whether physical entry will be used to effect the surveillance;
(E) the period of time during which the electronic surveillance is approved; and
(F) whenever more than one electronic, mechanical, or other surveillance device is to be used under the order, the authorized coverage of the device involved and what minimization procedures shall apply to information subject to acquisition by each device.
(2) Directions. — An order approving an electronic surveillance under this section shall direct
(A) that the minimization procedures be followed;
(B) that, upon the request of the applicant a specified communication or other common carrier, landlord, custodian, or other specified person, *or in circumstances where the Court finds, based upon specific facts provided in the application, that the actions of the target of the application may have the effect of thwarting the identification of a specified person*, such other persons, furnish the applicant forthwith all information, facilities, or technical assistance necessary to accomplish the electronic surveillance in such a manner as will protect its secrecy and produce a minimum of interference with the services that such carrier, landlord, custodian, or other person is providing that target of electronic surveillance;
(C) that such carrier, landlord, custodian, or other person maintain under security procedures approved by the Attorney General and the Director of

---

[3736] 50 U.S.C. § 1805(b).

[3737] Section 314(a)(2)(A) of H.Rept. 107-328, the conference report on the Intelligence Authorization Act for Fiscal Year 2002, to accompany H.R. 2883, added "if known" to the end of Section 1805(c)(1)(B) before the semi-colon. The conference version of the bill passed both the House and the Senate, and was signed by the President on December 28, 2001, as P.L. 107-108.

National Intelligence any records concerning the surveillance or the aid furnished that such person wishes to retain; and
(D) that the applicant compensate, at the prevailing rate, such carrier, landlord, custodian, or other person for furnishing such aid.[3738]
(3) Special directions for certain orders
An order approving an electronic surveillance under this section in circumstances where the nature and location of each of the facilities or places at which the surveillance will be directed is unknown shall direct the applicant to provide notice to the court within ten days after the date on which surveillance begins to be directed at any new facility or place, unless the court finds good cause to justify a longer period of up to 60 days, of —
(A) the nature and location of each new facility or place at which the electronic surveillance is directed;
(B) the facts and circumstances relied upon by the applicant to justify the applicant's belief that each new facility or place at which the electronic surveillance is directed is or was being used, or is about to be used, by the target of the surveillance;
(C) a statement of any proposed minimization procedures that differ from those contained in the original application or order, that may be necessitated by a change in the facility or place at which the electronic surveillance is directed; and
(D) the total number of electronic surveillances that have been or are being conducted under the authority of the order.

The italicized portions of Section 1805(c)(1)(B) and Section 1805(c)(2)(B) reflect changes, added by P.L. 107-108 and P.L. 107-56 respectively, intended to provide authority for "multipoint" or "roving" electronic surveillance where the actions of the target of the surveillance, such as switching phones and locations repeatedly, may thwart that surveillance. The Conference Report on H.R. 2338, the Intelligence Authorization Act for Fiscal Year 2002 (which became P.L. 107-108), H.Rept. 107-328, at page 24, provided the following explanation of these changes:

> *The multipoint wiretap amendment to FISA in the USA PATRIOT Act (section 206) allows the FISA court to issue generic orders of assistance to any communications provider or similar person, instead of to a particular communications provider. This change*

[3738] 50 U.S.C. § 1805(c). The italics in 50 U.S.C. § 1805(c)(2)(B), above, indicate new language added by Section 206 of P.L. 107-56. Where circumstances suggest that a target's actions may prevent identification of a specified person, this new language appears to permit the Foreign Intelligence Surveillance Court to require a service provider, other common carrier, landlord, custodian or other persons to provide necessary assistance to the applicant for a FISA order for electronic surveillance. The heading to Section 6 of P.L. 107-56 refers to this as "roving surveillance authority." H.Rept. 107-328 calls this a "multipoint" wiretap. Intelligence Authorization Act for Fiscal Year 2002, 107th Cong., 1st Sess., H.Rept. 107-328, Conference Report, at 24 (Dec. 6, 2001).

permits the Government to implement new surveillance immediately if the FISA target changes providers in an effort to thwart surveillance. The amendment was directed at persons who, for example, attempt to defeat surveillance by changing wireless telephone providers or using pay phones.

Currently, FISA requires the court to "specify" the "nature and location of each of the facilities or places at which the electronic surveillance will be directed." 50 U.S.C. § 105(c)(1)(B). Obviously, in certain situations under current law, such a specification is limited. For example, a wireless phone has no fixed location and electronic mail may be accessed from any number of locations.

To avoid any ambiguity and clarify Congress' intent, the conferees agreed to a provision which adds the phrase, "if known," to the end of 50 U.S.C. § 1805(c)(1)(B). The "if known" language, which follows the model of 50 U.S.C. § 1805(c)(1)(A), is designed to avoid any uncertainty about the kind of specification required in a multipoint wiretap case, where the facility to be monitored is typically not known in advance.

The underlined portions of subsection 1805(c) reflect changes made by P.L. 109-177, Section 108.

If the target of the electronic surveillance is a foreign power and each of the facilities or places at which the surveillance is directed is owned, leased, or exclusively used by that foreign power, the order does not need to include the information covered by Section 1805(c)(1)(C), (D), and (F), but must generally describe the information sought, the communications or activities subject to surveillance, the type of electronic surveillance used, and whether physical entry is needed. 50 U.S.C. § 1805(d).

Such an order may approve an electronic surveillance for the period of time necessary to achieve its purpose or for ninety days, whichever is less, unless the order is targeted against a foreign power as defined in 50 U.S.C. § 1801(a)(1), (2), or (3),[3739] or against an agent of a foreign power who is not a United States person. In the case of an order targeted against a such a foreign power, the order shall approve an electronic surveillance for the period specified in the order or for one year, whichever is less. An order under FISA for surveillance targeted against

---

[3739] A "foreign power" as defined in 50 U.S.C. § 1801(a)(1), (2), or (3) includes "a foreign government or any component thereof, whether or not recognized by the United States;" "a faction of a foreign nation or nations, not substantially composed of United States persons;" or "an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments."

an agent of a foreign power who is not a U.S. person may be for the period specified in the order or 120 days, whichever is less.[3740]

Generally, upon application for an extension, a court may grant an extension of an order on the same basis as an original order. An extension must include new findings made in the same manner as that required for the original order. However, an extension of an order for a surveillance targeted against a foreign power as defined in 50 U.S.C. § 1801(a)(5) (a foreign-based political organization, not substantially composed of United States persons) or (6) (an entity that is directed and controlled by a foreign government or governments), or against a foreign power as defined in 50 U.S.C. § 1801(a)(4) (a group engaged in international terrorism or activities in preparation therefor) that is not a United States person, may be for a period of up to one year if the judge finds probable cause to believe that no communication of any individual United States person will be acquired during the period involved. In addition, an extension of an order for surveillance targeted at an agent of a foreign power who is not a U.S. person may be extended to a period not exceeding one year.[3741]

Certifications made by the Attorney General pursuant to 50 U.S.C. § 1802(a) and applications made and orders granted for electronic surveillance under title I of FISA, must be retained for a period of at least ten years from the date of the certification or application.[3742]

Emergency Authorization of Electronic Surveillance upon Attorney General Certification while an FISC Order Is Pursued.

Emergency situations are addressed in 50 U.S.C. § 1805(f). Notwithstanding other provisions of this subchapter, if the Attorney General reasonably determines that an emergency situation exists with respect to the employment of electronic surveillance to obtain foreign intelligence information before an order authorizing such surveillance can with due diligence be obtained and that the factual basis for issuance of an order under this subchapter to approve such surveillance exists, he may authorize electronic surveillance if specified steps are taken. At the time of the Attorney General's emergency authorization, he or his designee must inform an FISC judge that the decision to employ emergency

---

[3740] 50 U.S.C. § 1805(e)(1)(B), as added by Section 207 of P.L. 107-56, and amended by Section 105 of P.L. 109-177.

[3741] 50 U.S.C. § 1805(e)(2)(A) and (B). Section 207 of P.L. 107-56 appears to have included a mistaken citation here, referring to 50 U.S.C. § 1805(d)(2) instead of 50 U.S.C. § 1805(e)(2) (emphasis added). Section 314(c)(1) of P.L. 107-108 corrected the apparent error from P.L. 107-56, Section 207, so that the reference is now to 50 U.S.C. § 1805(e)(2). Subsection 105(e)(2)(B) of FISA, 50 U.S.C. § 1805(e)(2)(B), was amended by Section 105 of P.L. 109-177.

[3742] 50 U.S.C. § 1805(h).

electronic surveillance has been made. An application for a court order under Section 1804 must be made to that judge as soon as practicable, but not more than 72 hours after the Attorney General authorizes such surveillance. If the Attorney General authorizes emergency electronic surveillance, he must require compliance with the minimization procedures required for the issuance of a judicial order under this subchapter. Absent a judicial order approving the emergency electronic surveillance, the surveillance must terminate when the information sought is obtained, when the application for the order is denied, or after 72 hours from the time of the Attorney General's authorization, whichever is earliest.[3743] If no judicial order approving the surveillance is issued, the information garnered may not be received in evidence or otherwise disclosed in any court proceeding, or proceeding in or before any grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof. No information concerning any United States person acquired through such surveillance may be disclosed by any Federal officer or employee without the consent of that person, unless the Attorney General approves of such disclosure or use where the information indicates a threat of death or serious bodily harm to any person.[3744]

[3743] Section 314(a)(2)(B) of P.L. 107-108, the Intelligence Authorization Act for Fiscal Year 2002, H.Rept. 107-328, replaced 24 hours with 72 hours in each place that it appears in 50 U.S.C. § 1805(f).

[3744] Some of the provisions dealing with interception of wire, oral, or electronic communications in the context of criminal law investigations, 18 U.S.C. §§ 2510 et seq., may also be worthy of note. With certain exceptions, these provisions, among other things, prohibit any person from engaging in intentional interception; attempted interception; or procuring others to intercept or endeavor to intercept wire, oral, or electronic communication; or intentional disclosure; attempting to disclose; using or endeavoring to use the contents of a wire, oral or electronic communication, knowing or having reason to know that the information was obtained by such an unlawful interception. 18 U.S.C. § 2511. "Person" is defined in 18 U.S.C. § 2510(6) to include "any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation." Among the exceptions to Section 2511 are two of particular note: (2)(e) Notwithstanding any other provision of this title or section 705 or 706 of the Communications Act of 1934, it shall not be unlawful for an officer, employee, or agent of the United States in the normal course of his official duty to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, as authorized by that Act.

(2)(f) Nothing contained in this chapter or chapter 121, or section 705 of the Communications Act of 1934, shall be deemed to affect the acquisition by the United States Government of foreign intelligence information from international or foreign communications, or foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic communications system, utilizing a means other than electronic surveillance as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, and procedures in this chapter and the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which electronic surveillance, as defined in section 101 of such Act, and the interception of domestic wire and oral communications may be conducted.

Among other things, Section 2512 prohibits any person from intentionally manufacturing, assembling, possessing, or selling any electronic, mechanical, or other device, knowing that its

design renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications and that such device or any component thereof has been or will be sent through the mail or transported in interstate or foreign commerce. It also prohibits any person from intentionally sending such a device through the mail or sending or carrying such a device in interstate or foreign commerce, knowing that such surreptitious interception is its primary purpose. Similarly, intentionally advertising such a device, knowing or having reason to know that the advertisement will be sent through the mail or transported in interstate or foreign commerce is foreclosed. Again an exception to these general prohibitions in Section 2512 may be of particular interest:

(2) It shall not be unlawful under this section for —
(a) ...
(b) an officer, agent, or employee of, or a person under contract with, the United States ... in the normal course of the activities of the United States ..., to send through the mail, send or carry in interstate or foreign commerce, or manufacture, assemble, possess, or sell any electronic, mechanical, or other device knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications.

In addition, Section 107 of the Electronic Communications Privacy Act of 1986, P.L. 99-508, 100 Stat. 1858, October 21, 1986, [which enacted 18 U.S.C. §§ 1367, 2621, 2701 to 2711, 3117, and 3121 to 3126; and amended 18 U.S.C. §§ 2232, 2511-2513, and 25162520], provided generally that, "[n]othing in this act or the amendments made by this act constitutes authority for the conduct of any intelligence activity." It also stated:

(b) Certain Activities Under Procedures Approved by the Attorney General. — Nothing in chapter 119 [interception of wire, oral or electronic communications] or chapter 121 [stored wire and electronic communications and transactional records access] of title 18, United States Code, shall affect the conduct, by officers or employees of the United States Government in accordance with other applicable Federal law, under procedures approved by the Attorney General of activities intended to —
(1) intercept encrypted or other official communications of United States executive branch entities or United States Government contractors for communications security purposes;
(2) intercept radio communications transmitted between or among foreign powers or agents of a foreign power as defined by the Foreign Intelligence Surveillance Act of 1978 [50 U.S.C. § 1801 et seq.]; or
(3) access an electronic communication system used exclusively by a foreign power or agent of a foreign power as defined by the Foreign Intelligence Surveillance Act of 1978 [50 U.S.C. § 1801 et seq.].

In addition, Chapter 121 of title 18 of the United States Code deals with stored wire and electronic communications and transactional records. Under 18 U.S.C. § 2701, intentionally accessing without authorization a facility through which an electronic communication service is provided, or intentionally exceeding an authorization to access such a facility and thereby obtaining, altering, or preventing authorized access to a wire or electronic communication while it is in electronic storage in such system is prohibited. Upon compliance with statutory requirements in 18 U.S.C. § 2709, the Director of the FBI or his designee in a position not lower than Deputy Assistant Director may seek access to telephone toll and transactional records for foreign counterintelligence purposes. The FBI may disseminate information and records obtained under this section only as provided in guidelines approved by the Attorney General for foreign intelligence collection and foreign counterintelligence investigations conducted by the FBI, and, "with respect to dissemination to an agency of the United States, only if such information is clearly relevant to the authorized responsibilities of such agency." 18 U.S.C. § 2709(d).

50 U.S.C. § 1805(g) — Authority for Electronic Surveillance for Testing of Electronic Equipment; Discovering Unauthorized Electronic Surveillance; or Training of Intelligence Personnel in Use of Electronic Equipment.

Notwithstanding any other provision of title I of FISA, under Section 1805(g), federal officers, employees, or agents are authorized in the normal course of their official duties to conduct electronic surveillance not targeted against the communications of any particular person or persons, under procedures approved by the Attorney General, solely to:

(1) test the capability of electronic equipment, if —
(A) it is not reasonable to obtain the consent of the persons incidentally subjected to the surveillance;
(B) the test is limited in extent and duration to that necessary to determine the capability of the equipment;
(C) the contents of any communication acquired are retained and used only for the purpose of determining the capability of the equipment, are disclosed only to test personnel, and are destroyed before or immediately upon completion of the test; and:
(D) Provided, That the test may exceed ninety days only with the prior approval of the Attorney General;
(2) determine the existence and capability of electronic surveillance equipment being used by persons not authorized to conduct electronic surveillance, if —
(A) it is not reasonable to obtain the consent of persons incidentally subjected to the surveillance;
(B) such electronic surveillance is limited in extent and duration to that necessary to determine the existence and capability of such equipment; and
(C) any information acquired by such surveillance is used only to enforce chapter 119 of Title 18, or section 605 of Title 47, or to protect information from unauthorized surveillance; or
(3) train intelligence personnel in the use of electronic surveillance equipment, if —
(A) it is not reasonable to —
(i) obtain the consent of the persons incidentally subjected to the surveillance;
(ii) train persons in the course of surveillances otherwise authorized by this subchapter; or
(iii) train persons in the use of such equipment without engaging in electronic surveillance;
(B) such electronic surveillance is limited in extent and duration to that necessary to train the personnel in the use of the equipment; and
(C) no contents of any communication acquired are retained or disseminated for any purpose, but are destroyed as soon as reasonably possible.

50 U.S.C. § 1805(i) — Limitation on Liability for Compliance with FISC Order Authorizing Electronic Surveillance or Physical Search.

Section 1805(i) bars any cause of action in any court against any provider of a wire or electronic communication service, landlord, custodian, or other person (including any officer, employee, agent, or other specified person thereof) that furnishes any information, facilities, or technical assistance in accordance with a court order or request for emergency assistance under FISA for electronic surveillance or a physical search.[3745]

50 U.S.C. § 1806 — Use of Information Obtained from FISA Electronic Surveillance.

The uses to which information gathered pursuant to electronic surveillance under FISA may be put are addressed under 50 U.S.C. § 1806.[3746]

[3745] Section 225 of P.L. 107-56 appeared to create a second subsection 1805(h), which precluded any cause of action in any court "against any provider of a wire or electronic communication service, landlord, custodian, or other person (including any officer, employee, agent, or other specified person thereof) that furnishes any information, facilities, or technical assistance in accordance with a court order or request for emergency assistance" under FISA. This immunity provision was included in 50 U.S.C. § 1805, and was denominated "Immunity for Compliance with FISA Wiretap" in Section 225 of the USA PATRIOT Act, both facts which might lead one to conclude that it applied only to electronic surveillance under FISA, but this does not appear to be the view of expressed in H.Rept. 107-328, the conference report accompanying H.R. 2883, which became P.L. 107-108. P.L. 107-108 redesignated 50 U.S.C. § 1805(h) as 50 U.S.C. § 1805(i). In H.Rept. 107-328, the conferees expressed the view that "the text of section 225 refers to court orders and requests for emergency assistance 'under this act,' which makes clear that it applies to physical searches (and pen-trap requests — for which there already exists an immunity provision, 50 U.S.C. § 1842(f) — and subpoenas) as well as electronic surveillance." *Id.* at 25. Section 314(a)(2)(C) of P.L. 107-108 changed subsection (h), which was added to 50 U.S.C. § 1805 by Section 225 of P.L. 107-56, to subsection (i). In addition, Section 314(a)(2)(D) of P.L. 107-108 added "for electronic surveillance or physical search" to the end of the newly designated 50 U.S.C. § 1805(i) before the final period.

[3746] The provisions of Section 1806 are as follows:

(a) Compliance with minimization procedures; privileged communications; lawful purposes

Information acquired from an electronic surveillance conducted pursuant to this subchapter concerning any United States person may be used and disclosed by Federal officers and employees without the consent of the United States person only in accordance with the minimization procedures required by this subchapter. No otherwise privileged communication obtained in accordance with or in violation of this subchapter shall lose its privileged character. No information acquired from an electronic surveillance pursuant to this subchapter may be used or disclosed by Federal officers or employees except for lawful purposes.

(b) Statement for disclosure

No information acquired pursuant to this subchapter shall be disclosed for law enforcement purposes unless such disclosure is accompanied by a statement that such information, or any information derived therefrom, may only be used in a criminal proceeding with the advance authorization of the Attorney General.

(c)

Notification by United States

Whenever the Government intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, against an aggrieved person, any information obtained or derived from an electronic surveillance of that aggrieved person pursuant to the authority of this subchapter, the Government shall, prior to the trial, hearing, or other proceeding or at a reasonable time prior to an effort to so disclose or so use that information or submit it in evidence, notify the aggrieved person and the court or other authority in which the information is to be disclosed or used that the Government intends to so disclose or so use such information.

(d) Notification by States or political subdivisions
Whenever any State or political subdivision thereof intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of a State or a political subdivision thereof, against an aggrieved person any information obtained or derived from an electronic surveillance of that aggrieved person pursuant to the authority of this subchapter, the State or political subdivision thereof shall notify the aggrieved person, the court or other authority in which the information is to be disclosed or used, and the Attorney General that the State or political subdivision thereof intends to so disclose or so use such information.

(e) Motion to suppress
Any person against whom evidence obtained or derived from an electronic surveillance to which he is an aggrieved person is to be, or has been, introduced or otherwise used or disclosed in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, may move to suppress the evidence obtained or derived from such electronic surveillance on the grounds that —
(1) the information was unlawfully acquired; or
(2) the surveillance was not made in conformity with an order of authorization or approval. Such a motion shall be made before the trial, hearing, or other proceeding unless there was no opportunity to make such a motion or the person was not aware of the grounds of the motion.

(f) In camera and ex parte review by district court
Whenever a court or other authority is notified pursuant to subsection (c) or (d) of this section, or whenever a motion is made pursuant to subsection (e) of this section, or whenever any motion or request is made by an aggrieved person pursuant to any other statute or rule of the United States or any State before any court or other authority of the United States or any State to discover or obtain applications or orders or other materials relating to electronic surveillance or to discover, obtain, or suppress evidence or information obtained or derived from electronic surveillance under this chapter, the United States district court or, where the motion is made before another authority, the United States district court in the same district as the authority, shall, notwithstanding any other law, if the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States, review in camera and ex parte the application, order, and such other materials relating to the surveillance as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted. In making this determination, the court may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance only where such disclosure is necessary to make an accurate determination of the legality of the surveillance.

(g) Suppression of evidence; denial of motion
If the United States district court pursuant to subsection (f) of this section determines that the surveillance was not lawfully authorized or conducted, it shall, in accordance with the requirements of law, suppress the evidence which was unlawfully obtained or derived from electronic surveillance of the aggrieved person or otherwise grant the motion of the aggrieved

person. If the court determines that the surveillance was lawfully authorized and conducted, it shall deny the motion of the aggrieved person except to the extent that due process requires discovery or disclosure.

(h) Finality of orders
Orders granting motions or requests under subsection (g) of this section, decisions under this section that electronic surveillance was not lawfully authorized or conducted, and orders of the United States district court requiring review or granting disclosure of applications, orders, or other materials relating to a surveillance shall be final orders and binding upon all courts of the United States and the several States except a United States court of appeals and the Supreme Court.

(i) Destruction of unintentionally acquired information
In circumstances involving the unintentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States, unless the Attorney General determines that the contents indicate a threat of death or serious bodily harm to any person.

(j) Notification of emergency employment of electronic surveillance; contents; postponement, suspension or elimination
If an emergency employment of electronic surveillance is authorized under section 1805(e) of this title and a subsequent order approving the surveillance is not obtained, the judge shall cause to be served on any United States person named in the application or on such other United States persons subject to electronic surveillance as the judge may determine in his discretion it is in the interest of justice to serve, notice of —
(1) the fact of the application;
(2) the period of the surveillance; and
(3) the fact that during the period information was or was not obtained.

On an ex parte showing of good cause to the judge the serving of the notice required by this subsection may be postponed or suspended for a period not to exceed ninety days. Thereafter, on a further ex parte showing of good cause, the court shall forgo ordering the serving of the notice required under this subsection.

(k) Consultation with Federal law enforcement officer
(1) Federal officers who conduct electronic surveillance to acquire foreign intelligence information under this title may consult with Federal law enforcement officers or law enforcement personnel of a State or political subdivision of a State (including the chief executive officer of that State or political subdivision who has the authority to appoint or direct the chief law enforcement officer of that State or political subdivision) to coordinate efforts to investigate or protect against —

(A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
(B) sabotage or international terrorism by a foreign power or an agent of a foreign power; or
(C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power.

(2) Coordination authorized under paragraph (1) shall not preclude the certification required by section 104(a)(7)(B) [50 U.S.C. § 1804(a)(7)(B) (referring to a certification by the Assistant to the President for National Security Affairs or other designated certifying authority "that a significant purpose of the surveillance is to obtain foreign intelligence information")] or the entry of an order

Under this section, disclosure, without the consent of the person involved, of information lawfully acquired under FISA electronic surveillance which concerns a United States person must be in compliance with the statutorily mandated minimization procedures. Communications which were privileged when intercepted remain privileged. Where information acquired under FISA electronic surveillance is disclosed for law enforcement purposes, neither that information nor any information derived therefrom may be used in a criminal proceeding without prior authorization of the Attorney General. If the United States Government intends to disclose information acquired under FISA electronic surveillance or derived therefrom in any proceeding before a court, department, officer regulatory body or other authority of the United States against an aggrieved person,[3747] then the Government must give prior notice of its intent to disclose to the aggrieved person and to the court or other authority involved. Similarly, a State or political subdivision of a State that intends to disclose such information against an aggrieved person in a proceeding before a State or local authority must give prior notice of its intent to the aggrieved person, the court or other authority, and the Attorney General.[3748]

---

under section 105 [50 U.S.C. § 1805]. (Emphasis added.) Subsection 1806(k) was added by Section 504 of P.L. 107-56. The italicized portion of subsection 1806(k)(1), above, was added by Section 898 of the Homeland Security Act of 2002, P.L. 107-296. The term "aggrieved person," as used in connection with electronic surveillance under FISA, is defined under 50 U.S.C. § 1801(k) to mean "a person who is the target of an electronic surveillance or any other person whose communications or activities were subject to electronic surveillance."

[3747] For the definition of "aggrieved person" as that term is used with respect to targets of electronic surveillance under FISA, see fn. 42, *supra*.

[3748] It is worthy of note that Section 892 of the Homeland Security Act of 2002, P.L. 107-296, while not expressly amending FISA, addressed procedures for the sharing of homeland security information. It required the President to prescribe and implement procedures under which relevant federal agencies, including those in the intelligence community, would share relevant and appropriate homeland security information with other federal agencies and, where appropriate, with State and local personnel. Section 892 provided, in part:

Sec. 892. Facilitating Homeland Security Information Sharing Procedures.

(a) Procedures for Determining Extent of Sharing of Homeland Security Information. —

(1) The President shall prescribe and implement procedures under which relevant Federal agencies —

(A) share relevant and appropriate homeland security information with other Federal agencies, including the Department, and appropriate State and local personnel;

(B) identify and safeguard homeland security information that is sensitive but unclassified; and

(C) to the extent that such information is in classified form, determine whether, how, and to what extent to remove classified information, as appropriate, and with which such personnel it may be shared after such information is removed.

(2) The President shall ensure that such procedures apply to all agencies of the Federal Government.

(3) Such procedures shall not change the substantive requirements for the classification and safeguarding of classified information.

(4) Such procedures shall not change the requirements and authorities to protect sources and methods.

(b) Procedures for Sharing of Homeland Security Information. —

50 U.S.C. § 1806(c)-(f) — U.S. District Court Consideration of Notices, Motions to Suppress or Discovery Motions.

(1) Under procedures prescribed by the President, all appropriate agencies, including the intelligence community, shall, through information sharing systems, share homeland security information with Federal agencies and appropriate State and local personnel to the extent such information may be shared, as determined in accordance with subsection
(a), together with assessments of the credibility of such information.
(2) Each information sharing system through which information is shared under paragraph (1) shall —
(A) have the capability to transmit unclassified or classified information, though the procedures and recipients for each capability may differ;
(B) have the capability to restrict delivery of information to specified subgroups by geographic location, type of organization, position of a recipient within an organization, or a recipient's need to know such information;
(C) be configured to allow the efficient and effective sharing of information; and
(D) be accessible to appropriate State and local personnel.
(3) The procedures prescribed in paragraph (1) shall establish conditions on the use of information shared under paragraph (1) —
(A) to limit the redissemination of such information to ensure that such information is not used for an unauthorized purpose;
(B) to ensure the security and confidentiality of such information;
(C) to protect the constitutional and statutory rights of any individuals who are subjects of such information; and
(D) to provide data integrity through the timely removal and destruction of obsolete or erroneous names and information.
(4) ....
(5) Each appropriate Federal agency, as determined by the President, shall have access to each information sharing system through which information is shared under paragraph (1), and shall therefore have access to all information, as appropriate, shared under such paragraph.
(6) The procedures prescribed under paragraph (1) shall ensure that appropriate State and local personnel are authorized to use such information systems —
(A) to access information shared with such personnel; and
(B) to share, with others who have access to such information sharing systems, the homeland security information of their own jurisdictions, which shall be marked appropriately as pertaining to potential terrorist activity.
(7) Under procedures prescribed jointly by the Director of National Intelligence and the Attorney General, each appropriate Federal agency, as determined by the President, shall review and assess the information shared under paragraph (6) and integrate such information with existing intelligence. ....

Subsection (f)(1) of Section 892 of P.L. 107-296, defined "homeland security information" to mean "information possessed by a Federal, State, or local agency" that "relates to the threat of terrorist activity;" "relates to the ability to prevent, interdict, or disrupt terrorist activity;" "would improve the identification or investigation of a suspected terrorist or terrorist organization;" "or would improve the response to a terrorist act." "State and local personnel" is defined to mean persons involved in prevention, preparation, or response for terrorist attack who fall within the following categories: "State Governors, mayors, and other locally elected officials;" "State and local law enforcement personnel and firefighters;" "public health and medical professionals;" "regional, State, and local emergency management agency personnel, including State adjutant generals;" "other appropriate emergency response agency personnel;" and "employees of private-sector entities that affect critical infrastructure, cyber, economic, or public health security, as designated by the Federal Government in procedures developed pursuant to this section."

Section 1806 also sets out in camera and ex parte U.S. district court review procedures to be followed where such notification is received, or where the aggrieved person seeks to discover or obtain orders or applications relating to FISA electronic surveillance, or to discover, obtain, or suppress evidence or information obtained or derived from the electronic surveillance, and the Attorney General files an affidavit under oath that such disclosure would harm U.S. national security. The focus of this review would be to determine whether the surveillance was lawfully conducted and authorized. Only where it is needed to make an accurate determination of these issues does the section permit the court to disclose to the aggrieved person, under appropriate security measures and protective orders, parts of the application, order, or other materials related to the surveillance. If, as a result of its review, the district court determines that the surveillance was unlawful, the resulting evidence must be suppressed.[3749] If the surveillance was lawfully authorized and conducted, the motion of the aggrieved person must be denied except to the extent that due process requires discovery or disclosure. Resultant court orders granting motions or requests of the aggrieved person for a determination that the surveillance was not lawfully conducted or authorized and court orders requiring review or granting disclosure are final orders binding on all Federal and State courts except a U.S. Court of Appeals and the U.S. Supreme Court.

[3749] *But see*, United States v. Thomson, 752 F. Supp. 75, 77 (W.D. N.Y. 1990), stating that,

If the Court determines that the surveillance was unlawfully authorized or conducted, it must order disclosure of the FISA material. 50 U.S.C. § 1806(g) .... In United States v. Belfield, 692 F.2d 141 (D.C. Cir. 1982), the court stated that "even when the government has purported not to be offering any evidence obtained or derived from the electronic surveillance, a criminal defendant may claim that he has been the victim of an illegal surveillance and seek discovery of the FISA surveillance material to ensure that no fruits thereof are being used against him." *Id.* at 146.

It may be noted that the Section 1806(g) does not state that a court must order disclosure of the FISA material if the court finds that the FISA electronic surveillance was unlawfully authorized or conducted. Rather, the provision in question states in pertinent part that, "If the United States district court pursuant to subsection (f) of this section determines that the surveillance was not lawfully authorized or conducted, it shall, in accordance with the requirements of law, suppress the evidence which was unlawfully obtained or derived from electronic surveillance of the aggrieved person or otherwise grant the motion of the aggrieved person...." While a district court will normally consider in camera and ex parte a motion to suppress under Subsection 1806(e) or other statute or rule to discover, disclose, or suppress information relating to a FISA electronic surveillance, Subsection 1806(f) does permit a district court, in determining the legality of a FISA electronic surveillance, to disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order or other materials relating to the surveillance only to the extent necessary to make an accurate determination of the legality of the surveillance. Belfield indicated that a criminal defendant may seek to discover FISA surveillance material to ensure that no fruits of an illegal surveillance are being used against him, but it appears to stop short of saying that in every instance where the court finds an illegal surveillance disclosure must be forthcoming. "The language of section 1806(f) clearly anticipates that an ex parte, in camera determination is to be the rule. Disclosure and an adversary hearing are the exception, occurring only when necessary." Belfield, supra, 692 F.2d at 147. See also, United States v. Squillacote, 221 F.3d 542, 552554 (4th Cir. 2000), cert. denied, 532 U.S. 971 (2001).

If the contents of any radio communication are unintentionally acquired by an electronic, mechanical, or other surveillance device in circumstances where there is a reasonable expectation of privacy and where a warrant would be required if the surveillance were to be pursued for law enforcement purposes, then the contents must be destroyed when recognized, unless the Attorney General finds that the contents indicate a threat of death or serious bodily harm to any person.

As noted above, Section 1805 provides for emergency electronic surveillance in limited circumstances, and requires the subsequent prompt filing of an application for court authorization to the FISC in such a situation. Under Section 1806, if the application is unsuccessful in obtaining court approval for the surveillance, notice must be served upon any United States person named in the application and such other U.S. persons subject to electronic surveillance as the judge determines, in the exercise of his discretion, is in the interests of justice. This notice includes the fact of the application, the period of surveillance, and the fact that information was or was not obtained during this period. Section 1806 permits postponement or suspension of service of notice for up to ninety days upon ex parte good cause shown. Upon a further ex parte showing of good cause thereafter, the court will forego ordering such service of notice.

50 U.S.C. § 1806(k) — Consultation by Federal Officers Conducting FISA Electronic Surveillance with Federal Law Enforcement Officers.

P.L. 107-56, Section 504, added a new subsection 1806(k)(1). Under this subsection, federal officers who conduct electronic surveillance to acquire foreign intelligence under FISA are permitted to consult with Federal law enforcement officers to coordinate investigative efforts or to protect against —

(A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
(B) sabotage or international terrorism by a foreign power or an agent of a foreign power; or
(C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power.

This subsection indicates further that such coordination would not preclude certification as required by 50 U.S.C. § 1804(a)(7)(B) or entry of a court order under 50 U.S.C. § 1805.

50 U.S.C. §§ 1807 and 1808 — Congressional Oversight.

Reporting requirements are included in Sections 1807 and 1808. Under Section 1807, each year in April, the Attorney General is directed to transmit to the Administrative Office of the United States Courts and to the Congress a report covering the total number of applications made for orders and extensions of orders approving electronic surveillance under FISA during the previous year,

and the total number of orders and extensions granted, modified, or denied during that time period.

Section 1808(a) requires the Attorney General to fully inform the House Permanent Select Committee on Intelligence, the Senate Select Committee on Intelligence, and the Senate Judiciary Committee semiannually about all electronic surveillance under FISA.[3750] Each such report must contain a description of the total number of applications made for orders and extensions of orders approving electronic surveillance under this subchapter where the nature and location of each facility or place at which the electronic surveillance will be directed is unknown; each criminal case in which information acquired by electronic surveillance under FISA has been authorized for use at trial during the period covered by the report; and the total number of emergency employments of electronic surveillance under section 1805(f) of this title and the total number of subsequent orders approving or denying such electronic surveillance.[3751]

50 U.S.C. § 1809 — Criminal Sanctions.

Section 1809 provides criminal sanctions for intentionally engaging in electronic surveillance under color of law except as authorized by statute; or for disclosing or using information obtained under color of law by electronic surveillance, knowing or having reason to know that surveillance was not authorized by statute. The provision makes it a defense to prosecution under this subsection if the defendant is a law enforcement officer or investigative officer in the course of his official duties and the electronic surveillance was authorized by and conducted under a search warrant or court order of a court of competent jurisdiction. Section 1809 provides for Federal jurisdiction over such an offense if the defendant is a Federal officer or employee at the time of the offense.

50 U.S.C. § 1810 — Civil Liability.

Civil liability is also provided for under Section 1810, where an aggrieved person, who is neither a foreign power nor an agent of a foreign power, has been subjected to electronic surveillance, or where information gathered by electronic

---

[3750] 50 U.S.C. § 1808(a)(1), as amended by P.L. 109-177, Section 108(c)(1). Subsection 1808(b) directed the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence to report annually for five years after the date of enactment to the House and the Senate respectively concerning implementation of FISA, including any recommendations for amendment, repeal, or continuation without amendment. P.L. 106567, Title VI, Sec. 604(b) (Dec. 27, 2000), 114 Stat. 2853, required the Attorney General to submit to the Senate Select Committee on Intelligence, the Senate Judiciary Committee, the House Permanent Select Committee on Intelligence, and the House Judiciary Committee a report on the authorities and procedures utilized by the Department of Justice to determine whether or not to disclose information acquired under FISA for law enforcement purposes. 50 U.S.C. § 1806 note.

[3751] 50 U.S.C. § 1808(a)(2), as amended by P.L. 109-177, Section 108(c)(2).

surveillance about an aggrieved person has been disclosed or used in violation of Section 1809.

50 U.S.C. § 1811 — Electronic Surveillance without FISC Order after Congressional Declaration of War.

Finally, Section 1811 provides that, notwithstanding any other law, the President, through the Attorney General, may authorize electronic surveillance without a court order to acquire foreign intelligence information for up to 15 calendar days following a declaration of war by Congress.

Physical searches for foreign intelligence gathering purposes.

Physical searches for foreign intelligence purposes are addressed in 50 U.S.C. § 1821 *et seq*.[3752] While tailored for physical searches, the provisions in many respects follow a pattern similar to that created for electronic surveillance. The definitions from 50 U.S.C. § 1801 for the terms "foreign power," "agent of a foreign power," "international terrorism," "sabotage," "foreign intelligence information," "Attorney General," "United States person," "United States," "person," and "State" also apply to foreign intelligence physical searches except where specifically provided otherwise.

Minimization procedures also apply to physical searches for foreign intelligence purposes. Those defined under 50 U.S.C. § 1821(4) are tailored to such physical searches and, like those applicable to electronic surveillance under 50 U.S.C. § 1801(h), these procedures are designed to minimize acquisition and retention, and to prohibit dissemination, of nonpublicly available information concerning unconsenting U.S. persons, consistent with the needs of the United States to obtain, produce and disseminate foreign intelligence.[3753]

[3752] The physical search provisions of FISA were added as Title III of that Act by P.L. 103359, Title VIII, on October 14, 1994, 108 Stat. 3443. Some of these provisions were subsequently amended by P.L. 106-567, Title VI, on December 27, 2000, 114 Stat. 2852-53; and by P.L. 107-56.

[3753] Specifically, 50 U.S.C. § 1821(4) defines "minimization procedures" with respect to physical search to mean:

(A) specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purposes and technique of the particular physical search, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information;

(B) procedures that require that nonpublicly available information, which is not foreign intelligence information, as defined in section 1801(e)(1) of this title, shall not be disseminated in a manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to understand such foreign intelligence information or assess its importance;

(C) notwithstanding subparagraphs (A) and (B), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes; and

50 U.S.C. § 1822 — Physical Searches without FISC Order of Premises Owned or Controlled by Certain Foreign Powers.

Under 50 U.S.C. § 1822, the President, acting through the Attorney General, may authorize physical searches to acquire foreign intelligence information without a court order for up to one year if the Attorney General certifies under oath that the search is solely directed at premises, property, information or materials owned by or under the open and exclusive control of certain foreign power or powers.[3754] For these purposes, "foreign power or powers" means a foreign government or component of a foreign government, whether or not recognized by the United States, a faction of a foreign nation or nations, not substantially composed of U.S. persons; or an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments.[3755] In addition, the Attorney General must certify that there is no substantial likelihood that the physical search will involve the premises, information, material or property of a U.S. person, and that the proposed minimization procedures with respect to the physical search are consistent with 50 U.S.C. § 1821(4)(1)-(4).[3756] Under normal circumstances, these minimization procedures and any changes to them are reported to the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence by the Attorney General at least 30 days before their effective date. However, if the Attorney General determines that immediate action is required, the statute mandates that he advise these committees immediately of the minimization procedures and the need for them to become effective immediately. In addition, the Attorney General must assess compliance with these minimization procedures and report such assessments to these congressional committees.

(D) notwithstanding subparagraphs (A), (B), and (C), with respect to any physical search approved pursuant to section 1822(a) of this title, procedures that require that no information, material, or property of a United States person shall be disclosed, disseminated, or used for any purpose or retained for longer than 72 hours, unless a court order under section 1824 of this title is obtained or unless the Attorney General determines that the information indicates a threat of death or serious bodily harm to any person.

Section 314(a)(3) of P.L. 107-108, the Intelligence Authorization Act of 2002, changed the previous 24 hour period in the minimization procedures under 50 U.S.C. § 1821(4)(D) to a 72 hour period.

[3754] The President provided such authority to the Attorney General by Executive Order 12949, Section 1, 60 Fed. Reg. 8169 (February 9, 1995), if the Attorney General makes the certifications necessary under 50 U.S.C. § 1822(a)(1).

[3755] See 50 U.S.C. § 1801(a)(1), (2), or (3).

[3756] While this is the citation cross-referenced in Section 1822, it appears that the cross-reference should read 50 U.S.C. § 1821(4)(A)-(D).

The certification of the Attorney General for a search under 50 U.S.C. § 1822 is immediately transmitted under seal to the Foreign Intelligence Surveillance Court, and maintained there under security measures established by the Chief Justice of the United States with the Attorney General's concurrence, in consultation with the Director of National Intelligence. Such a certification remains under seal unless one of two circumstances arise: (1) either an application for a court order with respect to the physical search is made to the Foreign Intelligence Surveillance Court under 50 U.S.C. § 1821(4) (dealing with minimization procedures) and § 1823 (dealing with the process by which a federal officer, with the approval of the Attorney General, may apply for an order from the FISC approving a physical search for foreign intelligence gathering purposes); or (2) the certification is needed to determine the legality of a physical search under 50 U.S.C. § 1825 (dealing with use of the information so gathered).

In connection with physical searches under 50 U.S.C. § 1822, the Attorney General may direct a landlord, custodian or other specified person to furnish all necessary assistance needed to accomplish the physical search in a way that would both protect its secrecy and minimize interference with the services such person provides the target of the search. Such person may also be directed to maintain any records regarding the search or the aid provided under security procedures approved by the Attorney General and the Director of National Intelligence. The provision of any such aid must be compensated by the Government.[3757]

As in the case of applications for electronic surveillance under FISA, the Foreign Intelligence Surveillance Court (FISC) has jurisdiction to hear applications and grant applications with respect to physical searches under 50 U.S.C. § 1821 et seq. No FISC judge may hear an application already denied by another FISC judge. If an application for an order authorizing a physical search under FISA is denied, the judge denying the application must immediately provide a written statement of reasons for the denial. If the United States so moves, the record is then transmitted under seal to the court of review established under 50 U.S.C. § 1803(b). If the court of review determines that the application was properly denied, it, in turn, must provide a written statement of the reasons for its decision, which must be transmitted under seal to the Supreme Court upon petition for certiorari by the United States.[3758] Any of the proceedings with respect to an application for a physical search under FISA must be conducted expeditiously, and the record of such proceedings must be kept under appropriate security measures.

50 U.S.C. § 1823 — Application for an FISC Order Authorizing a Physical Search.

[3757] 50 U.S.C. § 1822(a)(4).

[3758] 50 U.S.C. § 1822(c), (d).

The requirements for application for an order for a physical search under FISA are included in 50 U.S.C. § 1823. While tailored to a physical search, the requirements strongly parallel those applicable to electronic surveillance under 50 U.S.C. § 1804(a)(1)-(9).[3759] Like Section 1804(a)(7)(B) with respect to required certifications for an application for electronic surveillance under FISA, Section 1823(a)(7)(B) was amended by P.L. 107-56, Section 218, to require that the

---

[3759] Each application for an order approving such a physical search, having been approved by the Attorney General based upon his understanding that the application satisfies the criteria and requirements of 50 U.S.C. § 1821 et seq., must be made by a Federal officer in writing upon oath or affirmation to an FISC judge. Under subsection (a) of Section 1823, the application must include:
(1) the identity of the Federal officer making the application;
(2) the authority conferred on the Attorney General by the President and the approval of the Attorney General to make the application;
(3) the identity, if known, or a description of the search, and a detailed description of the premises or property to be searched and of the information, material, or property to be seized, reproduced, or altered;
(4) a statement of the facts and circumstances relied upon by the applicant to justify the applicant's belief that —
(A) the target of the physical search is a foreign power or an agent of a foreign power;
(B) the premises or property to be searched contains foreign intelligence information; and
(C) the premises or property to be searched is owned, used, possessed by, or is in transit to or from a foreign power or an agent of a foreign power;
(5) a statement of the proposed minimization procedures;
(6) a statement of the nature of the foreign intelligence sought and the manner in which the physical search is to be conducted;
(7) a certification or certifications by the Assistant to the President for National Security Affairs or an executive branch official or officials designated by the President from among those executive branch officers employed in the area of national security or defense and appointed by the President, by and with the advice and consent of the Senate —
(A) that the certifying official deems the information sought to be foreign intelligence information;
(B) that a significant purpose of the search is to obtain foreign intelligence information;
(C) that such information cannot reasonably be obtained by normal investigative techniques; 80 (...continued)
(D) that designates the type of foreign intelligence information being sought according to the categories described in section 1801(e) of this title; and
(E) includes a statement explaining the basis for the certifications required by subparagraphs (C) and (D);
(8) where the physical search involves a search of the residence of a United States person, the Attorney General shall state what investigative techniques have previously been utilized to obtain the foreign intelligence information concerned and the degree to which these techniques resulted in acquiring such information; and

(9) a statement of the facts concerning all previous applications that have been made to any judge under this subchapter involving any of the persons, premises, or property specified in the application, and the action taken on each previous application. (Emphasis added.) Under Section 1823(b), the Attorney General may require any other affidavit or certification from any other officer in connection with an application for a physical search that he deems appropriate. Under Section 1823(c), the FISC judge to whom the application is submitted may also require that the applicant provide other information as needed to make the determinations necessary under 50 U.S.C. § 1824.

Assistant to the President for National Security Affairs or designated Executive Branch official[3760] certify, among other things, that a significant purpose (rather than "that the purpose") of the physical search is to obtain foreign intelligence information.[3761] Section 1823(d) also parallels Section 1804(e) (dealing with requirements for some applications for electronic surveillance under FISA), in that, if requested in writing by the Director of the FBI, the Secretary of Defense, the Secretary of State, or the Director of National Intelligence,[3762] the Attorney General must personally review an application for a FISA physical search if the target is one described by Section 1801(b)(2). 50 U.S.C. § 1801(b)(2) deals with targets who knowingly engage in clandestine intelligence gathering activities involving or possibly involving violations of federal criminal laws by or on behalf of a foreign power; targets who, at the direction of an intelligence service or network of a foreign power, engage in other clandestine intelligence activities involving or potentially involving federal crimes by or on behalf of a foreign power; targets who knowingly engage in sabotage or international terrorism, activities in preparation for sabotage or international terrorism, or activities on behalf of a foreign power; targets who knowingly aid, abet, or conspire with anyone to engage in any of the previously listed categories of activities; or targets who knowingly enter the United States under false identification by or on behalf

---

[3760] In Section 2 of E.O. 12949, 60 Fed. Reg. 8169 (February 9, 1995), as amended by Section 2 of E.O. 13383, 70 Fed. Reg. 41,933 (July 15, 2005), the President authorized the Attorney General to approve applications to the Foreign Intelligence Surveillance Court under 50 U.S.C. § 1823, to obtain court orders for physical searches for the purpose of collecting foreign intelligence information. In Section 3 of that executive order, the President designated the Secretary of State, the Secretary of Defense, the Director of National Intelligence, the Director of the Federal Bureau of Investigation, the Deputy Secretary of State, the Deputy Secretary of Defense, the Director of the Central Intelligence Agency, and the Principal Deputy Director of National Intelligence to make the certifications required by 50 U.S.C. § 1823(a)(7), in support of an application for a court order for a physical search for foreign intelligence purposes. None of these officials may exercise this authority to make the appropriate certifications unless he or she is appointed by the President, with the advice and consent of the Senate.

[3761] Section 303(a)(7)(B) of FISA, 50 U.S.C. § 1823(a)(7)(B) (see italicized language in the quote of the statutory section in fn. 57, supra). Extrapolating from the U.S. Foreign Intelligence Surveillance Court of Review's interpretation of the "significant purpose" language as applied to electronic surveillance under FISA in In re Sealed Case, 310 F.3d 717, 728-38 (U.S. Foreign Intell. Surveil. Ct. Rev. 2002), this language appears to exclude FISA as authority for a physical search where the sole purpose of an investigation is criminal prosecution. The government must have a measurable foreign intelligence purpose other than criminal prosecution, even of foreign intelligence crimes, in order to satisfy the "significant purpose" standard. This reasoning suggests that the primary purpose of the investigation may be criminal prosecution, so long as collection of foreign intelligence information is also a significant purpose of the search.

[3762] The authority of these officials to make such a written request is non-delegable except where such official is disabled or unavailable. Each must make provision in advance for delegation of this authority should he or she become disabled or unavailable. 50 U.S.C. § 1823(d)(1)(B) and (C).

or a foreign power or who assume a false identity on behalf of a foreign power while present in the United States.[3763]

Should the Attorney General, after reviewing an application, decide not to approve it, he must provide written notice of his determination to the official requesting the review of the application, setting forth any modifications needed for the Attorney General to approve it. The official so notified must supervise the making of the suggested modifications if the official deems them warranted. Unless the Attorney General or the official involved is disabled or otherwise unable to carry out his or her respective responsibilities under Section 1823, those responsibilities are non-delegable.

50 U.S.C. § 1824 — Issuance of an FISC Order Authorizing a Physical Search.

As in the case of the issuance of an order approving electronic surveillance under 50 U.S.C. § 1805(a), certain findings by the FISC judge are required before an order may be forthcoming authorizing a physical search for foreign intelligence information under 50 U.S.C. § 1824(a). Once an application under Section 1823 has been filed, an FISC judge must enter an ex parte order, either as requested or as modified, approving the physical search if the requisite findings are made. These include findings that:

(1) the President has authorized the Attorney General to approve applications for physical searches for foreign intelligence purposes;
(2) the application has been made by a Federal officer and approved by the Attorney General;
(3) on the basis of the facts submitted by the applicant there is probable cause to believe that —
(A) the target of the physical search is a foreign power or an agent of a foreign power, except that no United States person may be considered an agent of a foreign power solely on the basis of activities protected by the first amendment to the Constitution of the United States; and
(B) the premises or property to be searched is owned, used, possessed by, or is in transit to or from an agent of a foreign power or a foreign power;
(4) the proposed minimization procedures meet the definition of minimization contained in this subchapter; and
(5) the application which has been filed contains all statements and certifications required by section 1823 of this title, and, if the target is a United States person, the certification or certifications are not clearly erroneous on the basis of the statement made under section 1823(a)(7)(E) of this title and any other information furnished under section 1823(c) of this title.

[3763] *See* fn. 44, *supra*.

Like Section 1805(b) regarding electronic surveillance under FISA, an FISC judge making a probable cause determination under Section 1824 may consider the target's past activities, plus facts and circumstances pertinent to the target's present or future activities.[3764]

As in the case of an order under 50 U.S.C. § 1805(c) with respect to electronic surveillance, an order granting an application for a physical search under FISA must meet statutory requirements in 50 U.S.C. § 1824(c) as to specifications and directions. An order approving a physical search must specify:

(A) the identity, if known, or a description of the target of the physical search;
(B) the nature and location of each of the premises of property to be searched;
(C) the type of information, material, or property to be seized, altered, or reproduced;
(D) a statement of the manner in which the physical search is to be conducted and, whenever more than one physical search is authorized under the order, the authorized scope of each search and what minimization procedures shall apply to the information acquired by each search; and
(E) the period of time during which the physical searches are approved; ....
In addition, the order must direct:
(A) that the minimization procedures be followed;
(B) that, upon the request of the applicant, a specified landlord, custodian, or other specified person furnish the applicant forthwith all information, facilities, or assistance necessary to accomplish the physical search in such a manner as will protect its secrecy and produce a minimum of interference with the services that such landlord, custodian, or other person is providing to the target of the physical search;
(C) that such landlord, custodian, or other person maintain under security procedures approved by the Attorney General and the Director of National

Intelligence[3765] any records concerning the search or the aid furnished that such person wishes to retain;

(D) that the applicant compensate, at the prevailing rate, such landlord, custodian, or other person for furnishing such aid; and
(E) that the federal officer conducting the physical search promptly report to the court the circumstances and results of the physical search.[3766] Subsection 1824(d)

[3764] 50 U.S.C. § 1824(b).

[3765] Section 1071(e) replaced "Director of Central Intelligence" with "Director of National Intelligence" in each place where it appeared in FISA. This was one of those locations.

[3766] 50 U.S.C. § 1824(c)(1), (2).

sets the limits on the duration of orders under this section and makes provision for extensions of such orders if certain criteria are met.[3767]

50 U.S.C. § 1824(e) — Emergency Authorization of a Physical Search upon Attorney General Certification while FISC Order Is Pursued.

Subsection 1824(e) deals with emergency orders for physical searches. It permits the Attorney General, under certain circumstances, to authorize execution of a physical search if the Attorney General or his designee informs an FISC judge that the decision to execute an emergency search has been made, and an application under 50 U.S.C. § 1821 et seq. is made to that judge as soon as possible, within 72 hours[3768] after the Attorney General authorizes the search. The Attorney General's decision to authorize such a search must be premised upon a determination that "an emergency situation exists with respect to the execution of a physical search to obtain foreign intelligence information before an

---

[3767] P.L. 107-56, Section 207(a)(2), amended 50 U.S.C. § 1824(d)(1) so that it provided:
(1) An order under this section may approve a physical search for the period necessary to achieve its purpose, or for 90 days, whichever is less, except that (A) an order under this section shall approve a physical search targeted against a foreign power, as defined in paragraph (1), (2), or (3) of section 101(a) [50 U.S.C. § 1801(b)(1)(A)], for the period specified in the application or for one year, whichever is less, and (B) an order under this section for a physical search against an agent of a foreign power as defined in section 101(b)(1)(A) [50 U.S.C. § 1801(b)(1)(A)] may be for the period specified in the application or for 120 days, whichever is less. The language in italics reflects the changes made by P.L. 107-56. The 90 day time period reflected in the first sentence replaced earlier language which provided for 45 days.

Section 207(b)(2) of P.L. 107-56 amended 50 U.S.C. § 1824(d)(2) to provide:
(2) Extensions of an order issued under this title [50 U.S.C. §§ 1821 et seq.] may be granted on the same basis as the original order upon an application for an extension and new findings made in the same manner as required for the original order, except that an extension of an order under this Act for a physical search targeted against a foreign power, as defined in section 101(a)(5) or (6) [50 U.S.C. § 1801(a)(5) or (6)], or against a foreign power, as defined in section 101(a)(4) [50 U.S.C. § 1801(a)(4)] , that is not a United States person, or against an agent of a foreign power as defined in section 101(b)(1)(A) [50 U.S.C. § 1801(b)(1)(A)], may be for a period not to exceed one year if the judge finds probable cause to believe that no property of any individual United States person will be acquired during the period. (Emphasis added.) Section 105(b) of P.L. 109-177, amended subsection 1824(d)(2) to replace "as defined in section 101(b)(1)(A)," with "who is not a United States person." Thus, as amended, provides in pertinent part that an extension of a FISA order for a physical search targeted against an agent of a foreign power who is not a United States person may be for a period not to exceed one year if the judge finds probable cause to believe that no property of any individual United States person will be acquired during the period.

Under subsection 1824(d)(3), the judge, at or before the end of the time approved for a physical search or for an extension, or at any time after the physical search is carried out, may review circumstances under which information regarding U.S. persons was acquired, retained, or disseminated to assess compliance with minimization techniques.

[3768] Section 314(a)(4) of the Intelligence Authorization Act for Fiscal Year 2002, P.L. 107108, amended 50 U.S.C. § 1824(e) by striking "24 hours" where it occurred and replacing it with "72 hours."

order authorizing such search can with due diligence be obtained," and "the factual basis for issuance of an order under this title [50 U.S.C. § 1821 et seq.] to approve such a search exists."[3769] If such an emergency search is authorized by the Attorney General, he must require that the minimization procedures required forissuance of a judicial order for a physical search under 18 U.S.C. § 1821 et seq. be followed.[3770] If there is no judicial order for a such a physical search, then the search must terminate on the earliest of the date on which the information sought is obtained, the date on which the application for the order is denied, or the expiration of the 72 hour period from the Attorney General's authorization of the emergency search.[3771] If an application for approval is denied or if the search is terminated and no order approving the search is issued, then neither information obtained from the search nor evidence derived from the search may be used in evidence or disclosed in any

> *... trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof, and no information concerning any United States person acquired from such search shall subsequently be used or disclosed in any other manner by Federal officers or employees without the consent of such person, except with the approval of the Attorney General, if the information indicates a threat of death or serious bodily harm to any person. A denial of the application made under this subsection may be reviewed as provided in section 302 [50 U.S.C. § 1822].*[3772]

Subsection 1824(f) requires retention of applications made and orders granted under 50 U.S.C. § 1821 *et seq*., for a minimum of ten years from the date of the application.

<u>50 U.S.C. § 1825 — Use of Information Obtained from a FISA Physical Search.</u>

Like 50 U.S.C. § 1806 with respect to electronic surveillance under FISA, 50 U.S.C. § 1825 restricts and regulates the uses of information secured under a FISA physical search. Such information may only be used or disclosed by Federal officers or employees for lawful purposes. Federal officers and employees must comply with minimization procedures if they use or disclose information

---

[3769] 50 U.S.C. § 1824(e)(1)(A)(i) and (ii). See fn. 89, supra, regarding substitution of "72 hours" for "24 hours" in Subsection 50 U.S.C. § 1824(e)(3)(C) by P.L. 107-108, Sec. 314(a)(4).

[3770] 50 U.S.C. § 1824(e)(2).

[3771] 50 U.S.C. § 1824(e)(3).

[3772] 50 U.S.C. § 1824(e)(4).

gathered from a physical search under FISA concerning a United States person.[3773] If a physical search involving the residence of a United States person is authorized and conducted under 50 U.S.C. § 1824, and at any time thereafter the Attorney General determines that there is no national security interest in continuing to maintain the search's secrecy, the Attorney General must provide notice to the United States person whose residence was searched. This notice must include both the fact that the search pursuant to FISA was conducted and the identification of any property of that person which was seized, altered, or reproduced during the search.[3774] Disclosure for law enforcement purposes of information acquired under 50 U.S.C. § 1821 et seq., must be accompanied by a statement that such information and any derivative information may only be used in a criminal proceeding with advance authorization from the Attorney General.[3775]

The notice requirements relevant to intended use or disclosure of information gleaned from a FISA physical search or derivative information, are similar to those applicable where disclosure or use of information garnered from electronic surveillance is intended. If the United States intends to use or disclose information gathered during or derived from a FISA physical search in a trial, hearing, or other proceeding before a court, department, officer, agency, regulatory body or other authority of the United States against an aggrieved person, the United States must first give notice to the aggrieved person, and the court or other authority.[3776] Similarly, if a State or political subdivision of a state intends to use or disclose any information obtained or derived from a FISA physical search in any trial, hearing, or other proceeding before a court, department, officer, agency, regulatory body, or other State or political subdivision against an aggrieved person, the State or locality must notify the aggrieved person, the pertinent court or other authority where the information is to be used, and the Attorney General of the United States of its intention to use or disclose the information.[3777]

<u>50 U.S.C. §§ 1825(d)-(g) — U.S. District Court Consideration of Notices, Motions to Suppress, or Discovery Motions.</u>

[3773] 50 U.S.C. § 1825(a).

[3774] 50 U.S.C. § 1825(b).

[3775] 50 U.S.C. § 1825(c).

[3776] 50 U.S.C. § 1825(d). "Aggrieved person," as defined in 50 U.S.C. § 1821(2), "means a person whose premises, property, information, or material is the target of a physical search or any other person whose premises, property, information, or material was subject to physical search."

[3777] 50 U.S.C. § 1825(e).

An aggrieved person may move to suppress evidence obtained or derived from a FISA physical search on one of two grounds: that the information was unlawfully acquired; or that the physical search was not made in conformity with an order of authorization or approval. Such a motion to suppress must be made before the trial, hearing or other proceeding involved unless the aggrieved person had no opportunity to make the motion or was not aware of the grounds of the motion.[3778]

In camera, ex parte review by a United States district court may be triggered by receipt of notice under Subsections 1825(d) or (e) by a court or other authority; the making of a motion to suppress by an aggrieved person under Subsection 1825(f); or the making of a motion or request by an aggrieved person under any other federal or state law or rule before any federal or state court or authority to discover or obtain applications, orders, or other materials pertaining to a physical search authorized under FISA or to discover, obtain, or suppress evidence or information obtained or derived from a FISA physical search. If the Attorney General files an affidavit under oath that disclosure of any adversary hearing would harm U.S. national security, the U.S. district court receiving notice or before whom a motion or request is pending, or, if the motion is made to another authority, the U.S. district court in the same district as that authority, shall review in camera and ex parte the application, order, and such other materials relating to the physical search at issue needed to determine whether the physical search of the aggrieved person was lawfully authorized and conducted. If the court finds it necessary to make an accurate determination of the legality of the search, the court may disclose portions of the application, order, or other pertinent materials to the aggrieved person under appropriate security procedures and protective orders, or may require the Attorney General to provide a summary of such materials to the aggrieved person.[3779]

If the U.S. district court makes a determination that the physical search was not lawfully authorized or conducted, then it must "suppress the evidence which was unlawfully obtained or derived from the physical search of the aggrieved person or otherwise grant the motion of the aggrieved person." If, on the other hand, the court finds that the physical search was lawfully authorized or conducted, the motion of the aggrieved person will be denied except to the extent that due process requires discovery or disclosure.[3780]

If the U.S. district court grants a motion to suppress under 50 U.S.C. § 1825(h); deems a FISA physical search unlawfully authorized or conducted; or orders review or grants disclosure of applications, orders or other materials pertinent to

---

[3778] 50 U.S.C. § 1825(f).

[3779] 50 U.S.C. § 1825(g).

[3780] 50 U.S.C. § 1825(h).

a FISA physical search, that court order is final and binding on all federal and state courts except a U.S. Court of Appeals or the U.S. Supreme Court.[3781]

As a general matter, where an emergency physical search is authorized under 50 U.S.C. § 1824(d), and a subsequent order approving the resulting search is not obtained, any U.S. person named in the application and any other U.S. persons subject to the search that the FISC judge deems appropriate in the interests of justice must be served with notice of the fact of the application and the period of the search, and must be advised as to whether information was or was not obtained during that period.[3782] However, such notice may be postponed or suspended for a period not to exceed 90 days upon an ex parte showing of good cause to the judge, and, upon further good cause shown, the court must forego such notice altogether.[3783]

50 U.S.C. § 1825(k) — Consultation by Federal Officers Doing FISA Searches with Federal Law Enforcement Officers.

Section 504(b) of P.L. 10756, added a new 50 U.S.C. § 1825(k) to the statute, which deals with consultation by federal officers doing FISA searches with federal law enforcement officers. Section 899 of the Homeland Security Act of 2002, P.L. 107-296 expanded this authority to also permit consultation with "law enforcement personnel of a State or political subdivision of a State (including the chief executive officer of that State or political subdivision who has the authority to appoint or direct the chief law enforcement officer of that State or political subdivision)." Under this new language, as amended, federal officers "who conduct physical searches to acquire foreign intelligence information" under 50 U.S.C. § 1821 et seq., may consult with federal law enforcement officers or state or local law enforcement personnel:

> *... to coordinate efforts to investigate or protect against*
> *(A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;*
> *(B) sabotage or international terrorism by a foreign power or an agent of a foreign power; or*
> *(C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power.*[3784]

[3781] 50 U.S.C. § 1825(i).

[3782] 50 U.S.C. § 1825(j)(1).

[3783] 50 U.S.C. § 1825(j)(2).

[3784] 50 U.S.C. § 1825(k)(1).

Such coordination does not preclude certification required under 50 U.S.C. § 1823(a)(7) or entry of an order under 50 U.S.C. § 1824.[3785]

50 U.S.C. § 1826 — Congressional Oversight.

50 U.S.C. § 1826 provides for semiannual congressional oversight of physical searches under FISA.[3786] The Attorney General is directed to "fully inform" the Permanent Select Committee on Intelligence of the House of Representatives, the Select Committee on Intelligence of the Senate, and the Senate Judiciary Committee[3787] with respect to all physical searches conducted under 50 U.S.C. § 1821 *et seq*. Also on a semiannual basis, the Attorney General is required to provide a report to "those committees" and to the House Judiciary Committee[3788]

[3785] 50 U.S.C. § 1825(k)(2).

[3786] See also the discussion of new reporting requirements added by Section 6002 of P.L. 108-458, the Intelligence Reform and Terrorism Prevention Act of 2004, 50 U.S.C. § 1871, discussed at fn. 165, infra, and accompanying text.

[3787] P.L. 109-177, Section 109(a) added the Senate Judiciary Committee to the committees to be fully informed by the Attorney General as to FISA physical searches.

[3788] The term "those committees" in the second sentence of 50 U.S.C. § 1826 appears to be subject to at three possible interpretations. Section 109(a)(1) of P.L. 109-177 amends the first sentence of Section 1826 "in the first sentence, by inserting ", and the Committee on the Judiciary of the Senate," after "Senate." The amending language in Subsection 109(a)(2) or P.L. 109-177, amends 50 U.S.C. § 1826 "in the second sentence, by striking "and the Committees on the Judiciary of the House of Representatives and the Senate" and inserting "and the Committee on the Judiciary of the House of Representatives." In light of this sequence of amendments, the phrase "those committees" in the second paragraph might to refer to the Intelligence Committees alone, rather than to the Intelligence Committees and the Senate Judiciary Committee referred to in the previous sentence. If this is the case, then the semiannual report referred to in this sentence would be submitted only to the Intelligence Committees and the House Judiciary Committee. Under this view, the replacement of "and the Committees on the Judiciary of the House of Representatives and the Senate" with "and the Committee on the Judiciary of the House of Representatives" would reflect an intent to eliminate access to the report for the Senate Judiciary Committee, while leaving the access of the House Judiciary Committee extant. Alternatively, if "those committees" refers to all three committees listed in the first sentence, then replacing a reference to both Senate and House Judiciary Committees with a reference only to the House Judiciary Committee would eliminate a redundancy in the language, while giving both Intelligence Committees and both Judiciary Committees access to the report. The Conference Report to P.L. 109-177, H.Rept. 109-333, USA PATRIOT Improvement and Reauthorization Act of 2005, 109th Cong., 1st Sess. 93 (December 8, 2005), appears to give the provision a third reading which does include both House and Senate Judiciary Committees as recipients of the report on emergency employment of physical searches under FISA, as well as electronic surveillance and pen registers, but makes no mention of the Intelligence Committees. It states:
Section 109. Enhanced congressional oversight
Section 109 of the conference report is similar to section 10 of the Senate amendment, bu with an additional new provision. Section 109 of the conference report is identical to section 10 of the Senate amendment and requires: (1) the FISA court to publish its rules; and (2) reporting to the House and Senate Judiciary Committees of the use of the emergency employments of electronic surveillance, physical searches, and pen register and trap and trace devices. Section 109(c) of the

setting forth: the total number of applications for orders approving FISA physical searches during the preceding six month period; the total number of those orders granted, modified, or denied; the number of such physical searches involving the residences, offices, or personal property of United States persons; the number of occasions, if any, the Attorney General gave notice under 50 U.S.C. § 1825(b);[3789] and the total number of emergency physical searches authorized by the Attorney General under section 1824(e) of this title and the total number of subsequent orders approving or denying such physical searches.[3790]

50 U.S.C. § 1827 — Criminal Sanctions.

Section 1827 imposes criminal sanctions for intentionally executing a physical search for foreign intelligence gathering purposes under color of law within the United States except as authorized by statute. In addition, criminal penalties attach to a conviction for intentionally disclosing or using information obtained by a physical search under color of law within the United States for the purpose of gathering intelligence information, where the offender knows or has reason to know that the information was obtained by a physical search not authorized by statute. In either case, this section provides that a person convicted of such an offense faces a fine of not more than $10,000,[3791] imprisonment for not more

---

conference report also requires that the Secretary of the Department of Homeland Security submit a written report providing a description of internal affairs operations at U.S. Citizenship & Immigration Services to the Judiciary Committees of the House and the Senate.

The language of 50 U.S.C. § 1826, as so amended, provides: On a semiannual basis the Attorney General shall fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate, and the Committee on the Judiciary of the Senate, concerning all physical searches conducted pursuant to this subchapter. On a semiannual basis the Attorney General shall also provide to those committees and the Committee on the Judiciary of the House of Representatives a report setting forth with respect to the preceding six-month period —
(1) the total number of applications made for orders approving physical searches under this subchapter;
(2) the total number of such orders either granted, modified, or denied;
(3) the number of physical searches which involved searches of the residences, offices, or personal property of United States persons, and the number of occasions, if any, where the Attorney General provided notice pursuant to section 1825(b) of this title; and

(4) the total number of emergency physical searches authorized by the Attorney General under section 1824(e) of this title and the total number of subsequent orders approving or denying such physical searches.

[3789] See fn. 86, supra, and accompanying text.

[3790] The reporting requirement regarding the total number of emergency physical searches authorized under 50 U.S.C. § 1824(e) was added by Section 109(a)(5) of P.L. 109-177.

[3791] This section was added in 1994 as Title III, Section 307 of P.L. 95-511, by P.L. 103-359, Title VIII, § 807(a)(3), 108 Stat. 3452. If a fine were to be imposed under the general fine provisions 18

than five years or both. Federal jurisdiction attaches where the offense is committed by an officer or employee of the United States. It is a defense to such a prosecution if the defendant was a law enforcement or investigative officer engaged in official duties and the physical search was authorized and conducted pursuant to a search warrant or court order by a court of competent jurisdiction.

50 U.S.C. § 1828 — Civil Action.

In addition, an aggrieved person other than a foreign power or an agent of a foreign power as defined under section 1801(a) or 1801(b)(1)(A),[3792] whose premises, property, information, or material within the United States was physically searched under FISA; or about whom information obtained by such a search was disclosed or used in violation of 50 U.S.C. § 1827, may bring a civil action for actual damages, punitive damages, and reasonable attorney's fees and other investigative and litigation costs reasonably incurred.[3793]

50 U.S.C. § 1829 — Physical Searches without FISC Order after Congressional Declaration of War.

In times of war, the President, through the Attorney General, may authorize physical searches under FISA without a court order to obtain foreign intelligence information for up to 15 days following a declaration of war by Congress.[3794]

Pen registers or trap and trace devices[3795] used for foreign intelligence gathering purposes.

U.S.C. § 3571, rather than under the offense provision, the maximum fine would be $250,000 for an individual.

[3792] For definitions, see fn. 44, *supra*.

[3793] 50 U.S.C. § 1828. Actual damages are defined to be "not less than liquidated damages of $1,000 or $100 per day for each violation, whichever is greater." 50 U.S.C. § 1828(1).

[3794] 50 U.S.C. § 1829.

[3795] Under 50 U.S.C. § 1841(2), the terms "pen register" and "trap and trace device" are given the meanings in 18 U.S.C. § 3127. Under Section 3127, "pen register" ...

means a device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached, but such term does not include any device used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business; ....

As defined by 18 U.S.C. § 3127(4), "trap and trace device" "means a device which captures the incoming electronic or other impulses which identify the originating number of an instrument or device from which a wire or electronic communication was transmitted." 50 U.S.C. § 1841 is the

Title IV of FISA, 50 U.S.C. § 1841 et seq., was added in 1998, amended by P.L. 107-56,[3796] and amended further by Section 314(5) of P.L. 107-108.

50 U.S.C. § 1842(a)-(c) — Application for an FISC Order Authorizing Installation and Use of Pen Register or Trap and Trace Device.

Under 50 U.S.C. § 1842(a)(1), notwithstanding any other provision of law, the Attorney General or a designated attorney for the Government may apply for an order or extension of an order authorizing or approving the installation and use of a pen register or trap and trace device "*for any investigation to protect against international terrorism or clandestine intelligence activities, provided such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution*" conducted by the Federal Bureau of Investigation (FBI) under guidelines approved by the Attorney General pursuant to E.O. 12333 or a successor order.[3797] This authority is separate from the authority to conduct electronic surveillance under 50 U.S.C. § 1801 et seq.[3798]

Each such application is made in writing upon oath or affirmation to an FISC judge or to a U.S. magistrate judge publicly designated by the Chief Justice of the United States to hear such applications and grant orders approving installation of pen registers or trap and trace devices on behalf of an FISC judge. The application must be approved by the Attorney General or a designated attorney for the Government. Each application must identify the federal officer seeking to use the pen register or trap and trace device covered by the application. It must also include a certification by the applicant "that the information likely to be obtained is relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution."[3799] Under 50 U.S.C. §

---

section that defines terms applicable to the pen register and trap and trace device portions of FISA.

[3796] Title IV of FISA was added by Title VI, Sec. 601(2) of P.L. 105-272, on October 20, 1998, 112 Stat. 2405-2410, and amended by P.L. 107-56 and by P.L. 107-108.

[3797] The italicized language was added by P.L. 107-56, Section 214(a)(1), replacing language which had read "for any investigation to gather foreign intelligence information or information concerning international terrorism."

[3798] 50 U.S.C. § 1842(a)(2).

[3799] This language, added by P.L. 107-56, Section 214(a)(2), replaced stricken language which read:

(2) a certification by the applicant that the information to be obtained is relevant to an ongoing foreign intelligence or international terrorism investigation being conducted by the Federal Bureau of Investigation under guidelines approved by the Attorney General; and

(3) information which demonstrates that there is reason to believe that the telephone line to which the pen register or trap and trace device is to be attached, or the communication

1842, as amended by P.L. 107-56, pen registers and trap and trace devices may now be installed and used not only to track telephone calls, but also other forms of electronic communication such as e-mail.

50 U.S.C. § 1842(d) — Issuance of FISC Order for Installation and Use of Pen Register or Trap and Trace Device.

Once an application is made under Section 1842, the judge[3800] must enter an ex parte order[3801] as requested or as modified approving the installation and use of a

---

instrument or device to be covered by the pen register or trap and trace device, has been or is about to be used in communication with —
(A) an individual who is engaging or has engaged in international terrorism or clandestine intelligence activities that involve or may involve a violation of the criminal laws of the United States; or

(B) a foreign power or agent of a foreign power under circumstances giving reason to believe that the communication concerns or concerned international terrorism or clandestine intelligence activities that involve or may involve a violation of the criminal laws of the United States.

[3800] This section refers simply to "judge." In light of 50 U.S.C. § 1842(b), it would appear that this may refer to either an FISC judge or a U.S. magistrate judge designated by the Chief Justice under Section 1842(b)(2) to hear applications for and grant orders approving installation and use of pen registers or trap and trace devices on behalf of an FISC judge. The legislative history on this provision does not appear to clarify this point. The language was included in the bill reported out as an original measure by the Senate Select Committee on Intelligence, S. 2052, as Sec. 601. The Committee's report, S.Rept. 105-185, indicates that magistrate judges were included in the legislation to parallel their use in connection with receipt of applications and approval of pen registers and trap and trace devices in the context of criminal investigations, but reflected the Committee's understanding that the authority provided in the legislation to designate magistrate judges to consider applications for pen registers and trap and trace devices in the foreign intelligence gathering context would be closely monitored by the Department of Justice and this designation authority would not be exercised until the Committee was briefed on the compelling need for such designations, as reflected, for example, through statistical information on the frequency of applications to the FISC under the new procedure. S.Rept. 105-185, at 28 (May 7, 1998). The provision authorizing the use of pen registers and trap and trace devices in foreign intelligence and international terrorism investigations, Sec. 601 of the bill as passed, was among those included in the conference version of H.R. 3694 which was passed in lieu of S. 2052. H.Rept. 105-80, at 32 (October 5, 1998).
[3801] Under 50 U.S.C. § 1842(d)(2)(A), such an order
(A) shall specify —
(i) the identity, if known, of the person who is the subject of the investigation;
(ii) the identity, if known, of the person to whom is leased or in whose name is listed the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied; and
(iii) the attributes of the communications to which the order applies, such as the number or other identifier, and, if known, the location of the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied and, in the case of a trap and trace device, the geographic limits of the trap and trace order;
(B) shall direct that —
(i) upon request of the applicant, the provider of a wire or electronic communication service, landlord, custodian, or other person shall furnish any information, facilities, or technical assistance necessary to accomplish the installation and operation of the pen register or trap and

trace device in such a manner as will protect its secrecy and produce a minimum amount of interference with the services that such provider, landlord, custodian, or other person is providing the person concerned;
(ii) such provider, landlord, custodian, or other person —
(I) shall not disclose the existence of the investigation or of the pen register or trap and trace device to any person unless or until ordered by the court; and
(II) shall maintain, under security procedures approved by the Attorney General and the Director of National Intelligence pursuant to section 1805(b)(2)(C) of this title, any records concerning the pen register or trap and trace device or the aid furnished; and
(iii) the applicant shall compensate such provider, landlord, custodian, or other person for reasonable expenses incurred by such provider, landlord, custodian, or other person in providing such information, facilities, or technical assistance; and
(C) shall direct that, upon the request of the applicant, the provider of a wire or electronic communication service shall disclose to the Federal officer using the pen register or trap and trace device covered by the order —
(i) in the case of the customer or subscriber using the service covered by the order (for the period specified by the order) —
(I) the name of the customer or subscriber;
(II) the address of the customer or subscriber;
(III) the telephone or instrument number, or other subscriber number or identifier, of the customer or subscriber, including any temporarily assigned network address or associated routing or transmission information;
(IV) the length of the provision of service by such provider to the customer or subscriber and the types of services utilized by the customer or subscriber;
(V) in the case of a provider of local or long distance telephone service, any local or long distance telephone records of the customer or subscriber;
(VI) if applicable, any records reflecting period of usage (or sessions) by the customer or subscriber; and
(VII) any mechanisms and sources of payment for such service, including the number of any credit card or bank account utilized for payment for such service; and
(ii) if available, with respect to any customer or subscriber of incoming or outgoing communications to or from the service covered by the order —
(I) the name of such customer or subscriber;
(II) the address of such customer or subscriber;
(III) the telephone or instrument number, or other subscriber number or identifier, of such customer or subscriber, including any temporarily assigned network address or associated routing or transmission information; and
(IV) the length of the provision of service by such provider to such customer or subscriber and the types of services utilized by such customer or subscriber.

The italicized portions of this section reflect amended language from P.L. 107-56, Section 214 (a)(4). In 50 U.S.C. § 1842(d)(2)(B)(ii)(II), the reference to the "Director of National Intelligence" replaced a reference to the "Director of Central Intelligence" pursuant to Section 1071(e) of P.L. 108-458. Subsection 128(a)(3) added 50 U.S.C. § 1842(d)(2)(C).

P.L. 107-108, Section 314(a)(5)(B), replaced "of a court" at the end of 50 U.S.C. § 1842(f) with "of an order issued," so that the language now reads: (f) No cause of action shall lie in any court against any provider of a wire or electronic communication service, landlord, custodian, or other person (including any officer, employee, agent, or other specified person thereof) that furnishes any information, facilities, or technical assistance under subsection (d) in accordance with the terms of an order issued under this section. (Emphasis added.) Cf., 50 U.S.C. § 1805(i), which contains an immunity grant which, at first blush would appear to apply only to electronic surveillance under FISA, but which has been interpreted at page 25 of H.Rept. 107-328, the

pen register or trap and trace device if the application meets the requirements of that section. Generally, an order issued under 50 U.S.C. § 1842 may authorize the installation and use of a pen register or trap and trace device for a period not to exceed 90 days. Extensions of such an order may also be granted for up to 90 days. However, in the case of an application under subsection 1842(c) where the applicant has certified that the information likely to be obtained is foreign intelligence information not concerning a United States person, an order, or an extension of an order for a FISA pen register or trap and trace device may be up to one year.[3802]

50 U.S.C. § 1842(f) — Limitation of Liability.

Section 1842(f) bars any cause of action in any court against any provider of a wire or electronic communication service, landlord, custodian, or other person (including any officer, employee, agent, or other specified person thereof) that furnishes any information, facilities, or technical assistance under subsection 1842(d) in accordance with the terms of an order issued under this section.

50 U.S.C. § 1843 — Emergency Attorney General Authorization of Pen Register or Trap and Trace Device while FISC Order Is Pursued.

Section 1843 of Title 18 of the United States Code focuses upon authorization for installation and use of a pen register or trap and trace device under FISA during specified types of emergencies. This provision applies when the Attorney General makes a reasonable determination that:
(1) an emergency requires the installation and use of a pen register or trap and trace device to obtain foreign intelligence information not concerning a United States person or information to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution before an order authorizing the installation and use of the pen register or trap and trace device, as the case may be, can with due diligence be obtained under section 1842 of this title; and

---

conference report accompanying H.R. 2883 (the conference version of which became P.L. 107-108) to apply to electronic surveillance, physical searches and pen register and trap and trace devices. This subsection was added as 50 U.S.C. § 1805(h) by Section 225 of P.L. 107-56, and redesignated 50 U.S.C. § 1805(i) by Section 314(a)(2)(C) of P.L. 107-108. See discussion at fn. 66, supra.

[3802] 50 U.S.C. § 1842(e), as amended by Section 105(c) of P.L. 109-177. Under 50 U.S.C. § 1842(g), unless otherwise ordered by the judge, the results of a pen register or trap and trace device are furnished at reasonable intervals during regular business hours for the duration of the order to the authorized Government official or officials.

(2) the factual basis for issuance of an order under section 1842(c) of this title to approve the installation and use of the pen register or trap and trace device, as the case may be, exists.[3803]

Upon making such a determination, the Attorney General may authorize the installation and use of a pen register or trap and trace device for this purpose if two criteria are met. First, the Attorney General or his designee must inform a judge referred to in Section 1842(b)[3804] at the time of the emergency authorization that the decision to install and use the pen register or trap and trace device has been made. Second, an application for a court order authorizing a pen register or trap and trace device under 50 U.S.C. § 1842(a)(1) must be made to the judge as soon as practicable, but no later that 48 hours after the emergency authorization.[3805] If no order approving the installation and use of a pen register or trap and trace device is forthcoming, then the installation and use of such pen register or trap and trace device must terminate at the earlier of the time when the information sought is obtained, the time when the application for the order is denied under 50 U.S.C. § 1842, or the expiration of 48 hours from the time the Attorney General made his emergency authorization.[3806]

If an application for an order sought under Section 1843(a)(2) is denied, or if the installation and use of the pen register or trap and trace device is terminated, and no order approving it is issued under 50 U.S.C. § 1842(b)(2), then no information obtained or evidence derived from the use of the pen register or trap and trace device may be received in evidence or disclosed in any trial, hearing or other proceeding in any court, grand jury, department, office, agency, regulatory body, legislative committee or other federal state or local authority. Furthermore, in such circumstances, no information concerning a United States person acquired from the use of the pen register or trap and trace device may later be used or disclosed in any other way by federal officers or employees without consent of the U.S. person involved, with one exception. If the Attorney General approves the disclosure because the information indicates a threat of death or serious bodily harm to anyone, then disclosure without consent of the U.S. person involved is permitted.[3807]

[3803] 50 U.S.C. § 1843(b) (italics reflect language added by P.L. 107-56, § 214(b)(2), in place of language which read "foreign intelligence information or information concerning international terrorism.") Similar language was inserted in 50 U.S.C. § 1843(a) by P.L. 10756, § 214(b)(1), in place of language that paralleled that stricken from subsection 1843(b).

[3804] See discussion of the term "judge" as used in Section 1842(b) in fn. 121, supra.

[3805] 50 U.S.C. § 1843(a).

[3806] 50 U.S.C. § 1843(c)(1).

[3807] 50 U.S.C. § 1843(c)(2).

50 U.S.C. § 1844 — Use of Pen Register or Trap and Trace Device without FISC Order after Congressional Declaration of War.

If Congress declares war, then, notwithstanding any other provision of law, the President, through the Attorney General, may authorize use of a pen register or trap and trace device without a court order to acquire foreign intelligence information for up to 15 calendar days after the declaration of war.[3808]

50 U.S.C. § 1845 — Use of Information Obtained from FISA Pen Register or Trap and Trace Device.

50 U.S.C. § 1845 sets parameters with respect to the use of information obtained through the use of a pen register or trap and trace device under 50 U.S.C. § 1841 et seq. Federal officers and employees may only use or disclose such information with respect to a U.S. person without the consent of that person in accordance with Section 1845.[3809] Any disclosure by a Federal officer or employee of information acquired pursuant to FISA from a pen register or trap and trace device must be for a lawful purpose.[3810] Disclosure for law enforcement purposes of information acquired under 50 U.S.C. § 1841 et seq. is only permitted where the disclosure is accompanied by a statement that the information and any derivative information may only be used in a criminal proceeding with the advance authorization of the Attorney General.[3811]

Under 50 U.S.C. § 1845(c), when the United States intends to enter into evidence, use, or disclose information obtained by or derived from a FISA pen register or trap and trace device against an aggrieved person[3812] in any federal trial, hearing, or proceeding, notice requirements must be satisfied. The Government, before the trial, hearing, or proceeding or a reasonable time before the information is to be proffered, used or disclosed, must give notice of its intent both to the

---

[3808] 50 U.S.C. § 1844.

[3809] 50 U.S.C. § 1845(a)(1).

[3810] 50 U.S.C. § 1845(a)(2).

[3811] 50 U.S.C. § 1845(b).

[3812] "Aggrieved person" is defined in 50 U.S.C. § 1841(3) for purposes of 50 U.S.C. § 1841 et seq. as any person:
(A) whose telephone line was subject to the installation or use of a pen register or trap and trace device authorized by subchapter IV [50 U.S.C. § 1841 et seq.]; or

(B) whose communication instrument or device was subject to the use of a pen register or trap and trace device authorized by subchapter IV to capture incoming electronic or other communications impulses.

aggrieved person involved[3813] and to the court or other authority in which the information is to be disclosed or used.

If a state or local government intends to enter into evidence, use, or disclose information obtained or derived from such a trap and trace device against an aggrieved person in a state or local trial, hearing or proceeding, it must give notice to the aggrieved person and to the Attorney General of the United States of the state or local government's intent to disclose or use the information.[3814]

50 U.S.C. §1845(c)-(f) — U.S. District Court Consideration of Notices, Motions to Suppress, or Discovery Motions.

The aggrieved person in either case may move to suppress the evidence obtained or derived from a FISA pen register or trap and trace device on one of two grounds: that the information was unlawfully acquired; or that the use of the pen register or trap and trace device was not made in conformity with an order of authorization or approval under 50 U.S.C. § 1841 *et seq*.[3815]

If notice is given under 50 U.S.C. §§ 1845(c) or (d), or a motion or request is made to suppress or to discover or obtain any applications, orders, or other materials relating to use of a FISA pen register or trap and trace device or information obtained by or derived from such use, the Attorney General may have national security concerns with respect to the effect of such disclosure or of an adversary hearing. If he files an affidavit under oath that disclosure or any adversary hearing would harm the national security of the United States, the United States district court in which the motion or request is made, or where the motion or request is made before another authority, the U.S. district court in the same district, shall review in camera and ex parte the application, order, and other relevant materials to determine whether the use of the pen register or trap and trace device was lawfully authorized and conducted.[3816] In so doing, the court may only disclose portions of the application, order or materials to the aggrieved person or order the Attorney General to provide the aggrieved person with a summary of these materials if that disclosure is necessary to making an accurate

---

[3813] The statute refers to notice to the "aggrieved person." Here it is using this term in the context of a pen register or trap and trace device under FISA (see fn. 90 for the applicable definition of "pen register" and "trap and trace device" in 50 U.S.C. § 1841(2) and fn. 106 for the applicable definition of "aggrieved person" in 50 U.S.C.§ 1841(3), supra). The term "aggrieved person" is also defined in both 50 U.S.C. §§ 1801(k) (in the context of electronic surveillance, see fn. 67, supra) and 1825(d) (in the context of a physical search, see fn. 97, supra).

[3814] 50 U.S.C. § 1845(d).

[3815] 50 U.S.C. § 1845(e).

[3816] 50 U.S.C. § 1845(f)(1).

determination of the legality of the use of the pen register or trap and trace device.[3817]

Should the court find that the pen register or trap and trace device was not lawfully authorized or conducted, it may suppress the unlawfully obtained or derived evidence or "otherwise grant the motion of the aggrieved person."[3818] On the other hand, if the court finds the pen register or trap and trace device lawfully authorized and conducted, it may deny the aggrieved person's motion except to the extent discovery or disclosure is required by due process.[3819] Any U.S. district court orders granting motions or request under Section 1845(g), finding unlawfully authorized or conducted the use of a pen register or trap and trace device, or requiring review or granting disclosure of applications, orders or other materials regarding installation and use of a pen register or trap and trace device are deemed final orders. They are binding on all federal and state courts except U.S. courts of appeals and the U.S. Supreme Court.[3820]

50 U.S.C. § 1846 — Congressional Oversight.

Section 1846 deals with congressional oversight of the use of FISA pen registers and trap and trace devices.[3821] It requires the Attorney General semiannually to fully inform the House Permanent Select Committee on Intelligence, the Senate Select Committee on Intelligence, and the House and Senate Judiciary Committees[3822] regarding all FISA uses of pen registers and trap and trace devices. In addition, the Attorney General, on a semi-annual basis, must report to the House Permanent Select Committee on Intelligence, the Senate Select Committee on Intelligence, the House Judiciary Committee and the Senate Judiciary Committee on the total number of applications made for orders approving the use of such pen registers and trap and trace devices; the total number of such orders granted, modified, or denied during the previous six month period; the total number of pen registers and trap and trace devices whose installation and use was authorized by the Attorney General on an emergency basis under section 1843 of this title, and the total number of subsequent orders

---

[3817] 50 U.S.C. § 1845(f)(2).

[3818] 50 U.S.C. § 1845(g)(1).

[3819] 50 U.S.C. § 1845(g)(2).

[3820] 50 U.S.C. § 1845(h).

[3821] See also Section 6002 of P.L. 108-458, the Intelligence Reform and Terrorism Prevention Act of 2004, which amended FISA to add additional reporting requirements codified at 50 U.S.C. § 1871. These new reporting requirements are discussed at fn. 165, infra, and accompanying text.

[3822] 50 U.S.C. § 1846(a). P.L. 109-177, Section 128(b), added the House and Senate Judiciary Committees to the list of committees to be kept fully informed by the Attorney General regarding all use of FISA pen registers and trap and trace devices.

approving or denying the installation and use of such pen registers and trap and trace devices.[3823]

Access to certain business records or other tangible things for foreign intelligence purposes.

Added in 1998, Title V of FISA, 50 U.S.C. § 1861 et seq., was substantially changed by P.L. 107-56, and modified further by P.L. 107-108, P.L. 109-177, and P.L. 109-178.[3824] Although denominated "access to certain business records for

---

[3823] 50 U.S.C. § 1846(b). P.L. 109-177, Section 109(b)(3), added the reporting requirements with respect to the total number of emergency pen registers and trap and trace devices authorized by the Attorney General under 50 U.S.C. § 1843, and the total number of subsequent orders approving or denying such installation and use.

[3824] Title V of FISA was added by Title VI, Sec. 602, of P.L. 105-272, on October 20, 1998, 112 Stat. 2411-12, and significantly amended by P.L. 107-56 and P.L. 107-108. The prior version of 50 U.S.C. § 1861 provided definitions for "foreign power," "agent of a foreign power," "foreign intelligence information," "international terrorism," and "Attorney General," "common carrier," "physical storage facility," "public accommodation facility," and "vehicle rental facility" for purposes of 50 U.S.C. § 1861 et seq. The prior version of Section 1862 was much more narrowly drawn than the new version added in P.L. 107-56 and amended by P.L. 107-108. The earlier version read:

(a) The Director of the Federal Bureau of Investigation or a designee of the Director (whose rank shall be no lower than Assistant Special Agent in Charge) may make an application for an order authorizing a common carrier, public accommodation facility, physical storage facility, or vehicle rental facility to release records in its possession for an investigation to gather foreign intelligence information or an investigation concerning international terrorism which investigation is being conducted by the Federal Bureau of Investigation under such guidelines as the Attorney General approves pursuant to Executive Order No. 12333, or a successor order.

(b) Each application under this section —

(1) shall be made to —

(A) a judge of the court established by section 1803(a) of this title; or

(B) a United States Magistrate Judge under chapter 43 of Title 28 [28 U.S.C. § 631 et seq.], who is publicly designated by the Chief Justice of the United States to have the power to hear applications and grant orders for the release of records under this section on behalf of a judge of that court; and

(2) shall specify that —

(A) the records concerned are sought for an investigation described in subsection (a); and

(B) there are specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or an agent of a foreign power.

(c) (1) Upon application made pursuant to this section, the judge shall enter an ex parte order as requested, or as modified, approving the release of records if the judge finds that the application satisfied the requirements of this section.

(2) An order under this subsection shall not disclose that it is issued for purposes of an investigation described in subsection (a).

(d) (1) Any common carrier, public accommodation facility, physical storage facility, or vehicle rental facility shall comply with an order under subsection (c).

(2) No common carrier, public accommodation facility, physical storage facility, or vehicle rental facility, or officer, employee, or agent thereof, shall disclose to any person (other than those officers, agents, or employees of such common carrier, public accommodation facility , physical storage facility, or vehicle rental facility necessary to fulfill the requirement to disclose information to the Federal Bureau of Investigation under this section) that the Federal Bureau of

foreign intelligence and international terrorism investigations," the reach of Section 1861, as amended by the USA PATRIOT Act, P.L. 107-108, P.L. 109-177, and P.L. 109-178, is now substantially broader than business records alone.

50 U.S.C. § 1861(a)(1) — Applications for FISC Order for Production of any Tangible Thing.

Under 50 U.S.C. § 1861(a)(1), subject to Subsection 1861(a)(3), the Director of the FBI, or his designee (who must be at the Assistant Special Agent in Charge level or higher in rank) may apply for an order requiring

> *... the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution.*[3825]

Investigation has sought or obtained records pursuant to an order under this section. Congressional oversight was covered under the prior provisions by 50 U.S.C. §1863, which was similar, but not identical to the new Section 1862. The former Section 1863 stated:
(a) On a semiannual basis, the Attorney General shall fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate concerning all request for records under this subchapter [50 U.S.C. § 1861 et seq.].
(b) On a semiannual basis, the Attorney General shall provide to the Committees on the Judiciary of the House of Representatives and the Senate a report setting forth with respect to the preceding 6-month period —
(1) the total number of applications made for orders approving requests for records under this subchapter [50 U.S.C. § 1861 et seq.]; and

(2) the total number of such orders either granted, modified, or denied.

[3825] The italicized portion of Section 1861(a)(1) was added by Section 314(a)(6) of P.L. 107-108. H.Rept. 107-328, the conference report to accompany H.R. 2883, the Intelligence Authorization Act for Fiscal Year 2002 (which became P.L. 107-108), at page 24, describes the purpose of this addition as follows: Section 215 of the USA PATRIOT Act of 2001 amended title V of the FISA, adding a new section 501 [50 U.S.C. § 1861]. Section 501(a) now authorizes the director of the FBI to apply for a court order to produce certain records "for an investigation to protect against international terrorism or clandestine intelligence activities." Section 501(b)(2) directs that the application for such records specify that the purpose of the investigation is to "obtain foreign intelligence information not concerning a United States person." However, section 501(a)(1), which generally authorizes the applications, does not contain equivalent language. Thus, subsections (a)(1) and (b)(2) now appear inconsistent.

The conferees agreed to a provision which adds the phrase "to obtain foreign intelligence information not concerning a United States person or" to section 501(a)(1). This would make the language of section 501(a)(1) consistent with the legislative history of section 215 of the USA PATRIOT Act (see 147 Cong. Rec. S11006 (daily ed. Oct. 25, 2001) (sectional analysis)) and with the language of section 214 of the USA PATRIOT Act (authorizing an application for an order to

Subsection 1861(a)(2) requires that such an investigation must be conducted under guidelines approved by the Attorney General under E.O. 12333 or a successor order and prohibits such an investigation of a United States person based solely upon First Amendment protected activities.

Under Subsection 1861(a)(3), which was added by Section 106(a)(2) of P.L. 109-177, if the application is for an order requiring production of library circulation records, library patron lists, book sales records, book customer lists, firearms sales records, tax return records, educational records, or medical records containing information that would identify a person, the Director of the Federal Bureau of Investigation may delegate the authority to make such application to either the Deputy Director of the Federal Bureau of Investigation or the Executive Assistant Director for National Security (or any successor position). The Deputy Director or the Executive Assistant Director may not further delegate such authority.

An application for an order under Section 1861 must be made to an FISC judge or to a U.S. magistrate judge publicly designated by the Chief Justice of the United States to hear such applications and grant such orders for the production of tangible things on behalf of an FISC judge.[3826] The application must contain a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation (other than a threat assessment) conducted in accordance with 50 U.S.C. § 1861(a)(2) to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities.[3827]

50 U.S.C. § 1861(c) — Issuance of FISC Production Order.

When such an application is made, if the judge finds that the application meets the requirements of subsections 1861(a) and (b), he or she must enter an ex parte

---

use pen registers and trap and trace devices to "obtain foreign intelligence information not concerning a United States person.").

[3826] 50 U.S.C. § 1861(b)(1).

[3827] 50 U.S.C. § 1861(b)(2), as amended by Section 106(b) of P.L. 109-177. As so amended, the tangible things sought are presumed to be relevant to an authorized investigation if the applicant shows, in the statement of facts, that they pertain to a foreign power or an agent of a foreign power; the activities of a suspected agent of a foreign power who is the subject of such authorized investigation; or an individual in contact with, or known to, a suspected agent of a foreign power who is the subject of such authorized investigation. 50 U.S.C. § 1861(b)(2)(A)(i)-(iii). The application must also include an enumeration of the minimization procedures adopted by the Attorney General under Subsection 1861(g) that are applicable to the retention and dissemination by the Federal Bureau of Investigation of any tangible things to be made available to the Federal Bureau of Investigation based on the order requested in such application. 50 U.S.C. § 1861(b)(2)(B).

order as requested, or as modified, approving the release of tangible things. The order must direct that minimization procedures adopted pursuant to subsection 1861(g) be followed.[3828]

An order issued under 50 U.S.C. § 1861(c) must: describe the tangible things that are ordered to be produced with sufficient particularity to permit them to be fairly identified; include the date on which the tangible things must be provided, which must allow a reasonable period of time within which the tangible things can be assembled and made available; and provide recipients with clear and conspicuous notice of nondisclosure requirements under Subsection 1861(d). The order may only require the production of a tangible thing which may be subject to a subpoena duces tecum issued by a court of the United States in aid of a grand jury investigation or to any other order issued by a court of the United States directing the production of records or tangible things. An order issued under 50 U.S.C. § 1861(c) shall not disclose that it is issued for purposes of an investigation described in Subsection 1861(a).[3829]

50 U.S.C. § 1861(d) — Prohibition on Disclosure.

Subsection 1861(d) prohibits any person to disclose that the FBI has sought or obtained tangible things under Section 1861, except where the disclosure is made to persons necessary to the production of tangible things involved, to an attorney to obtain legal advice or assistance with respect to the production of things in response to the order, or to other persons as permitted by the Director of the FBI or his designee.[3830] A person to whom such disclosure is made is also subject to these nondisclosure requirements, and must be put on notice of the nondisclosure requirements by the person making such disclosures to him or her. At the request of the Director of the FBI or his designee, anyone making or intending to make such a disclosure must identify to the Director or his designee the person to whom the disclosure was or is to be made.[3831]

50 U.S.C. § 1861(e) — Limitation on Liability for Good Faith Compliance with Production Order.

[3828] 50 U.S.C. § 1861(c)(1), as amended by Subsection 106(c) of P.L. 109-177.

[3829] 50 U.S.C. § 1861(c)(2), as amended by Subsection 106(d) of P.L. 109-177.

[3830] 50 U.S.C. § 1861(d)(1)(A)-(C), as amended by Subsection 106(e) of P.L. 109-177.

[3831] 50 U.S.C. § 1861(d)(2), as amended by Subsection 106(e) of P.L. 109-177, and further amended by Section 4 of P.L. 109-178. As amended by Subsection 106(e) of P.L. 109-177, subsection 1861(d)(2)(C) included an exception to the notification requirement in that a person was not required to notify the Director or his designee that he or she intended to consult an attorney to obtain legal advice or assistance. This exception was deleted by Section 4 of P.L. 109-178.

Subsection 1861(e) precludes liability for persons who, in good faith, produce tangible things under such a Section 1861 order. It further indicates that production does not constitute a waiver of any privilege in any other proceeding or context.

50 U.S.C. § 1861(f) — Petitions for Review of Production Orders and Related Nondisclosure Orders before FISC Petition Review Pool.

Subsection 1861(f), which was added by Subsection 106(f) of P.L. 109-177 and amended by Section 3 of P.L. 109-178, gives a person in receipt of a production order[3832] under 50 U.S.C. § 1861 a means by which to challenge the legality of such order by filing a petition before the petition review pool of the FISC established by 50 U.S.C. § 1803(e)(1). The recipient of a production order must wait at least one year after issuance of that order to challenge the nondisclosure order[3833] imposed in connection with the production order by filing a petition to modify or set aside the nondisclosure order before the petition review pool.[3834] The presiding judge must assign a petition filed with the pool under subsection 1861(f)(2)(A)(i) to one of the FISC judges in the pool immediately, and the judge receiving such petition must conduct an initial review of it within 72 hours. If the petition is deemed frivolous, the assigned judge must immediately deny it and affirm the production order or nondisclosure order at issue. If the assigned judge does not find the petition frivolous, he or she must promptly consider it under the PROCEDURES FOR REVIEW OF PETITIONS FILED PURSUANT TO SECTION 501(F) OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED, established under 50 U.S.C. § 1803(e)(2), and provide a written statement for the record of the reasons for any determination made. An order setting aside a nondisclosure order may be stayed, upon request of the Government, pending review by the Court of Review.[3835]

A petition to modify or set aside a production order may only be granted if the judge finds the order does not meet the requirements of 50 U.S.C. § 1861 or is otherwise unlawful. If the judge does not modify or set aside the production order, he or she must immediately affirm the order and order the recipient to comply with it.[3836] A petition to modify or set aside a nondisclosure order may only be granted if the judge finds that there is no reason to believe that disclosure

---

[3832] The term "production order" is defined under 50 U.S.C. § 1861(f)(1)(A) to mean "an order to produce any tangible thing" under 50 U.S.C. § 1861.

[3833] The term "nondisclosure order" is defined under 50 U.S.C. § 1861(f)(1)(B) to mean "an order imposed under subsection [1861](d)."

[3834] 50 U.S.C. § 1861(f)(2)(A)(i).

[3835] 50 U.S.C. §1861(f)(2)(A)(ii) and (iii).

[3836] 50 U.S.C. § 1861(f)(2)(B).

may endanger U.S. national security; interfere with a criminal, counterterrorism, or counterintelligence investigation; interfere with diplomatic relations; or endanger the life or physical safety of any person. If, upon the filing of a petition to modify or set aside a nondisclosure order, the Attorney General, Deputy Attorney General, an Assistant Attorney General, or the Director of the FBI certifies that disclosure may endanger the national security of the United States or interfere with diplomatic relations, that certification will be treated as conclusive unless the judge finds that the certification was made in bad faith. If a petition to modify or set aside a nondisclosure order is denied, the recipient may not file another petition to modify or set aside that nondisclosure order for one year.[3837] A production order or nondisclosure order that is not explicitly modified or set aside under Section 1861 remains in full effect.[3838]

The Government or any person receiving a production or nondisclosure order may file a petition before the Court of Review to review a decision by a petition review pool judge to affirm, modify, or set aside such order. The Court of Review must provide a written statement of the reasons for its decision for the record. The record will be transmitted under seal to the U.S. Supreme Court for review on a petition for certiorari by the Government or any person receiving such order.[3839]

Judicial proceedings under 50 U.S.C. § 1861(f) are to be concluded as expeditiously as possible, and the record of such proceedings is to be maintained under security measures established by the Chief Justice of the United States, in consultation with the Attorney General and the Director of National Intelligence. Petitions are to be filed under seal. Upon the request of the Government, the court in proceedings under Subsection 1861(f) shall review ex parte and in camera any Government submissions, or portions thereof, which may contain classified information.[3840]

50 U.S.C. § 1861(h) — Use of Information Acquired from Tangible Things Received Under Production Order.

Subsection 1861(g), as added by Subsection 106(g) of P.L. 109-177, requires the Attorney General to adopt specific minimization procedures[3841] governing

[3837] 50 U.S.C. § 1861(f)(2)(C)(i), (ii), and (iii).

[3838] 50 U.S.C. § 1861(f)(2)(D).

[3839] 50 U.S.C. § 1861(f)(3).

[3840] 50 U.S.C. § 1861(f)(4) and (5).

[3841] Subsection 50 U.S.C. § 1861(g)(2) defines the term "minimization procedures" to mean:
(A) specific procedures that are reasonably designed in light of the purpose and technique of an order for the production of tangible things, to minimize the retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States

retention and dissemination by the FBI or any tangible things, or information in those things, received by the FBI in response to an order under 50 U.S.C. § 1861. Subsection 1861(h), also added by Subsection 106(g) of P.L. 109-177, provides that information acquired from tangible things received by the FBI pursuant to an order under 50 U.S.C. § 1861 concerning any U.S. person may be used and disclosed by federal officers and employees without that U.S. person's consent only in accordance with these minimization procedures. Otherwise privileged information acquired from tangible things received by the FBI title V of FISA, 50 U.S.C. §§ 1861-1862, retains its privileged character. Information acquired by the FBI under Section 1861 orders may only be used or disclosed by federal officers or employees for lawful purposes.

50 U.S.C. § 1862 — Congressional Oversight.

50 U.S.C. § 1862 deals with congressional oversight.[3842] Subsection 1862(a), as amended by Subsection 106(h) of P.L. 109-177, requires the Attorney General annually to fully inform the House Permanent Select Committee on Intelligence, the Senate Select Committee on Intelligence, and the House and Senate Committees on the Judiciary regarding all request for production of tangible things under Section 1861.[3843] Subsection 1862(b) requires the Attorney General, in April of each year, to report to the House and Senate Judiciary Committees with respect to the previous calendar year on the total number of applications for Section 1861 orders for production of tangible things; the total number of such orders granted, modified, or denied; and the number of such orders either granted, modified, or denied for the production of each of the following: library circulation records, library patron lists, book sales records, or book customer lists; firearms sales records; tax return records; educational records; and medical records containing information that would identify a person. Under Subsection 1862(c), in April of each year, the Attorney General is required to submit an

---

persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information;
(B) procedures that require that nonpublicly available information, which is not foreign intelligence information as defined in section 101(e)(1) [of FISA, 50 U.S.C. § 1801(e)(1)], shall not be disseminated in a manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to understand foreign intelligence information or assess its importance; and

(C) notwithstanding subparagraphs (A) and (B), procedures that allow the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained and disseminated for law enforcement purposes.

[3842] See also Section 6002 of P.L. 108-458, the Intelligence Reform and Terrorism Prevention Act of 2004, which added new reporting requirements codified at 50 U.S.C. § 1871. For a discussion of these additional reporting requirements, see fn. 165, infra, and accompanying text.

[3843] Section 314(a)(7) of P.L. 107-108 corrected two references in 50 U.S.C. § 1862 as passed in the USA PATRIOT Act. P.L. 107-108 replaced "section 1842 of this title" with "section 1861 of this title," in both places in 50 U.S.C. § 1862 where it appeared.

unclassified report to Congress with respect to the preceding year setting forth the total number of applications made for orders approving requests for the production of tangible things under 50 U.S.C. § 1861; and the total number of such orders either granted, modified, or denied.

Section 106A of P.L. 109-177 directs the Inspector General of the U.S. Department of Justice to perform a comprehensive audit of the effectiveness and use, including improper or illegal use, of the investigative authority under title V of FISA, 50 U.S.C. § 1861 et seq., for fiscal years 2002-2006, and sets out detailed requirements for the audit. The results of the audit are to be submitted in two unclassified reports (one for 2002-2004 and one for 2005-2006) to the House and Senate Judiciary Committees, the House Permanent Select Committee on Intelligence, and the Senate Select Committee on Intelligence.

50 U.S.C. § 1871 — Additional Reporting Requirements.

Section 6002 of P.L. 108-458, the Intelligence Reform and Terrorism Prevention Act of 2004, created additional semiannual reporting requirements under FISA. Under the new language, the Attorney General, on a semiannual basis, must submit to the House Permanent Select Committee on Intelligence, the Senate Select Committee on Intelligence, the House Judiciary Committee and the Senate Judiciary Committee, in a manner consistent with protection of national security, reports setting forth with respect to the preceding six month period:

(1) the aggregate number of persons targeted for orders issued under this Act, including a breakdown of those targeted for —
(A) electronic surveillance under section 105 [50 U.S.C. § 1805];
(B) physical searches under section 304 [50 U.S.C. § 1824];
(C) pen registers under section 402 [50 U.S.C. § 1842]; and
(D) access to records under section 501 [50 U.S.C. § 1861];
(2) the number of individuals covered by an order issued pursuant to section 101(b)(1)(C) [50 U.S.C. § 1801(b)(1)(C)];
(3) the number of times that the Attorney General has authorized that information obtained under this Act may be used in a criminal proceeding or any information derived therefrom may be used in a criminal proceeding;
(4) a summary of significant legal interpretations of this Act involving matters before the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review, including interpretations presented in applications or pleadings filed with the Foreign Intelligence Surveillance Court or the Foreign Intelligence Court of Review by the Department of Justice; and
(5) copies of all decisions (not including orders) or opinions of the Foreign Intelligence Surveillance Court or Foreign Intelligence Surveillance Court of

Review that include significant construction or interpretation of the provisions of this Act.[3844]

Private Right of Action in U.S. District Court for Those Aggrieved by Willful Violations of 50 U.S.C. §§ 1806(a), 1825(a), or 1845(a) of FISA

In addition to provisions which amended FISA explicitly, other provisions of the USA PATRIOT Act, P.L. 107-56, touched upon FISA, at least tangentially. For example, Section 223 of P.L. 107-56, among other things, created a new 18 U.S.C. § 2712. This new section, in part, created an exclusive private right of action for any person aggrieved by any willful violation of sections 106(a), 305(a), or 405(a) of FISA (50 U.S.C. §§ 1806(a), 1825(a), 1845(a), respectively) to be brought against the United States in U.S. district court to recover money damages. Such monetary relief would amount to either actual damages or $10,000, whichever is greater; and reasonably incurred litigation costs. It also set forth applicable procedures.[3845]

[3844] These new reporting requirements were added to the Foreign Intelligence Surveillance Act, as amended, as a new Title VI of the Act, 50 U.S.C. § 1871.

[3845] Another provision, Section 901 of the USA PATRIOT Act, amended 50 U.S.C. § 4033(c) (Section 103(c) of the National Security Act of 1947) regarding the responsibilities of the Director of Central Intelligence (DCI). The amendment added to those authorities and responsibilities, placing upon the DCI the responsibility to establish

... requirements and priorities for foreign intelligence information to be collected under the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. § 1801 et seq.), and provide assistance to the Attorney General to ensure that information derived from electronic surveillance or physical searches under that Act is disseminated so it may be used efficiently and effectively for foreign intelligence purposes, except that the Director shall have no authority to direct, manage, or undertake electronic surveillance or physical search operations pursuant to that Act unless otherwise authorized by statute or Executive order.

Section 1011 of the Intelligence Reform and Terrorism Prevention Act of 2004, P.L.108-458, amended Title I of the National Security Act of 1947, 50 U.S.C. § 402 et seq., to strike the previous Sections 102 through 104 of the Act 50 U.S.C. §§ 403, 403-1, 403-3, and 403-4, and insert new Sections 102 through 104A. The new Section 102 created the position of Director of National Intelligence (DNI). Section 102A outlined authorities and responsibilities of the position. Under the new Section 102A(f)(6) of the National Security Act, the DNI was given responsibility:

to establish requirements and priorities for foreign intelligence information to be collected under [FISA], and provide assistance to the Attorney General to ensure that information derived from electronic surveillance or physical searches under that act is disseminated so that it may be used efficiently and effectively for foreign intelligence purposes, except that the Director shall have no authority to direct, manage, or undertake electronic surveillance or physical search operations pursuant to that act unless otherwise authorized by statute or Executive order.

New Section 102A(f)(8) of the National Security Act, as enacted by P.L. 108-458, Section 1011, provided that, "Nothing in this act shall be construed as affecting the role of the Department of Justice or the Attorney General with respect to applications under the Foreign Intelligence

Sunset Provisions

Section 224 of the USA PATRIOT Act set a sunset for many of the provisions in P.L. 107-56 of December 31, 2005, including all of the FISA amendments except that in Section 208 of P.L. 107-56, which increased the number of FISC judges from 7 to 11. Section 224 was repealed by the USA PATRIOT Improvement and Reauthorization Act of 2005, P.L. 109-177, Subsection 102(a). Subsection 102(b) of P.L. 109-177 provided that Sections 105(c)(2) of FISA, 50 U.S.C. § 1805(c)(2) (dealing with multipoint or roving wiretaps under FISA), 501 of FISA, 50 U.S.C. § 1861 (dealing with production of any tangible thing under FISA), and 502 of FISA, 50 U.S.C. § 1862 (dealing with congressional oversight of such production under FISA) will sunset on December 31, 2009. However, Subsection 102(b) of P.L. 109177 excepts from the application of the sunset provision any particular foreign intelligence investigations that began before December 31, 2009, or any criminal offenses or potential offenses which began or occurred before December 31, 2009. As to those particular investigations or offenses, applicable provisions would continue in effect after December 31, 2009.

Section 6001(a) of the Intelligence Reform and Terrorism Prevention Act of 2004, P.L. 108-458, expanded the definition of "agent of a foreign power" in 50 U.S.C. § 1801(b)(1)(C) to include any person other than a U.S. person who engages in international terrorism or activities in preparation for international terrorism.[3846] Under Section 103 of P.L. 109-177, this so-called "lone wolf" terrorist provision will also sunset on December 31, 2009, except with respect to any particular foreign intelligence investigation that began before that date, or with respect to any particular offense or potential offense that began or occurred before that date.

Published Decisions of the FISC and the U.S. Foreign Intelligence Surveillance Court of Review

The FISC Decision

Summary

In its May 17, 2002, decision, the FISC considered a government motion for the court "to vacate the minimization and 'wall' procedures in all cases now or ever before the Court, including this Court's adoption of the Attorney General's July 1995 intelligence sharing procedures, which are not consistent with new

---

Surveillance Act." Section 1071(e) of P.L. 108-458, amended FISA to insert "Director of National Intelligence" in lieu of "Director of Central Intelligence" in each place in which it appeared.

[3846] Before the repeal of Section 224 of P.L.107-56,, the sunset provision in Section 224 and the exceptions thereto, as amended, also applied to "lone wolf" terrorist provision added to the definition of "agent of a foreign power"" in 50 U.S.C. § 1801(b)(1)(C) by Section 6001(a) of P.L. 108-458.

intelligence sharing procedures submitted for approval with this motion."[3847] The court viewed the new intelligence sharing procedures under review as proposed new Attorney General minimization procedures. In a memorandum and order written by the then Presiding Judge, U.S. District Court Judge Royce Lamberth, issued on the last day of his tenure on the FISC, and concurred in by all of the judges then sitting on the FISC, the FISC granted the Department of Justice (DOJ) motion with significant modifications to section II.B. of what the FISC characterized as the proposed minimization procedures. The court required a continuation of the Attorney General's 1995 minimization procedures, as subsequently modified by the Attorney General and the Deputy Attorney General, and preservation of a "wall" procedure to maintain separation between FBI criminal investigators and DOJ prosecutors and raw FISA investigation data regarding the same facts or individuals, so as to prevent these law enforcement personnel from becoming "de facto partners in FISA surveillances and searches,"[3848] while permitting extensive sharing of information between such investigations.

The FISC was particularly concerned with those aspects of section II.B. of the proposed procedures which would permit criminal prosecutors and law enforcement officers to initiate, direct or control electronic surveillance or physical searches under FISA, with an eye towards law enforcement objectives, rather than foreign intelligence information gathering. The FISC set the stage for its analysis by recounting a significant number of past instances where FISA applications had included false, inaccurate or misleading information regarding information sharing or compliance with "wall" procedures in FBI affidavits or, in one case, in a statutorily required certification by the FBI Director; and past occasions where the FISC's orders had been violated in regard to information sharing and unauthorized dissemination of FISA information to criminal investigators and prosecutors. While both the FBI's and DOJ's Offices of Professional Responsibility had been investigating these incidents for over a year

---

[3847] In re All Matters Submitted to the Foreign Intelligence Surveillance Court, 218 F. Supp. 2d 611, 613 (U.S. Foreign Intell. Surveil. Ct. 2002). A copy of a March 6, 2002, Memorandum from the Attorney General to the Director, FBI; Assistant Attorney General, Criminal Division; Counsel for Intelligence Policy; and United States Attorneys entitled "Intelligence Sharing Procedures for Foreign Intelligence and Foreign Counterintelligence Investigations Conducted by the FBI " may be found at [http://fas.org/irp/agency/doj/fisa/ag030602.html].

[3848] *Id.* at 620. In Chapter 3 of The 9/11 Commission Report, Final Report of the National Commission on Terrorist Attacks Upon the United States 78-80 (W.W. Norton & Co. 2004) (Final Report), the Commission perceived the evolution of the "wall" as a result of statutory language, court interpretation, DOJ interpretation of the legislative language and court decisions, DOJ procedures to manage information sharing between Justice Department prosecutors and the FBI, misunderstanding and misapplication of those procedures, DOJ's Office of Intelligence Policy and Review's (OIPR) stringent exercise of its gate-keeping role, and inaccurate perceptions of field agents. In Chapter 8 of the Final Report, at 269-72, the Commission recounted some of the effects of what it saw as the confusion surrounding the rules governing the use and sharing of information gathered through intelligence channels.

at the time of the writing of the opinion, the court had not been advised of any explanations as to how such misrepresentations had occurred. The court's dissatisfaction with these irregularities formed a backdrop for its analysis of the motion and applications before it.

Discussion of the Memorandum Opinion and Order.

Its analysis was based upon its reading of the statutory language and premised, in part, on the fact that the USA PATRIOT Act had not amended the provisions of FISA dealing with minimization requirements, although other FISA provisions had been modified. The minimization provisions with respect to both electronic surveillance and physical searches under FISA continue to be designed to "minimize the acquisition and retention, and prohibit the dissemination, of non-publicly available information concerning unconsenting United States persons, consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information."[3849] The court regarded the standard it applied to the proposed procedures before it as "mandated in [50 U.S.C.] § 1805(a)(4) and § 1824(a)(4), which state that 'the proposed minimization procedures meet the definition of minimization procedures under § 101(h), [§ 1801(h) and §1824(4)] of the act.'"

In its memorandum opinion, the FISC first discussed the court's jurisdiction, noting that the text of the statute "leaves little doubt that the collection of foreign intelligence information is the raison d'etre for the FISA."[3850] The court found support for this conclusion in a review of pertinent provisions of the act. It found further support in E.O. 12139 and E.O. 12949, which give the Attorney General

---

[3849] 50 U.S.C. §§ 1802(h), 1821(4)(A) (emphasis added).

[3850] FISC op., 218 F. Supp. 2d at 613. "Foreign intelligence information" is a term of art in FISA, defined in 50 U.S.C. § 1801(e) to mean:

(e) (1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against —

(A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

(B) sabotage or international terrorism by a foreign power or an agent of a foreign power; or

(C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or

(2) information with respect to a foreign power or foreign territory that relates to, and if concerning a U.S. person is necessary to —

(A) the national defense or the security of the United States; or

(B) the conduct of the foreign affairs of the United States.

In reaching its decision, the FISC indicated that it was not addressing directly the Department of Justice argument that, so long as a significant purpose of a FISA surveillance or physical search was to gather foreign intelligence information, the primary purpose of such an investigation could be criminal investigation or prosecution. FISC op., 218 F. Supp. 2d at 615 n.2. The FISC was not receptive to the DOJ theory that a "wall" procedure separating a foreign intelligence investigation under FISA from a criminal investigation involving the same target or factual underpinnings was an artificial separation which was not compelled by FISA.

authority to approve the filing of applications for orders for electronic surveillances and physical searches and authorize the Director of the FBI and other senior executives to make required certifications under FISA for the "purpose of obtaining foreign intelligence information." The FISC therefore concluded that its jurisdiction was limited to granting FISA orders for electronic surveillance and physical searches for the collection of foreign intelligence information under the standards and procedures prescribed in the act.[3851] In reaching this conclusion, the FISC, in a footnote, characterized the issue before it as "whether the FISA authorizes electronic surveillance and physical searches primarily for law enforcement purposes so long as the Government also has 'a significant' foreign intelligence purpose." Rejecting the approach taken by the Government in its supplemental brief in the case, the Court stated that "its decision is not based on the issue of its jurisdiction but on the interpretation of minimization procedures."[3852] Maintaining its focus upon the minimization procedures, the FISC also declined to reach the question raised by the Attorney General "whether FISA may be used primarily for law enforcement purposes."[3853]

The court also regarded the scope of its findings regarding minimization[3854] as applicable "only to communications concerning U.S. persons as defined in §

[3851] FISC op., 218 F. Supp. 2d at 614.

[3852] *Id.* at 614 n.1(emphasis added).

[3853] *Id.* at 615 n.2.

[3854] FISA defines "minimization procedures" with respect to electronic surveillance in 50 U.S.C. § 1801(h). The term is defined under FISA with respect to physical searches in 50 U.S.C. § 1821(4). As the two definitions are similar, the definition from Section 1801(h) is included for illustrative purposes.

(h) "Minimization procedures", with respect to electronic surveillance, means —

(1) specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information;

(2) procedures that require that nonpublicly available information, which is not foreign intelligence information, as defined in subsection (e)(1) of this section, shall not be disseminated in a manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to understand foreign intelligence information or assess its importance;

(3) notwithstanding paragraphs (1) and (2), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes; and

(4) notwithstanding paragraphs (1), (2), and (3), with respect to any electronic surveillance approved pursuant to section (1802(a) of this title, procedures that require that no contents of any communication to which a United States person is a party shall be disclosed, disseminated, or used for any purpose or retained for longer than 72 hours unless a court order under section 1805 of this title is obtained or unless the Attorney General determines that the information indicates a threat of death or serious bodily harm to any person.

1801(i) of the act: U.S. citizens and permanent resident aliens whether or not they are named targets in the electronic surveillance and physical searches."[3855] It emphasized that its opinion was not applicable to communications of foreign powers as defined under 50 U.S.C. § 1801(a), or to non-U.S. persons.[3856]

After stating its continued approval of the "Standard Minimization Procedures for a U.S. Person Agent of a Foreign Power," the court turned its attention to two sections of supplementary minimization procedures adopted by the Attorney General on March 6, 2002, regarding "II. Intelligence sharing procedures concerning the Criminal Division," and "III. Intelligence sharing procedures concerning a USAO [U.S. Attorney's Office]." The FISC regarded these procedures as minimization procedures as that term is defined under FISA by virtue of the fact that they were adopted by the Attorney General and were "designed to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons."[3857] Therefore, these procedures were measured against the standard for minimization procedures set forth in 50 U.S.C. §§ 1805(a)(4) and 1824(a)(4):

> *... The operative language of each section to be applied by the Court provides that minimization procedures must be reasonably designed in light of their purpose and technique, and mean —*
>
> *specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular surveillance, [search] to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information. §1801(h)(1) and §1821(4)(A).*[3858]

The court then reviewed the minimization procedures upon which it had been relying prior to the application before it, to wit, the Attorney General's 1995

[3855] FISC op., 218 F. Supp. 2d at 614. This provision defines a "United States person" as follows:

... a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 1101(a)(20) of Title 8), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in subsection (a)(1), (2), or (3) of this section.

[3856] *Id.*

[3857] *Id.* at 616.

[3858] *Id.*

"Procedures for Contacts between the FBI and Criminal Division Concerning FI [Foreign Intelligence] and Foreign Counterintelligence Investigations," as augmented by the Attorney General in January 2000 and expanded further by the Deputy Attorney General in August 2001. The FISC indicated that these procedures permitted the following "substantial consultation and coordination":

a. reasonable indications of significant federal crimes in FISA cases are to be reported to the Criminal Division of the Department of Justice;
b. [t]he Criminal Division may then consult with the FBI and give guidance to the FBI aimed at preserving the option of criminal prosecution, but may not direct or control the FISA investigation toward law enforcement objectives;
c. the Criminal Division may consult further with the appropriate U.S. Attorney's Office about such FISA cases;
d. on a monthly basis senior officials of the FBI provide briefings to senior officials of the Justice Department, including OIPR [Office of Intelligence Policy and Review] and the Criminal Division, about intelligence cases, including those in which FISA is or may be used;
e. all FBI 90-day interim reports and annual reports of counterintelligence investigations, including FISA cases, are being provided to the Criminal Division, and must now contain a section explicitly identifying any possible federal criminal violations;
f. all requests for initiation or renewal of FISA authority must now contain a section devoted explicitly to identifying any possible federal criminal violations;
g. the FBI is to provide monthly briefings directly to the Criminal Division concerning all counterintelligence investigations in which there is a reasonable indication of a significant federal crime;
h. prior to each briefing the Criminal Division is to identify (from FBI reports) those intelligence investigations about which it requires additional information and the FBI is to provide the information requested; and
i. since September 11, 2001, the requirement that OIPR be present at all meetings and discussions between the FBI and Criminal Division involving certain FISA cases has been suspended; instead, OIPR reviews a daily briefing book to inform itself and this Court about those discussions.[3859]

The FISC indicated further that it "routinely approved the use of information screening 'walls' proposed by the government in its applications" to maintain both the appearance and the fact that FISA surveillances and searches were not being used "sub rosa for criminal investigations."[3860] In March 2000, September

---

[3859] *Id.* at 619-20 (emphasis supplied.)

[3860] *Id.* at 620.

2000, and March 2001, the FISC was advised by the Department of Justice of a significant number of erroneous statements or omissions of material facts in FISA applications, almost all of which involved misstatements or omissions as to information sharing and unauthorized disseminations to criminal investigators and prosecutors.[3861] Although the FBI and the Department of Justice Office of Professional Responsibility had been investigating the circumstances involved in these misstatements and omissions for over a year, as of the date of the opinion, the court had not been advised of the reasons for these erroneous statements. The court responded to these concerns in 2001 by instituting supervisory measures to assess compliance with "wall" procedures.

In the case before the FISC, the government moved that all "wall" procedures be eliminated in international terrorism surveillances and physical searches under FISA. The FISC indicated that the new 2002 procedures proposed by the Attorney General would apply to two types of cases in which "*FISA is the only effective tool available* to both counterintelligence and criminal investigators" (emphasis supplied) — those involving overlapping investigations (which the court described as cases, usually international terrorism cases, in which separate intelligence and criminal investigations of the same FISA target who is a U.S. person are conducted by different FBI agents, where separation can easily be maintained) and those involving overlapping interests (i.e., cases in which one investigation of a U.S. person FISA target is conducted by a team of FBI agents with both intelligence and criminal interests "usually involving espionage and similar cases in which separation is impractical").[3862] In both types of investigations, the FISC indicated that the 2002 proposed minimization procedures provided authority for "extensive consultations between the FBI and criminal prosecutors 'to coordinate efforts to investigate or protect against actual or potential attack, sabotage, international terrorism and clandestine intelligence activities by foreign powers and their agents....'" Such consultation is expressly provided for in 50 U.S.C. §§ 1806(k)(1) and 1825(k)(1).

Under the proposed minimization procedures, those consultations would include providing prosecutors with access to "all information" developed in FBI counterintelligence investigations, including through FISA, among other information. Section II.B. of the proposed minimization techniques would authorize criminal prosecutors to "consult extensively and provide advice and recommendations to intelligence officials about 'all issues necessary to the ability of the United States to investigate or protect against foreign attack, sabotage, terrorism, and clandestine intelligence activities.'" The FISC was particularly

---

[3861] The September 2000 notification to the FISC from the Department of Justice identified 75 cases of cases involving misstatements or omissions in FISA applications. The court does not indicate the specific number of FISA applications involved in the notifications on the other dates mentioned in the opinion. See FISC op., 218 F. Supp. 2d at 620-21.

[3862] FISC op., 218 F. Supp. 2d at 622.

concerned about the authority given criminal prosecutors under Section II.B. "to advise *FBI intelligence officials concerning 'the initiation, operation, continuation, or expansion of FISA searches or surveillance*.'"[3863] The court regarded this provision as "designed to use this Court's orders to enhance criminal investigation and prosecution, consistent with the government's interpretation of the recent amendments that FISA may now be 'used *primarily* for a law enforcement purpose.'"[3864] Under section III of the proposed procedures, U.S. attorneys are given the authority to engage in consultations to the same extent as the Criminal Division of DOJ under parts II.A. and II.B. in cases involving international terrorism. The FISC interpreted these procedures as giving criminal prosecutors "a significant role directing FISA surveillances and searches from start to finish in counterintelligence cases involving overlapping intelligence and criminal investigations or interests, guiding them to criminal prosecution."[3865]

In light of the court's past experience with FISA searches and surveillances, the FISC found the proposed procedures to be "designed to enhance the acquisition, retention and dissemination of *evidence for law enforcement purposes, instead* of being consistent with the need of the United States to 'obtain, produce, and disseminate *foreign intelligence information*' (emphasis added [by the FISC]) as mandated in § 1801(h) and § 1821(4)."[3866] The court regarded the procedures as, in effect, an effort by the government to amend FISA's definition of minimization procedures in ways that Congress had not and to substitute FISA for the electronic surveillance requirements of Title III of the Omnibus Crime Control and Safe Streets Act, 18 U.S.C. § 2510 et seq., and for the search warrant requirements in Rule 41 of the Federal Rules of Criminal Procedure. The court found this unacceptable. Nor was the court persuaded by the government's contention that the 1995 procedures' prohibition against criminal prosecutors "directing or controlling" FISA cases should be revoked. "If criminal prosecutors direct both the intelligence and criminal investigations, or a single investigation having combined interests, *coordination becomes subordination* of both investigations or interests to law enforcement objectives."[3867]

The FISC stated:

[3863] *Id.* at 623.

[3864] *Id.* (Emphasis added).

[3865] *Id.*

[3866] *Id.*

[3867] *Id.* at 623-24 (emphasis in original).

> *Advising FBI intelligence officials on the initiation, operation, continuation or expansion of FISA surveillances and searches of U.S. persons means that criminal prosecutors will tell the FBI when to use FISA (perhaps when they lack probable cause for a Title III electronic surveillance), what techniques to use, what information to look for, what information to keep as evidence and when use of FISA can cease because there is enough evidence to arrest and prosecute. The 2002 minimization procedures give the Department's criminal prosecutors every legal advantage conceived by Congress to be used by U.S. intelligence agencies to collect foreign intelligence information, ... based on a standard that the U.S. person is only using or about to use the places to be surveilled or searched, without any notice to the target unless arrested and prosecuted, and, if prosecuted, no adversarial discovery of the FISA applications and warrants. All of this may be done by use of procedures intended to minimize collection of U.S. person information, consistent with the need of the United States to obtain and produce foreign intelligence information. If direction of counterintelligence cases involving the use of highly intrusive FISA surveillances and searches by criminal prosecutors is necessary to obtain and produce foreign intelligence information, it is yet to be explained to the Court.*[3868]

Having found section II.B. of the proposed minimization procedures inconsistent with the statutory standard for minimization procedures under 50 U.S.C. §§ 1801(h) and 1821(4), the court substituted its own language in place of the second and third paragraphs of II.B. as submitted by the Attorney General. The substitute language permitted consultation between the FBI, the Criminal Division of DOJ, and the Office of Intelligence Policy and Review of DOJ (OIPR) "to coordinate their efforts to investigate or protect against foreign attack or other grave hostile acts, sabotage, international terrorism, or clandestine intelligence activities by foreign powers or [agents of foreign powers]," so that the goals and objectives of both the intelligence and law enforcement investigations or interests may be achieved. However, it prohibited law enforcement officials from making recommendations to intelligence officials regarding initiation, operation, continuation, or expansion of FISA surveillances and searches. In addition, the substitute language foreclosed law enforcement officials from directing or controlling the use of FISA procedures to enhance criminal prosecution; nor was advice intended to preserve the option of criminal prosecution to be permitted to inadvertently result in the Criminal Division directing or controlling an investigation involving FISA surveillance or physical searches to achieve law

---

[3868] *Id.* at 624.

enforcement objectives.[3869] While direct consultation and coordination were permitted, the substitute language required OIPR to be invited to all such consultations and, where OIPR was unable to attend, the language required OIPR to be apprized forthwith in writing of the substance of the consultations, so that the FISC could be notified at the earliest opportunity.[3870]

In its order accompanying the FISC memorandum opinion, the court held that the proposed minimization procedures, so modified, would be applicable to all future electronic surveillances and physical searches under FISA, subject to the approval of the court in each instance.[3871] In this order, the court also adopted a new administrative rule to monitor compliance. The new Rule 11 regarding criminal investigations in FISA cases provided:

> *All FISA applications shall include informative descriptions of any ongoing criminal investigations of FISA targets, as well as the substance of any consultations between the FBI and criminal prosecutors at the Department of Justice or a United States Attorney's Office.*[3872]

The Decision of the U.S. Foreign Intelligence Surveillance Court of Review

Summary

The FISC memorandum opinion and order discussed above were not appealed directly. Rather, the Department of Justice sought review in the U.S. Foreign Intelligence Surveillance Court of Review (Court of Review) of an FISC order which authorized electronic surveillance of an agent of a foreign power, but imposed restrictions on the government flowing from the FISC's May 17th decision, and of an order renewing that surveillance subject to the same restrictions. Because of the electronic surveillance context of these orders, the Court of Review's analysis was cast primarily in terms of such surveillance, although some aspects of its analysis may have broader application to other aspects of FISA. In its first decision ever, the Court of Review, in a lengthy per curiam opinion issued on November 18, 2002, reversed and remanded the FISC orders. In so doing the Court of Review emphasized that the May 17th decision, although never appealed, was "the basic decision before us and it [was] its

---

[3869] *Id.* at 625.

[3870] *Id.*

[3871] *Id.* at 627.

[3872] *Id.*

rationale that the government challenge[d]."[3873] After reviewing the briefs of the government and two amici curiae, the American Civil Liberties Union (joined on the brief by the Center for Democracy and Technology, the Center for National Security Studies, the Electronic Privacy Information Center, and the Electronic Frontier Foundation) and the National Association of Criminal Defense Lawyers, the Court of Review concluded that "FISA, as amended by the Patriot Act, supports the government's position, and that the restrictions imposed by the FISA court are not required by FISA or the Constitution."[3874]

Discussion of the Opinion

The Court of Review began its analysis by articulating its view of the May 17th FISC decision. The Court of Review stated that the FISC appeared to proceed in its opinion from the assumption that FISA constructed a barrier between counterintelligence/intelligence officials and law enforcement officers in the Executive Branch, but did not support that assumption with any relevant language from the statute.[3875] The Court of Review opined that this "wall" was implicit in the FISC's "apparent" belief that "it can approve applications for electronic surveillance only if the government's objective is not primarily directed toward criminal prosecution of the foreign agents for their foreign intelligence activity," while referencing neither statutory language in FISA nor USA PATRIOT Act amendments, which the government argued altered FISA to permit an application even if criminal prosecution was the primary goal.[3876] Instead, the Court of Review noted that the FISC relied upon its statutory authority to approve "minimization procedures" in imposing the restrictions at issue.

The Court of Review stated that the government raised two main arguments:
First, DOJ contended that the restriction, recognized by several courts of appeals[3877] prior to the enactment of the USA PATRIOT Act, that FISA could only

---

[3873] In re Sealed Case, 310 F.3d 717, 721 (U.S. Foreign Intell. Surveil. Ct. Rev. 2002) (hereinafter Court of Review op.).

[3874] *Id.* at 719-20.

[3875] *Id.* at 721.

[3876] *Id.*

[3877] The cases to which this appears to refer include decisions by both U.S. courts of appeals and U.S. district courts. Past cases considering the constitutional sufficiency of FISA in the context of electronic surveillance have rejected Fourth Amendment challenges and due process challenges under the Fifth Amendment to the use of information gleaned from a FISA electronic surveillance in a subsequent criminal prosecution, because the purpose of the FISA electronic surveillance, both initially and throughout the surveillance, was to secure foreign intelligence information and not primarily oriented towards criminal investigation or prosecution, United States v. Megahey, 553 F. Supp. 1180, 1185-1193 (D.N.Y.), aff'd without opinion, 729 F.2d 1444 (2d Cir. 1982), re-aff'd post-trial sub nom United States v. Duggan, 743 F.2d 59 (2d Cir. 1984); United States v. Ott, 827 F.2d 473, 475 (9th Cir. 1987); United States. v Badia, 827 F. 2d 1458, 1464 (11th Cir. 1987). See also, United States v. Johnson, 952 F.2d 565, 572 (1st Cir. 1991), rehearing and cert. denied,

506 U.S. 816 (1991) (holding that, although evidence obtained in FISA electronic surveillance may later be used in a criminal prosecution, criminal investigation may not be the primary purpose of the surveillance, and FISA may not be used as an end-run around the 4th Amendment); United States v. Pelton, 835 F.2d 1067, 1074-76 (4th Cir. 1987), cert. denied, 486 U.S.1010 (1987) (holding that electronic surveillance under FISA passed constitutional muster where the primary purpose of surveillance, initially and throughout surveillance, was gathering of foreign intelligence information; also held that an otherwise valid FISA surveillance was not invalidated because later use of the fruits of the surveillance in criminal prosecution could be anticipated. In addition, the court rejected Pelton's challenge to FISA on the ground that allowing any electronic surveillance on less than the traditional probable cause standard — i.e. probable cause to believe the suspect has committed, is committing, or is about to commit a crime for which electronic surveillance is permitted, and that the interception will obtain communications concerning that offense — for issuance of a search warrant was violative of the Fourth Amendment, finding FISA's provisions to be reasonable both in relation to the legitimate need of Government for foreign intelligence information and the protected rights of U.S. citizens); United States v. Cavanaugh, 807 F.2d 787, 790-91 (9th Cir. 1987) (defendant, convicted of espionage, appealed district court's refusal to suppress fruits of FISA electronic surveillance which intercepted defendant offering to sell defense secrets to representatives of Soviet Union. In affirming conviction, appellate court found FISA procedures had been followed, and upheld FISA against constitutional challenges. Court found, in part, that FISA probable cause requirement was reasonable under Fourth Amendment standard. "The application must state that the target of the electronic surveillance is a foreign power or an agent of a foreign power, and must certify that the purpose of the surveillance is to obtain foreign intelligence information and that the information cannot reasonably be obtained by normal investigative techniques. 50 U.S.C. § 1804(a). It is true, as appellant points out in his brief, that the application need not state that the surveillance is likely to uncover evidence of a crime; but as the purpose of the surveillance is not to ferret out criminal activity but rather to gather intelligence, such a requirement would be illogical. See United States District Court, 407 U.S. at 322 (recognizing distinction between surveillance for national security purposes and surveillance of 'ordinary crime'); ... And ... there is no merit to the contention that he is entitled to suppression simply because evidence of his criminal conduct was discovered incidentally as the result of an intelligence surveillance not supported by probable cause of criminal activity. See Duggan, 743 F.2d at 73n.5.") United States v. Rahman, 861 F. Supp. 247, 251 (S.D. N.Y. 1994). Cf., United States v. Bin Laden, 2001 U.S. Dist. LEXIS 15484 (S.D. N.Y., October 2, 2001); United States v. Bin Laden, 126 F. Supp. 264, 277-78 (S.D. N.Y. 2000) (adopting foreign intelligence exception to the warrant requirement for searches targeting foreign powers or agents of foreign powers abroad; noting that this "exception to the warrant requirement applies until and unless the primary purpose of the searches stops being foreign intelligence collection.... If foreign intelligence collection is merely a purpose and not the primary purpose of a search, the exception does not apply.")

Cf., United States v. Sarkissian, 841 F.2d 959, 964-65 (9th Cir. 1988) (FISA court order authorized electronic surveillance, which resulted in the discovery of plan to bomb the Honorary Turkish Consulate in Philadelphia, and of the fact that bomb components were being transported by plane from Los Angeles. The FBI identified likely airlines, flight plans, anticipated time of arrival, and suspected courier. Shortly before the arrival of a flight fitting these parameters, the investigation focused upon an individual anticipated to be a passenger on that flight. An undercover police officer spotted a man matching the suspected courier's description on that flight. The luggage from that flight was sniffed by a trained dog and x-rayed. A warrantless search was conducted of a suitcase that had been shown by x-ray to contain an unassembled bomb. Defendants unsuccessfully moved to suppress the evidence from the FISA wiretap and the warrantless search. On appeal the court upheld the warrantless suitcase search as supported by exigent circumstances. Defendants contended that the FBI's primary purpose for the surveillance had shifted at the time of the wiretap from an intelligence investigation to a criminal investigation

be used if the government's primary purpose in gathering foreign intelligence information was not criminal prosecution, was not supported by the statutory language or the legislative history of FISA. This argument was not presented to the FISC, but the Court of Review indicated that it could entertain the argument, because proceedings before the FISC and before the Court of Review were *ex parte*.[3878] Second, the government argued that, even if the primary purpose test was appropriate prior to the passage of the USA PATRIOT Act, the amendments made by that act eliminated that concept. The government also argued that the FISC's interpretation of the minimization procedures provisions misconstrued those provisions and amounted to "an end run" around the USA PATRIOT Act amendments. DOJ argued further that the FISC minimization procedures so intruded into the Department's operations as to be beyond the constitutional

---

and that court approval for the wiretap therefore should have been sought under Title III of the Omnibus Crime Control and Safe Streets Act, 18 U.S.C. § 2510 et seq., rather than FISA. The court, while noting that in other cases it had state that "the purpose of [electronic] surveillance" under FISA "must be to secure foreign intelligence information," "not to ferret out criminal activity;" declined to decide the issue of whether the applicable standard was that "the purpose" or that "the primary purpose" of a FISA surveillance must be gathering of foreign intelligence information. The court stated, "Regardless of whether the test is one of purpose or primary purpose, our review of the government's FISA materials convinces us that it is met in this case.... We refuse to draw too fine a distinction between criminal and intelligence investigations. "International terrorism," by definition, requires the investigation of activities that constitute crimes. 50 U.S.C. § 1806(f). That the government may later choose to prosecute is irrelevant. FISA contemplates prosecution based on evidence gathered through surveillance.... "Surveillances ... need not stop once conclusive evidence of a crime is obtained, but instead may be extended longer where protective measures other than arrest and prosecution are more appropriate." S. Rep. No. 701, 95th Cong., 1st Sess. 11 ... [(1978)].... FISA is meant to take into account "the differences between ordinary criminal investigations to gather evidence of specific crimes and foreign counterintelligence investigations to uncover and monitor clandestine activities ..." *Id.* .... At no point was this case an ordinary criminal investigation."). Cf., United States v. Falvey, 540 F. Supp. 1306 (E.D.N.Y. 1982) (distinguishing United States v. Truong Dinh Hung, 629 F.2d 908, 912-13 (4th Cir. 1980); and United States v. Butenko, 494 F.2d 593, 606 (3d Cir.) (en banc), cert. denied sub nom, Ivanov v. United States, 419 U.S. 881 (1974), which held that, while warrantless electronic surveillance for foreign intelligence purposes was permissible, when the purpose or primary purpose of the surveillance is to obtain evidence of criminal activity, evidence obtained by warrantless electronic surveillance is inadmissible at trial, 540 F. Supp. at 1313. In addressing the theory that the evidence in the case before it was obtained pursuant to a warrant, a lawfully obtained court order under FISA, id. at 1314, the court observed that the "bottom line of Truong is that evidence derived from warrantless foreign intelligence searches will be admissible in a criminal proceeding only so long as the primary purpose of the surveillance is to obtain foreign intelligence information." *Id.* at 1313-14. After noting that Congress, in enacting FISA, "expected that evidence derived from FISA surveillances could then be used in a criminal proceeding," the court concluded that "it was proper for the FISA judge to issue the order in this case because of the on-going nature of the foreign intelligence investigation.... The fact that evidence of criminal activity was thereafter uncovered during the investigation does not render the evidence inadmissible. There is no question in [the court's] mind that the purpose of the surveillance, pursuant to the order, was the acquisition of foreign intelligence information. Accordingly, [the court found] that the FISA procedures on their face satisfy the Fourth Amendment warrant requirement, and that FISA was properly implemented in this case." *Id.* at 1314.).

[3878] Court of Review op., 310 F.3d at 722 n.6.

authority of Article III judges. Finally, DOJ contended that application of the primary purpose test in a FISA case was not constitutionally compelled under the Fourth Amendment.

The Court of Review noted that, as enacted in 1978, FISA authorized the grant of an application for electronic surveillance to obtain foreign intelligence information if there is probable cause to believe that "the target of the electronic surveillance is a foreign power or an agent of a foreign power,"[3879] and that "each of the facilities or places at which the surveillance is directed is being used, or is about to be used by a foreign power or an agent of a foreign power."[3880] The reviewing court focused upon the close connection between criminal activity and the definitions of "agent of a foreign power" applicable to United States persons contained in 50 U.S.C. §§ 1801(b)(2)(A) and (C), to wit: "any person who 'knowingly engages in clandestine intelligence activities ... which activities involve or may involve a violation of the *criminal statutes* of the United States,' or 'knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor.'"[3881] The court noted further that FISA defined "international terrorism" to mean "activities that 'involve violent acts or acts dangerous to human life that are a violation of the *criminal laws* of the United States or of any State, or that would be a *criminal violation* if committed within

---

[3879] The Court of Review did not include in its quotation of 50 U.S.C. § 1805(a)(3)(A) the proviso that follows the quoted language: "Provided, That no United States person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States."

[3880] Court of Review op., 310 F.3d at 722, quoting portions of 50 U.S.C. § 1805(a)(3).

[3881] *Id.* at 723 (emphasis added by the Court of Review). The definitions of "agent of a foreign power" which apply to "any person" (including, by implication, United States persons) are set forth in 50 U.S.C. § 1801(b)(2). This subsection now contains five subparagraphs:

(b)
"Agent of a foreign power" means — ...
(2) any person who —
(A) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States;
(B) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States;
(C) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power;
(D) knowingly enters the United States under a false or fraudulent identity for or on behalf of a foreign power, or, while in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power; or

(E) knowingly aids or abets any person in the conduct of activities described in subparagraph (A), (B), or (C) or knowingly conspires with any person to engage in activities described in subparagraph (A), (B), or (C). The current subparagraph (D) was added in 1999, and the former subparagraph (D) was redesignated subparagraph (E).

the jurisdiction of the United States or any State.'"[3882] "Sabotage," as defined by FISA, covers activities that "'involve a violation of chapter 105 of [the criminal code] [18 U.S.C. §§ 2151-2156], or that would involve such a violation if committed against the United States.'"[3883] For purposes of its opinion, the Court of Review described these types of crimes as "foreign intelligence crimes."[3884]

[3882] *Id.* at 723, quoting 50 U.S.C. § 1801(c)(1) (emphasis added by the Court of Review). The remainder of the definition of "international terrorism" under 50 U.S.C. § 1801(c)(2) and (3) adds two more criteria for activities to be considered to be within this definition: (c) "International terrorism" means activities that — ...
(2) appear to be intended —
(A) to intimidate or coerce a civilian population;
(B) to influence the policy of a government by intimidation or coercion; or
(C) to affect the conduct of a government by assassination or kidnapping; and

(3) occur totally outside the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum.

[3883] Court of Review slip op. at 10, quoting 50 U.S.C. § 1801(d).

[3884] Although later acknowledging the possibility that the Justice Department had accepted the dichotomy between foreign intelligence gathering and law enforcement purposes "in an effort to conform to district court holdings," Court of Review op., 310 F.3d at 727, (most of the published decisions were court of appeals decisions rather than district court decisions) the Court of Review expressed puzzlement that "the Justice Department, at some point during the 1980's, began to read the statute as limiting the Department's ability to obtain FISA orders if it intended to prosecute the targeted agents — even for foreign intelligence crimes," while noting that 50 U.S.C. § 1804 at the time required that "a national security official in the Executive Branch — typically the Director of the FBI — ... certify that 'the purpose' of the surveillance was to obtain foreign intelligence information (amended by the Patriot Act to read 'a significant purpose.')" *Id.* at 723. The court did, however, discuss a series of 1982-1991 cases upholding the constitutional sufficiency of electronic surveillance under FISA as long as "the primary purpose" of the surveillance was gathering foreign intelligence information, rather than criminal prosecution. If foreign intelligence gathering was the primary purpose of a FISA electronic surveillance, initially and throughout the surveillance, and FISA was not being used as "an end run around the 4th Amendment," the courts permitted use of the fruits of the surveillance in subsequent criminal prosecutions. See the discussion of these cases at fn. 156, supra, of this report. This "primary purpose" approach to these FISA cases appears consistent with the "primary purpose" approach taken in a number of pre-FISA cases involving Fourth Amendment challenges to warrantless foreign intelligence surveillances. See constitutional analyses in United States v. Brown, 484 F.2d 418 (5th Cir. 1973), cert. denied, 415 U.S. 960 (5th Cir. 1974); United States v. Butenko, 494 F.2d 593 (3rd Cir. 1974) , cert. denied sub nom, Ivanov v. United States, 419 U.S. 881 (1974), and Zweibon v. Mitchell, 516 F.2d 594 (D.C. Cir. 1975), cert. denied, 425 U.S. 944 (1976); along with the Supreme Court's analysis, in a domestic surveillance context, in the Keith case, United States v. United States District Court, 407 U.S. 297 (1972), discussed in the "Background" section of this report, supra. The Court of Review appears to discount the significance of these decisions because the courts involved upheld lower court decisions permitting admission of information gathered under FISA in criminal trials. The Court of Review stated, "It may well be that the government itself, in an effort to conform to district court holdings, accepted the dichotomy it now contends is false. Be that as it may, since the cases that "adopt" the dichotomy do affirm district court opinions permitting the introduction of evidence gathered under a FISA order, there was not much need for the courts to focus on the opinion with which we are confronted." Court of Review op., 310 F.3d at 727.

The court observed that, as passed in 1978, 50 U.S.C. §1804 required a national security official of the Executive Branch, usually the FBI Director,[3885] to certify that "the purpose" of the electronic surveillance under FISA was to obtain foreign intelligence information, and opined that "it is virtually impossible to read the 1978 FISA to exclude from its purpose the prosecution of foreign intelligence crimes, most importantly because, as we have noted, the definition of an agent of a foreign power — if he or she is a U.S. person — is grounded on criminal conduct."[3886] It found further support for its view that "foreign intelligence information" included evidence of "foreign intelligence crimes" from the legislative history as reflected in H.Rept. 95-1283 and S.Rept. 95-701,[3887] while acknowledging that the House report also stated that FISA surveillances "are not primarily for the purpose of gathering evidence of a crime. They are to obtain foreign intelligence information, which when it concerns United States persons must be necessary to important national concerns."[3888] The Court of Review regarded the latter statement as an observation rather than a proscription.[3889]

The Court of Review saw the U.S. Court of Appeals for the Fourth Circuit's decision in *United States v. Truong Dinh Hung*, 629 F.2d 908 (4th Cir. 1980), a decision based upon constitutional analysis rather than FISA provisions, as the springboard for the "primary purpose" test cases interpreting FISA and

---

[3885] The pertinent language of 50 U.S.C. § 1804(a)(7) as passed in 1978 provided that each application for an order authorizing electronic surveillance under FISA shall include:
(7) a certification or certifications by the Assistant to the President for National Security Affairs or an executive branch official or officials designated by the President from those executive officers employed in the area of national security or defense and appointed by the President with the advice and consent of the Senate —
(A) that the certifying official deems the information sought to be foreign intelligence information;
(B) that the purpose of the surveillance is to obtain foreign intelligence information;
(C) that such information cannot reasonably be obtained by normal investigative techniques;
(D) that designates the type of foreign intelligence information being sought according to the categories described in section 1801(e) of this title; and
(E) including a statement of the basis for the certification that —
(i) the information sought is the type of foreign intelligence information designated; and

(ii) such information cannot reasonably be obtained by normal investigative techniques[.] Under 50 U.S.C. § 1804(d) as passed in 1978 and under current law, "The judge may require the applicant to furnish such other information as may be necessary to make the determinations required by section 1805 of this title."

[3886] Court of Review op., 310 F.3d at 723.

[3887] *Id.* at 724-25, citing H.Rept. 95-1283, at 49 (1978) and S.Rept. 95-701, at 10-11 (1978).

[3888] H.Rept. 95-1283, at 36 (1978).

[3889] Court of Review op., 310 F.3d at 725.

upholding FISA surveillances against Fourth Amendment challenges.[3890] After reviewing a number of the FISA cases applying the primary purpose test, the Court of Review concluded that a dichotomy between foreign intelligence gathering and criminal investigations implicit in the application of the primary purpose test was not statutorily compelled. The court found that FISA, as originally passed, did not "preclude or limit the government's use or proposed use of foreign intelligence information, which included evidence of certain kinds of criminal activity, in a criminal prosecution."[3891] In addition, the Court of Review, relying on arguments of the Department of Justice and the language of subsection 1805(a)(5), interpreted 50 U.S.C. §§ 1805 of FISA as originally enacted as not contemplating that the [FISC] would inquire into the government's purpose in seeking foreign intelligence information.[3892]

Further, the court rejected the FISC's characterization of the AttorneyGeneral's 1995 procedures, as modified and augmented in January 2000 and August 2001, as minimization procedures. These procedures were formally adopted by the FISC as minimization procedures defined in 50 U.S.C. §§ 1801(h) and 1821(4) in November 2001, after passage of the USA PATRIOT Act, and were incorporated in all applicable orders and warrants granted since their adoption by the FISC. On March 6, 2002, the Attorney General adopted new "Intelligence Sharing

---

[3890] Although Truong Dinh Hung was among the cases cited by some of the subsequent FISA cases, a "primary purpose" test had been previously applied in the 1974 Third Circuit decision in Butenko, supra, upholding a warrantless electronic surveillance in the face of challenges based upon the Fourth Amendment and Section 605 of the Communications Act where the primary purpose of the investigation was gathering foreign intelligence information. See discussion in the "Background" section of this report, supra, as well as the summary of this and other cases at fns. 156 and 163, *supra*.

[3891] Court of Review op., 310 F.3d at 727.

[3892] *Id.* at 723-24, 728. Section 1805(a), as enacted in 1978, set forth the necessary findings that a judge of the FISC had to make in order to enter an ex parte order as requested or as modified approving electronic surveillance under FISA:

(1) the President has authorized the Attorney General to approve applications for electronic surveillance for foreign intelligence information;

(2) the application has been made by a Federal officer and approved by the Attorney General;

(3) on the basis of the facts submitted by the applicant there is probable cause to believe that —

(A) the target of the electronic surveillance is a foreign power or an agent of a foreign power: Provided, That no United States person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States; and

(B) each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power;

(4) the proposed minimization procedures meet the definition of minimization procedures under section 1801(h) of this title;

(5) the application which has been filed contains all statements and certifications required by section 1804 of this title and, if the target is a United States person, the certification or certifications are not clearly erroneous on the basis of the statement made under section 1804(a)(7)(E) of this title and any other information furnished under section 1804(d) of this title.

Procedures," intended to supercede prior procedures, to "allow complete exchange of information and advice between intelligence and law enforcement officials," to "eliminate the 'direction and control' test," and to permit "exchange of advice between the FBI, OIPR, and the Criminal Division regarding 'the initiation, operation, continuation, or expansion of FISA searches or surveillance."[3893] The following day, the government filed a motion with the FISC advising the court of the Attorney General's adoption of the 2002 procedures, seeking to have that court adopt the new procedures in all matters before the FISC and asking the court to vacate its orders adopting the prior procedures as minimization procedures and imposing "wall" procedures in certain types of cases. That motion led to the FISC decision to adopt the 2002 procedures with modifications that was, by reference, before the Court of Review in its November 18, 2002, decision.

The Court of Review characterized the FISC's adoption of the Justice Department's 1995 procedures, as modified and augmented, as minimization procedures as follows:

> *Essentially, the FISA court took portions of the Attorney General's augmented 1995 Procedures — adopted to deal with the primary purpose standard — and imposed them generically as minimization procedures. In doing so, the FISA court erred. It did not provide any constitutional basis for its action — we think there is none — and misconstrued the main statutory provision on which it relied. The court mistakenly categorized the augmented 1995 Procedures as FISA minimization procedures and then compelled the government to utilize a modified version of those procedures in a way that is clearly inconsistent with the statutory purpose.*[3894]

The Court of Review interpreted "minimization procedures" under 50 U.S.C. § 1801(h) to be designed to protect, as far as reasonable, against the acquisition, retention, and dissemination of nonpublic information which is not foreign intelligence information. In light of the Court of Review's interpretation of "minimization procedures" under 50 U.S.C. § 1801(h), the court found no basis for the FISC's reliance upon that section "to limit criminal prosecutors' ability to advise FBI intelligence officials on the initiation, operation, continuation, or expansion of FISA surveillances to obtain foreign intelligence information, even if such information includes evidence of a foreign intelligence crime."[3895]

[3893] Court of Review op., 310 F.3d at 729.

[3894] *Id.* at 730.

[3895] *Id.* at 731.

In addition, the Court of Review found that the FISC had misconstrued its authority under 50 U.S.C. § 1805 and misinterpreted the definition of minimization procedures under 50 U.S.C. § 1801(h). The Court of Review expressed approbation for the Government's argument that the FISC, in imposing the modified 1995 procedures upon the Department of Justice as minimization procedures, "may well have exceeded the constitutional bounds that restrict an Article III court. The FISA court asserted authority to govern the internal organization and investigative procedures of the Department of Justice which are the province of the Executive Branch (Article II) and the Congress (Article I)."[3896]

The Court of Review deemed the FISC's "refusal ... to consider the legal significance of the Patriot Act's crucial amendments [to be] error."[3897] The appellate court noted that, as amended by the USA PATRIOT Act, the requirement in 50 U.S.C. § 1804(a)(7)(B) that the Executive Branch officer certify that "the purpose" of the FISA surveillance or physical search was to gather foreign intelligence information had been changed to "a significant purpose."[3898] The court noted that floor statements indicated that this would break down traditional barriers between law enforcement and foreign intelligence gathering,[3899] making it easier for law enforcement to obtain FISA court orders for surveillance or physical searches where the subject of the surveillance "is both a potential source of valuable intelligence and the potential target of a criminal prosecution."[3900] The court noted that some Members raised concerns about the Fourth Amendment implications of this language change which permitted the Government to obtain a court order under FISA "even if the primary purpose is a criminal investigation."[3901] Interestingly, although the Court of Review did not regard a dichotomy between foreign intelligence gathering and law enforcement

---

[3896] *Id.* at 731-32.

[3897] *Id.* at 732.

[3898] *Id.* at 728-29, 732-33.

[3899] *Id.* at 732, quoting Sen. Leahy, 147 Cong. Rec. S10992 (Oct. 25, 2001).

[3900] *Id.* at 733, quoting Sen. Feinstein, 147 Cong. Rec. S10591 (Oct. 11, 2001). In Section 13.5 of Chapter 13 of its Final Report, at 424, the 9/11 Commission, in discussing the future role of the FBI, observes in part: Counterterrorism investigations in the United States very quickly become matters that involve violations of criminal law and possible law enforcement action. Because the FBI can have agents working criminal matters and agents working intelligence investigations concerning the same international terrorism target, the full range of investigative tools against a suspected terrorist can be considered within one agency. The removal of the "wall" that existed before 9/11 between intelligence and law enforcement has opened up new opportunities for cooperative action within the FBI.

[3901] Court of Review op., 310 F.3d at 733, quoting Sen. Feingold, 147 Cong. Rec. S11021 (Oct. 25, 2001).

purposes as necessarily implied by the 1978 version of 50 U.S.C. § 1804(a)(7)(B), the court viewed the statutory change from "the purpose" to "a significant purpose" in the USA PATRIOT Act as recognizing such a dichotomy.[3902] The Court of Review disagreed with the FISC interpretation of the consultation authority under 50 U.S.C. § 1806(k).[3903] The Court of Review saw this provision as one which reflected the elimination of barriers between law enforcement and intelligence or counterintelligence gathering, without a limitation on law enforcement officers directing or controlling FISA surveillances. "[W]hen Congress explicitly authorizes consultation and coordination between different offices in the government, without even suggesting a limitation on who is to direct and control, it necessarily implies that either could take the lead."[3904]

In analyzing the "significant purpose" amendment to 50 U.S.C. § 1804(a)(7)(B), the Court of Review deemed this a clear rejection of the primary purpose test. If gathering foreign intelligence information is a significant purpose, another purpose such as criminal prosecution could be primary.[3905] Further, the court found that the term "significant" "imposed a requirement that the government have a measurable foreign intelligence purpose, other than just criminal prosecution of even foreign intelligence crimes.... Although section 1805(a)(5) ... may well have been intended to authorize the FISA court to review only the question whether the information sought was a type of foreign intelligence information, in light of the significant purpose amendment of section 1804, it seems section 1805 must be interpreted as giving the FISA court the authority to review the government's purpose in seeking the information."[3906] The Court of Review saw the "significant purpose" language as "excluding from the purpose of gaining foreign intelligence information a sole objective of criminal prosecution."[3907] If the government, at the commencement of a FISA surveillance has not yet determined whether to prosecute the target, "[s]o long as the government entertains a realistic option of dealing with the agent other than through criminal prosecution, it satisfies the significant purpose test."[3908] Under the Court of Review's analysis:

[3902] *Id.* at 734-35.

[3903] *Id.* at 733-34.

[3904] *Id.* at 734.

[3905] *Id.* at 734.

[3906] *Id.* at 735.

[3907] *Id.*

[3908] *Id.*

> *If the certification of the application's purpose articulates a broader objective than criminal prosecution — such as stopping an ongoing conspiracy — and includes other potential non-prosecutorial responses, the government meets the statutory test. Of course, if the court concluded that the government's sole objective was merely to gain evidence of past criminal conduct — even foreign intelligence crimes — to punish the agent rather than halt ongoing espionage or terrorist activity, the application should be denied.*[3909]

The court stated further that, while ordinary crimes may be intertwined with foreign intelligence crimes, the FISA process may not be utilized to investigate wholly unrelated ordinary crimes.[3910] The Court of Review emphasized that the government's purpose as reflected in the Section 1804(a)(7)(B) certification is to be judged by the FISC on the basis of

> *...the national security officer's articulation and not by a FISA court inquiry into the origins of an investigation nor an examination of the personnel involved. It is up to the Director of the FBI, who typically certifies, to determine the government's national security purpose, as approved by the Attorney General or Deputy Attorney General.... That means, perforce, if the FISA court has reason to doubt that the government has any real non-prosecutorial purpose in seeking foreign intelligence information it can demand further inquiry into the certifying officer's purpose — or perhaps even the Attorney General's or Deputy Attorney General's reasons for approval. The important point is that the relevant purpose is that of those senior officials in the Executive Branch who have the responsibility of appraising the government's national security needs."*[3911]

Turning from its statutory analysis to its examination of whether the statute, as amended, satisfied Fourth Amendment parameters, the Court of Review compared the FISA procedures with those applicable to criminal investigations of "ordinary crimes" under Supreme Court jurisprudence and under the wiretap provisions of Title III of the Omnibus Crime Control and Safe Streets Act. Relying upon *Dalia v. United States*, 441 U.S. 238, 255 (1979), the court indicated that in criminal investigations, beyond requiring that searches and seizures be reasonable, the Supreme Court has interpreted the Fourth Amendment's warrant requirement to demand satisfaction of three criteria: a warrant must be issued by

---

[3909] *Id.*

[3910] *Id.* at 736.

[3911] *Id.*

a neutral, detached magistrate; those seeking the warrant must demonstrate to the magistrate that there is probable cause to believe that the evidence sought will assist in a particular apprehension or conviction for a particular offense; and the warrant must describe with particularity the things to be seized and the place to be searched.[3912]

The Court of Review compared the procedures in Title III with those in FISA, finding in some respects that Title III had higher standards, while in others FISA included additional safeguards. In both, there was provision for a detached, neutral magistrate. The probable cause standard in Title III for criminal investigations was deemed more demanding than that in FISA. Title III requires a showing of probable cause that a specific individual has committed, is committing, or is about to commit a particular criminal offense. FISA requires a showing of probable cause that the target of the FISA investigative technique is a foreign power or an agent of a foreign power. A foreign power is not defined solely in terms of criminal activity. In the case of a target who is a U.S. person, the definition of "agent of a foreign power" contemplates, in part, the involvement of or, in the case of clandestine intelligence activities for a foreign power, the possibility of criminal conduct. The court regarded the lesser requirement with respect to criminal activity in the context of clandestine intelligence activities as to some extent balanced by the safeguard provided by FISA's requirement that there be probable cause to believe that the target is acting "for or on behalf of a foreign power."[3913]

With regard to the particularity requirement, as to the first element, Title III requires a finding of probable cause to believe that the interception will obtain particular communications regarding a specified crime. In contrast, FISA requires an official to designate the type of foreign intelligence information being sought and to certify that the information being sought is foreign intelligence information. When the target of the FISA investigation is a U.S. person, the standard of review applied by the FISC is whether there is clear error in the certification, a lower standard that a judicial finding of probable cause. While the FISC can demand that the government provide further information needed for the court to make its determination as to whether the certification is clearly erroneous, the statute relies also upon internal checks on Executive Branch decisions through the requirement that the certification must be made by a national security officer and approved by the Attorney General or Deputy Attorney General.

In connection with the second particularity element, Title III

[3912] *Id.* at 738.

[3913] *Id.* at 738-39.

> *... requires probable cause to believe that the facilities subject to surveillance are being used or are about to be used in connection with commission of a crime or are leased to, listed in the name of, or used by the individual committing the crime, 18 U.S.C. § 2518(3)(d), [while] FISA requires probable cause to believe that each of the facilities or places at which the surveillance is directed is being used, or is about to be used by a foreign power or agent [of a foreign power]. 50 U.S.C. § 1805(a)(3)(B). ... Simply put, FISA requires less of a nexus between the facility and the pertinent communications that Title III, but more of a nexus between the target and the pertinent communications."*[3914]

The Court of Review also compared Title III to FISA with respect to necessity (both statutes require that the information sought is not available through normal investigative procedures, although the standards differ somewhat),[3915] duration of surveillance (30 days under Title III, 18 U.S.C. § 2518(3)(c), as opposed to 90 days under FISA for U.S. persons, 50 U.S.C. § 1805(e)(1)),[3916] minimization and notice.

With respect to minimization, the Court of Review noted that Title III, under 18 U.S.C. § 2518(5), required minimization of what was acquired, directing that surveillance be carried out "in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter." FISA, on the other hand, "requires minimization of what is acquired, retained, and

---

[3914] *Id.* at 740.

[3915] For electronic surveillance to be approved, Title III requires a judicial finding that normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous. 18 U.S.C. § 2518(3)(c). FISA requires certification by the national security officer involved that the foreign intelligence information sought cannot reasonably be obtained by normal investigative means. 50 U.S.C. § 1804(a)(7)(C). The certification must include a statement of the basis for the certification that the information sought is the type of foreign intelligence information designated; and that such information cannot reasonably be obtained by normal investigative techniques. 50 U.S.C. § 1804(a)(7)(E)(i) and (ii). In issuing an ex parte order granting an application for electronic surveillance, the FISC judge must find that, in the case of a target who is a U.S. person, the certifications are not clearly erroneous on the basis of the statement made under 50 U.S.C. § 1804(a)(7)(e) and any other information furnished under Section 1804(d). Thus, the relevant findings to be made by the courts under the two statutes differ.

[3916] Court of Review op., 310 F.3d at 740. The difference, in the court's view, was "based on the nature of national security surveillance, which is 'often long range and involves the interrelation of various sources and types of information.' Keith, 407 U.S. at 322; see also S. Rep. at 16, 56." The court also noted that in FISA the "longer surveillance period is balanced by continuing FISA court oversight of minimization procedures during that period. 50 U.S.C. § 1805(e)(3); see also S. Rep. at 56."

disseminated."[3917] Observing that the FISC had found "in practice FISA surveillance devices are normally left on continuously, and the minimization occurs in the process of indexing and logging the pertinent communications," the Court of Review deemed the reasonableness of such an approach to be dependent upon the facts and circumstances of each case:[3918]

> *Less minimization in the acquisition stage may well be justified to the extent the intercepted communications are "ambiguous in nature or apparently involve[] guarded or coded language," or "the investigation is focusing on what is thought to be a widespread conspiracy [where] more extensive surveillance may be justified in an attempt to determine the precise scope of the enterprise." ... Given the targets of FISA surveillance, it will often be the case that intercepted communications will be in code or a foreign language for which there is no contemporaneously available translator, and the activities of foreign agents will involve multiple actors and complex plots....*[3919]

With respect to notice, the Court of Review observed that under 18 U.S.C. § 2518(8)(d), Title III mandated notice to the target of the surveillance and, in the judge's discretion, to other persons whose communications were intercepted, after the surveillance has expired. In contrast, under 50 U.S.C. § 1806(c) and (d), FISA does not require notice to a person whose communications were intercepted unless the government intends to use, disclose, or enter into evidence those communications or derivative information in a trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other federal, state or local authority against that person. The Court of Review noted that where such information was to be used against a criminal defendant, he or she would be given notice, and stated that "where such evidence is not ultimately going to be used for law enforcement," Congress had observed that "[t]he need to preserve secrecy for sensitive counterintelligence sources and methods justifies elimination of the notice requirement."[3920] In a footnote, the court noted that the Amici had drawn attention to the difference in the nature of the notice given the defendant or aggrieved person under Title III as opposed to FISA. Under Title III, a defendant is generally entitled under 18 U.S.C. § 2518(9) to obtain the application and order to challenge the legality of the surveillance. However, under FISA, the government must give the aggrieved person and the court or other authority (or in the case of a state or local use, the state or political

---

[3917] *Id.*

[3918] *Id.*

[3919] *Id.* at 740-41.

[3920] *Id.* at 741, *quoting* S.Rept. 95-701 at 12.

subdivision must give notice to the aggrieved person, the court or other authority, and the Attorney General) of their intent to so disclose or use communications obtained from the surveillance or derivative information. In addition, under 50 U.S.C. §§ 1806(f) and (g), if the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm national security, the U.S. district court may review in camera and ex parte the application, order, and other materials related to the surveillance, to determine whether the surveillance was lawfully authorized and conducted, whether disclosure or discovery is necessary, and whether to grant a motion to suppress. The Court of Review noted that these determinations are to be made by the U.S. district judge on a case by case basis, and stated that "whether such a decision protects a defendant's constitutional rights in a given case is not before us."[3921]

Based on this comparison of Title III and FISA, the Court of Review found that "to the extent that the two statutes diverge in constitutionally relevant areas — in particular, in their probable cause and particularity showings — a FISA order may not be a 'warrant' contemplated by the Fourth Amendment.... Ultimately, the question becomes whether FISA, as amended by the Patriot Act, is a reasonable response based on a balance of the legitimate need of the government for foreign intelligence information to protect against national security threats with the protected rights of citizens."[3922]

The court framed the question as follows: "does FISA amplify the President's power by providing a mechanism that at least approaches a classic warrant and which therefore supports the government's contention that FISA searches are constitutionally reasonable." In its analysis, the court first considered whether the *Truong* case articulated the correct standard. *Truong* held that the President had inherent authority to conduct warrantless searches to obtain foreign intelligence information, but did not squarely address FISA. Starting from the perspective that *Truong* deemed the primary purpose test to be constitutionally compelled as an application of the *Keith* case balancing standard, the Court of Review found that the *Truong* determination that "once surveillance becomes primarily a criminal investigation, the courts are entirely competent to make the usual probable cause determination, and ... individual privacy interests come to the fore and government foreign policy concerns recede when the government is primarily attempting to form the basis of a criminal investigation."[3923] The Court of Review found that this analysis was based upon a faulty premise that in the context of criminal prosecution "foreign policy concerns recede," and found further that the line the *Truong* court "sought to draw was inherently unstable,

---

[3921] *Id.*

[3922] *Id.* at 741-42.

[3923] *Id.* at 742-43, citing Truong, supra, 629 F.2d at 914-15.

unrealistic, and confusing."[3924] The Court of Review opined that in the context of counterintelligence, foreign policy concerns did not recede when the government moved to prosecute. Rather "the government's primary purpose is to halt the espionage or terrorism efforts, and criminal prosecutions can be, and usually are, interrelated with other techniques used to frustrate a foreign power's efforts."[3925]

In addition, the court found that the method of determining when an investigation became primarily criminal by looking to when the Criminal Division of the Department of Justice assumed the lead role, had led over time to the "quite intrusive organizational and personnel tasking the FISA court [had] adopted."[3926] The court found the "wall" procedure to generate dangerous confusion and create perverse organizational incentives that discouraged wholehearted cooperation of "all the government's personnel who can be brought to the task."[3927] This the court suggested could be thought to be dangerous to national security and could be thought to discourage desirable initiatives.

In addition, the court saw the primary purpose test as administered by the FISC, "by focusing on the subjective motivation of those who initiate investigations … was at odds with the Supreme Court's Fourth Amendment cases which regard subjective motivation of an officer conducting a search or seizure as irrelevant."[3928]

Assuming *arguendo* that FISA orders were not warrants within the scope of the Fourth Amendment, the Court of Review returned to the question of whether searches under FISA are constitutionally reasonable. While the Supreme Court has not considered directly the constitutionality of warrantless government searches for foreign intelligence purposes, the balance between the government's interest and personal privacy interests is key to an examination of this question. The Court of Review viewed *Keith* as suggesting that a somewhat relaxed

---

[3924] *Id.* at 743.

[3925] *Id.*

[3926] *Id.*

[3927] *Id.*

[3928] *Id.*, citing Whren v. United States, 517 U.S. 806, 13 (1996). See also, Arkansas v. Sullivan, 532 U.S. 769, 770-72 (2001); Scott v. United States, 438 U.S. 128, 135-138 (1978). In these cases, the Court has held that, in a Fourth Amendment probable cause analysis of a warrantless search or seizure, the fact that an otherwise lawful search or seizure may have been made as a pretext for searching for evidence of other criminal behavior does not render that search or seizure unconstitutional. One might note that the probable cause standard applicable to a search or seizure in a criminal investigation is different from that under FISA, so that the pretextual search criminal cases may not be directly analogous to the FISA situation.

standard might be appropriate in foreign intelligence crimes as opposed to ordinary crimes.[3929]

The Court of Review then briefly touched upon the Supreme Court's "special needs" cases, where the Court upheld searches not based on a warrant or individualized suspicion in extraordinary circumstances involving "special needs, beyond the normal need for law enforcement." In *City of Indianapolis v. Edmond*, 531 U.S. 32, 42 (2000), the U.S. Supreme Court held that a highway check point program designed to catch drug dealers was not within the "special needs" exception to the requirement that a search be based upon individualized suspicion, because "the government's 'primary purpose' was merely 'to uncover evidence of ordinary criminal wrongdoing.'" The Court stated that "the gravity of the threat alone cannot be dispositive of questions concerning what means law enforcement officers may employ to pursue a given purpose."[3930] The Court relied upon an examination of the primary purpose of the program, but not the motivations of individual officers, to determine whether the "special needs" standard had been met. The Supreme Court noted that an appropriately tailored road block could be used "to thwart an imminent terrorist attack."[3931]

After summarizing *Edmond*, the Court of Review emphasized that it is the nature of the threat or emergency that took the matter beyond the realm of ordinary crime control.[3932] It concluded that, while the gravity of the threat alone cannot be dispositive of the reasonableness of a search under the Fourth Amendment standard, it is a critical factor in the analysis. In its view, the "programmatic purpose" of FISA, "to protect the nation against terrorists and espionage threats directed by foreign powers," was one which, from FISA's inception, was distinguishable from "ordinary crime control."[3933] The Court of Review also concluded that, "[e]ven without taking into account the President's inherent constitutional authority to conduct warrantless foreign intelligence surveillance, we think the procedures and government showings required under FISA, if they do not meet the minimum Fourth Amendment warrant standards, certainly come close."[3934] Applying the balancing test that it had drawn from Keith between foreign intelligence crimes and ordinary crimes, the Court of Review held

---

[3929] *Id.* at 744.

[3930] 531 U.S. at 42, cited in Court of Review op., 310 F.3d at 745.

[3931] 531 U.S. at 44, cited in Court of Review op., 310 F.3d at 746.

[3932] Court of Review op., 301 F.3d at 746.

[3933] *Id.*

[3934] *Id.*

surveillances under FISA, as amended by the USA PATRIOT Act, were reasonable and therefore constitutional. In so doing, however, the Court of Review

> *acknowledged] … that the constitutional question presented by this case — whether Congress' disapproval of the primary purpose test is consistent with the Fourth Amendment — has no definitive jurisprudential answer. The Supreme Court's special needs cases involve random stops (seizures) not electronic searches. In one sense, they can be thought of as a greater encroachment into personal privacy because they are not based on any particular suspicion. On the other hand, wiretapping is a good deal more intrusive than an automobile stop accompanied by questioning.*[3935]

The Court of Review reversed the FISC's orders before it for electronic surveillance "to the extent they imposed conditions on the grant of the government's applications, vacate[d] the FISA court's Rule 11, and remand[ed] with instructions to grant the applications as submitted and proceed henceforth in accordance with this opinion."[3936]

50 U.S.C. § 1803(b) provides that, where the Court of Review upholds a denial by the FISC of a FISA application, the United States may file a petition for certiorari to the United States Supreme Court. Since consideration of applications for FISA orders is ex parte, there is no provision in FISA for an appeal to the United States Supreme Court from a decision of the Court of Review by anyone other than the United States. Nevertheless, on February 18, 2003, a petition for leave to intervene and a petition for writ of certiorari to the U.S. Foreign Intelligence Surveillance Court of Review was filed in this case in the U.S. Supreme Court by the American Civil Liberties Union, National Association of Criminal Defense Lawyers, American-Arab Anti-Discrimination Committee, and the Arab Community Center for Economic and Social Services. On March 14, 2003, the Bar Association of San Francisco filed a motion to file an amicus curiae brief in support of the motion to intervene and petition for certiorari. On March 24, 2003, the Supreme Court denied the motion for leave to intervene in order to file a petition for a writ of certiorari and denied the motion for leave to file an amicus curiae brief.[3937]

[3935] *Id.*

[3936] *Id.*

[3937] American Civil Liberties Union v. United States, Docket No. 02M69, 538 U.S. 920 (March 24, 2003). The disposition of the case appears on the Supreme Court's Order List for that date. It is interesting to note that both the Petition for Leave to Intervene and Petition for a Writ of Certiorari filed by the American Civil Liberties Union, et al., and the motion to file an amicus curiae brief of the Bar Association of San Francisco were filed under the name In re: Sealed Case of the Foreign Intelligence Surveillance Court of Review No. 02-001.

Conclusion

The Foreign Intelligence Surveillance Act, as amended, provides a statutory structure to be followed where electronic surveillance, 50 U.S.C. § 1801 et seq., physical searches, 50 U.S.C. § 1821 *et seq*., or pen registers or trap and trace devices, 50 U.S.C. § 1841 *et seq*., for foreign intelligence gathering purposes are contemplated. In addition, it provides a statutory mechanism for the FBI to seek production of "any tangible things" for an investigation seeking foreign intelligence information not involving a U.S. person or to protect against international terrorism or clandestine intelligence with respect to any person under 50 U.S.C. § 1861. FISA creates enhanced procedural protections where a United States person is involved, while setting somewhat less stringent standards where the surveillance involves foreign powers or agents of foreign powers. With its detailed statutory structure, it appears intended to protect personal liberties safeguarded by the First and Fourth Amendments while providing a means to ensure national security interests.

The USA PATRIOT Act, P.L. 107-56, increased the number of FISC judges from 7 to 11, while expanding the availability of FISA electronic surveillance, physical searches and pen registers and trap and trace devices. For example, under P.L. 107-56, an application for a court order permitting electronic surveillance or a physical search under FISA is now permissible where "a significant purpose" of the surveillance or physical search, rather than "the purpose" or, as interpreted by some courts, "the primary purpose" of the surveillance or physical search, is to gather foreign intelligence information. While the previous language withstood constitutional challenge, the Supreme Court has not yet determined the constitutional sufficiency of the change in the FISA procedures under the Fourth Amendment. On the other hand, the U.S. Foreign Intelligence Court of Review has examined a number of constitutional issues in *In re Sealed Case*, finding that FISA orders, if not satisfying the constitutional warrant requirement, are close to doing so; and finding that, even if a FISA order does not qualify as a warrant for Fourth Amendment purposes, electronic surveillance under FISA as amended by the USA PATRIOT Act is reasonable and therefore constitutional. At the same time, however, the Court of Review acknowledged that the constitutional question of whether Congress' disapproval of the primary purpose test is consistent with the Fourth Amendment "has no definitive jurisprudential answer."[3938]

The USA PATRIOT Act also amended FISA to allow court orders permitting so-called multipoint or "roving" electronic surveillance, where the orders do not require particularity with respect to the identification of the instrument, place, or facility to be intercepted, upon a finding by the court that the actions of the target

---

[3938] *Court of Review op*., 310 F.3d at 746.

of the surveillance are likely to thwart such identification. P.L. 107-108 further clarified this authority.

Under P.L. 107-56, pen registers and trap and trace devices may now be authorized for e-mails as well as telephone conversations. In addition, the act expanded the previous FBI access to business records, permitting court ordered access in connection with a foreign intelligence or international terrorism investigation not just to business records held by common carriers, public accommodation facilities, physical storage facilities, and vehicle rental facilities, but to any tangible things.

While expanding the authorities available for foreign intelligence investigations, FISA, as amended by the USA PATRIOT Act and the Intelligence Authorization Act for FY2002, also contains broader protections for those who may be the target of the various investigative techniques involved. For example, whether the circumstances involve electronic surveillance, physical searches, pen registers or trap and trace devices or access to business records and other tangible items, FISA, as amended by the USA PATRIOT Act, does not permit the court to grant orders based solely upon a United States person's exercise of First Amendment rights.[3939]

In addition, P.L. 107-56 created a new private right of action for persons aggrieved by inappropriate disclosure or use of information gleaned or derived from electronic surveillance, physical searches or the use of pen registers or trap and trace devices. These claims can be brought against the United States for certain willful violations by government personnel.

Finally, the inclusion of a sunset provision for the FISA changes made in the USA PATRIOT Act, with the exception of the increase in the number of FISC judges, provides an opportunity for the new authorities to be utilized and considered, and an opportunity for the Congress to revisit them in light of that experience.

Sections 898 and 899 of the Homeland Security Act of 2002, P.L. 107-296, amended FISA, 50 U.S.C. §§1806(k)(1) and 1825(k)(1) respectively, to permit federal officers conducting electronic surveillance or physical searches to acquire foreign intelligence information under FISA to consult with federal law enforcement officers "or law enforcement personnel of a state or political subdivision of a State (including the chief executive officer of that State or political subdivision who has the authority to appoint or direct the chief law enforcement officer of that State or political subdivision)." Such consultations are to coordinate efforts to investigate or protect against actual or potential attacks or other grave hostile acts of a foreign power or an agent of a foreign power;

[3939] *See, e.g.*,50 U.S.C. §§ 1805(a)(3)(A), 1824(a)(3)(A), 1842(a)(1), 1843(b), 1861(a)(1), and 1861(a)(2).

sabotage or international terrorism by a foreign power or an agent of a foreign power; or clandestine intelligence activities by an intelligence service or network of a foreign power or an agent of a foreign power. These sections also state that such consultations do not preclude the Assistant to the President for National Security Affairs or other designated Executive Branch officials from making the necessary certifications as part of the application process for a FISA court order under 50 U.S.C. §§ 1804(a)(7) or 1823(a)(7), nor are these consultations to preclude entry of an order under 50 U.S.C. §§ 1805 or 1824.[3940]

Section 6001 of Title VI of FISA, as added by the Intelligence Reform and Terrorism Prevention Act of 2004, P.L. 108-458, expanded the definition of "agent of a foreign power" in the context of non-U.S. persons to encompass those who engage in international terrorism or in activities in preparation for international terrorism, regardless of whether they have any connection or affiliation with a foreign government or other foreign organization or entity. This new definition is included among those FISA provisions subject to the sunset provisions in Section 224 of the USA PATRIOT Act, as amended. Section of the new Title VI of FISA also imposed new, detailed semiannual reporting requirements to facilitate congressional oversight of the implementation of the Act, which are codified at 50 U.S.C. § 1871.

[3940] Section 897 of the Homeland Security Act of 2002, which dealt with "Foreign Intelligence Information," amended Section 203(d)(1) of the USA PATRIOT Act, 50 U.S.C. § 403-5d(1), to provide authority, consistent with the responsibility of the DCI to protect intelligence sources and methods and that of the Attorney General to protect sensitive law enforcement information,

for information revealing a threat of an actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power, domestic or international sabotage, domestic or international terrorism, or clandestine intelligence gathering activities by an intelligence service or network of an foreign power or by an agent of a foreign power, within the United States or elsewhere, obtained as part of a criminal investigation to be disclosed to any appropriate Federal, State, local, or foreign government official for the purpose of preventing or responding to such a threat. Any official who receives information pursuant to this provision may use that information only as necessary in the conduct of that person's official duties subject to any limitations on the unauthorized disclosure of such information, and any State, local, or foreign official who receives information pursuant to this provision may use that information only consistent with such guidelines as the Attorney General and the Director of Central Intelligence shall jointly issue.

In light of the Court of Review's interpretation of "foreign intelligence information" under FISA as including investigations of what the Court of Review termed "foreign intelligence crimes," it is not clear whether this section might be interpreted as applicable to sharing of information gleaned from FISA surveillances, searches, pen registers, trap and trace devices, or business record requests, particularly where criminal prosecution is a goal of the investigation.

P.L. 108-458, after creating the new position of Director of National Intelligence in Section 1101 of the Act, included conforming amendments, which replaced references to the "Director of Central Intelligence" with "Director of National Intelligence" in a broad range of provisions. However, P.L. 108-458 does not appear to have replaced "Director of Central Intelligence"with "Director of National Intelligence" in 50 U.S.C. § 403-5d.

The USA PATRIOT Improvement and Reauthorization Act of 2005, P.L. 109177 (Reauthorization Act), Section 102, adopted a sunset of December 31, 2009, for FISC orders for multipoint or "roving" wiretaps under Section 105(a) of FISA, 50 U.S.C. § 1805(a), for FISC orders for production of tangible things under Section 501 of FISA, 50 U.S.C. § 1861, and congressional oversight requirements in Section 502 of FISA, 50 U.S.C. § 1862. Section 103 of P.L. 109-177 extended the sunset relating to "lone wolf" agents of foreign powers to December 31, 2009.

Section 105 of P.L. 109-177 extended the maximum duration initial orders authorizing of electronic surveillances and physical searches under Sections 105(e) and 304 of FISA to 120 days, while extensions of such electronic surveillances and physical searches could be for up to one year. The duration of both initial orders and extensions to orders authorizing installation and use of FISa pen registers or trap and trace devices is extended from 90 days to one year in cases where the Government has certified that the information likely to be obtained is foreign intelligence information not concerning a U.S. person.

Section 106(a) of P.L. 109-177permits the FBI Director to delegate his authority to make an application for a production order regarding library circulation records, library patron lists, book sales records, book customer lists, firearms sales records, tax return records, educational records, or medical records containing information that would identify a person, to either the Deputy Director of the Federal Bureau of Investigation or the Executive Assistant Director for National Security (or any successor position). Neither the Deputy Director nor the Executive Assistant Director may not further delegate such authority.

Section 106(b) of P.L.109-177 requires an application for a FISA production order to include statement of the facts supporting a reasonable belief that the tangible things sought are relevant to an authorized investigation (other than a threat assessment) to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities. It provides that certain tangible things are "presumptively relevant" to such an investigation if the statement of facts shows that they pertain to a foreign power or agent of a foreign power, the activities of a suspected agent of a foreign power who is the subject of the authorized investigation, or an individual in contact with or known to a suspected agent of a foreign power who is the subject of the investigation.

Section 106(c) of P.L. 109-177 provides that an FISC judge must approve a FISA production order if he or she finds that the application meets the statutory requirements. Under Section 106(d) of P.L. 109-177, such an ex parte order must include a particularized description of the tangible things sought, must allow a reasonable time for such things to be assembled, must notify the recipients of the production order of applicable nondisclosure requirements, and must be limited to things which may be subject to a grand jury subpoena or any other federal

court order directing production of records or tangible things. The order must not disclose that such order is issued for purposes of such an authorized investigation.

Section 106(d) of the Reauthorization Act prohibits the recipient of a production order from disclosing to anyone except those persons to whom disclosure is necessary to comply with such order; an attorney to obtain legal advice or assistance with respect to the production of things in response to the order; or other persons as permitted by the FBI Director or his designee. Subsection 106(e) of the measure requires the production order recipient, upon the request of the FBI Director or his designee, to identify to the FBI those to whom such disclosure has been or will be made, unless the disclosure has been or is to be made to an attorney from whom legal advice or assistance is sought.[3941]

Section 106(f) of P.L. 109-177 amends 50 U.S.C. § 1803 to establish a petition review pool of FISC judges to hear challenges to FISA production or related nondisclosure orders, and sets forth a detailed judicial review process for consideration of such petitions.

Section 106A of the Reauthorization Act directs the Inspector General of the U.S. Department of Justice to conduct a comprehensive audit of the effectiveness and use, including any improper or illegal use, of the investigative authority provided to the FBI under 50 U.S.C. 1861 for calendar years 2002-2006, and requires the results to be filed in two unclassified reports to the House and Senate Intelligence and Judiciary Committees.

Section 108(a) and (b) amend the requirements for an application and for an FISC order authorizing multipoint electronic surveillance under FISA. Subsection 108(c) expands the list of committees to whom the Attorney General's semiannual reports on FISA electronic surveillance to include not only the Intelligence Committees but also the Senate Judiciary Committee; and requires the report to include an additional category of information, that is, a description of the total number of applications made for orders approving such multipoint electronic surveillance.

Section 109(a) of P.L. 109-177 modifies the list of congressional committees receiving two semiannual reports from the Attorney General on physical searches under FISA pursuant to 50 U.S.C. § 1826, and requires the second of these reports to include, among other things, the total number of emergency physical searches authorized by the Attorney General under 50 U.S.C. § 1824(e) and the total number of subsequent orders approving or denying such physical searches.

[3941] *But see* the amendment in Section 4 of P.L. 109-178 deleting that exception, discussed *infra*.

Section 109(b) of P.L. 109-177 requires the Attorney General, in his semiannual statistical report submitted to the House and Senate Judiciary Committees on FISA pen registers and trap and trace devices, to include, among other things, the total number of pen registers and trap and trace devices whose installation and use was authorized by the Attorney General on an emergency basis under 50 U.S.C. §1843, and the total number of subsequent orders approving or denying the installation and use of such pen registers and trap and trace devices.

Section 109(d) of P.L. 109-177 amends 50 U.S.C. § 1803 to permit the FISC and Court of Review to establish such rules and procedures, and take such actions, as are reasonably necessary to administer their responsibilities under this chapter. Any such rules and procedures are to be recorded and transmitted to all of the judges on the FISC and on the Court of Review, the Chief Justice of the United States, the House and Senate Judiciary Committees, the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence.

Section 128(a)(3) of P.L. 109-177 added 50 U.S.C. § 1842(d)(2)(C), which permits the FISC, in an order authorizing use of a pen register or trap and trace device, to direct a wire or communication service provider to provide the federal officer using the device specific subscriber or customer information upon request. That information may include, with respect to a customer or subscriber using the service during the period of the order, the name of the customer or subscriber; the address of the customer or subscriber; the telephone or instrument number, or other subscriber number or identifier, of the customer or subscriber, including any temporarily assigned network address or associated routing or transmission information; the length of the provision of service by such provider to the customer or subscriber and the types of services utilized by the customer or subscriber. In the case of a provider of local or long distance telephone service, the information provided may include any local or long distance telephone records of the customer or subscriber; if applicable, any records reflecting period of usage (or sessions) by the customer or subscriber; any mechanisms and sources of payment for such service, including the number of any credit card or bank account utilized for payment for such service; and, if available, with respect to any customer or subscriber of incoming or outgoing communications to or from the service covered by the order, the name of such customer or subscriber; the address of such customer or subscriber; the telephone or instrument number, or other subscriber number or identifier, of such customer or subscriber, including any temporarily assigned network address or associated routing or transmission information; and the length of the provision of service by such provider to such customer or subscriber and the types of services utilized by such customer or subscriber.

Section 128(b) of P.L. 109-177 added the House and Senate Judiciary Committees to the list of committees to be kept fully informed by the Attorney General regarding all use of FISA pen registers and trap and trace devices.

Section 506 of P.L. 109-177 amends the definition of "Attorney General" under 50 U.S.C. § 1801(g) to include the Assistant Attorney General for National Security, so that the term includes "the Attorney General of the United States (or Acting Attorney General), the Deputy Attorney General, or, upon the designation of the Attorney General, the Assistant Attorney General designated as the Assistant Attorney General for National Security under section 507A of title 28, United States Code."

Section 3 of P.L. 109-178 amends the provisions in 50 U.S.C. § 1861(f) regarding judicial review of production orders and related nondisclosure orders. In addition, Section 4 of the measure amends 50 U.S.C. § 1861(d)(2) to provide that, at the request of the FBI Director or his designee, any person disclosing or intending to disclose that the FBI has sought or obtained tangible things under a FISA production order to someone in one of the three categories of individuals to whom such disclosure is permitted, shall identify to the Director or his designee the person to whom the disclosure will be or has been made. In so doing, the measure in effect deletes an exception to this identification requirement where the person to whom the disclosure is made is an attorney from whom the person making the disclosure is seeking legal advice or assistance.

In addition to examining the statutory structure in FISA, as amended, this report has explored two published decisions, one from the FISC in *In re All Matters Submitted to the Foreign Intelligence Surveillance Court* and one from the U.S. Foreign Intelligence Court of Review in *In re Sealed Case*. Because historically the decisions of the FISC have not been made public, and because the opinion of the U.S. Foreign Intelligence Surveillance Court of Review discussed in this report was the first decision ever made by that court, the recent decisions of the FISC and the Court of Review provided a unique opportunity to observe the decision-making processes and differing perspectives of the two courts created by FISA.

The FISC's decision was set against a backdrop of a significant number of instances in which the Department of Justice had failed to maintain a "wall" between foreign intelligence gathering and criminal investigations. All seven of the then sitting members of the FISC concurred in the May 17, 2002, order of the court, written by the then presiding judge of the court. The FISC, in its May 17th opinion and order, treated the Attorney General's proposed 2002 "Intelligence Sharing Procedures for Foreign Intelligence and Foreign Counterintelligence Investigations Conducted by the FBI" as minimization procedures, and approved them as modified. The modifications made by the Court permitted the FBI, the Criminal Division, and OIPR to consult with one another "to coordinate their efforts to investigate or protect against foreign attack or other grave hostile acts, sabotage, international terrorism, or clandestine intelligence activities by foreign powers or their agents." In so doing, the FISC permitted such cooperation and coordination to address, among other things, the exchange of information already acquired, identification of categories of information needed and being sought, prevention of either foreign intelligence gathering or criminal law

enforcement investigation or interest from obstructing or hindering the other; compromise of either investigation, and long term objectives and overall strategy of both investigations to insure that overlapping intelligence and criminal interests of the United States are both achieved.[3942] While permitting direct consultation and coordination between components, the FISC required that OIPR be invited to all consultations and, if OIPR was unable to attend, the modified procedures required that OIPR be "forthwith" informed in writing of the substance of the meeting so that the FISC could be notified promptly.[3943] In addition, under the procedures as modified by the FISC, law enforcement officials were prohibited from making recommendations to intelligence officials regarding the initiation, operation, continuation or expansion of FISA searches or surveillances. Nor could law enforcement officials direct or control the use of FISA procedures to enhance criminal prosecution. The FBI and the Criminal Division were given the responsibility to ensure that this did not occur, and were also required to make certain that advice intended to preserve the criminal prosecution option did not inadvertently result in the Criminal Division directing or controlling the investigation using FISA tools to further law enforcement objectives.[3944] In addition, the FISC adopted a new Rule 11, dealing with criminal investigations in FISA cases, to facilitate monitoring of compliance with its May 17, 2002 order. This rule required all FISA applications to include informative descriptions of ongoing criminal investigations of FISA targets, as well as the substance of consultations between the FBI and criminal prosecutors at the Department of Justice or a U.S. Attorney's office.

In its November 18, 2002 opinion, the Court of Review took a starkly different view of the Attorney General's proposed procedures and firmly rejected the FISC analysis and conclusions. The issue came before the Court of Review as an appeal of two FISC orders, one granting an application to authorize electronic surveillance of an agent of a foreign power subject to restrictions stemming from the FISC May 17th opinion and order and the other renewing the authorization for electronic surveillance subject to the same conditions.

The Court of Review held that the FISC's interpretation of the augmented 1995 procedures and the proposed 2002 procedures as minimization procedures under 50 U.S.C. § 1801(h) was in error. The Court of Review found that the FISC had misconstrued 50 U.S.C. §§ 1801(h) and 1805 and may have overstepped its constitutional authority by asserting authority to govern the internal organization and investigative procedures of the Justice Department.

[3942] *FISC op.*, 218 F. Supp. 2d at 626.

[3943] *Id.*

[3944] *Id.*

It found that FISA, as originally enacted, did not create a dichotomy between foreign intelligence information gathering and law enforcement investigations, nor did it require maintenance of a "wall" between such investigations. While FISA as enacted in 1978 required that a national security official certify that "the purpose" of the investigation was to gather foreign intelligence information, the court regarded the definition of "foreign intelligence information" as including evidence of criminal wrongdoing where a U.S. person is the target of the FISA investigation. In light of the fact that the definition of "agent of a foreign power" applicable to U.S. persons involved criminal conduct, or, in the context of clandestine intelligence operations, the possibility of criminal conduct, the court distinguished "foreign intelligence crimes" from "ordinary crimes." In foreign intelligence crimes, intelligence gathering and criminal investigations may become intertwined.

The Court of Review reviewed past court decisions requiring that, in seeking a FISA order authorizing electronic surveillance, the government must demonstrate that the "primary purpose" of the surveillance was to gather foreign intelligence information and not to further law enforcement purposes. Rejecting the "primary purpose test" as applied by the FISC and the courts of appeals of several circuits, the Court of Review did not find it to be compelled by the statutory language of FISA as originally enacted or by the Fourth Amendment.

The Court of Review also held the FISC to have been in error in its refusal "to consider the legal significance of the Patriot Act's crucial amendments...." In particular, the court focused upon the change of the required certification by the national security official from a certification that "the purpose" of the surveillance was to obtain foreign intelligence information to a certification that "a significant purpose" of the surveillance was to obtain foreign intelligence information in 50 U.S.C. § 1804(a)(7)(B); and the enactment of 50 U.S.C. § 1806(k), authorizing consultation and coordination by federal officers engaged in electronic surveillance to acquire foreign intelligence information with federal law enforcement officers.

Finding that the "significant purpose" amendment recognized the existence of a dichotomy between intelligence gathering and law enforcement purposes, the Court of Review concluded that this test was satisfied if the government had "a measurable foreign intelligence purpose, other than just criminal prosecution of even foreign intelligence crimes."[3945] While the gathering of foreign intelligence information for the sole objective of criminal prosecution would be precluded by the "significant purpose" language, if "the government entertains a realistic option of dealing with the agent [of a foreign power] other than through criminal

---

[3945] *Id.* at 735.

prosecution," the court found the "significant purpose" test satisfied.[3946] Although the court was of the view that, prior to passage of the USA PATRIOT Act, the FISC may well not have had authority under 50 U.S.C. § 1805(a)(5) to inquire into anything other than the issue of "whether the information sought was a type of foreign intelligence information, in light of the significant purpose amendment of section 1804" the Court of Review concluded that "it seems section 1805 must be interpreted as giving the FISA court the authority to review the government's purpose in seeking the information."[3947] The court held that the government's purpose under 50 U.S.C. § 1804(a)(7)(B) was "to be judged by the national security official's articulation and not by a FISA court inquiry into the origins of an investigation nor an examination of the personnel involved.... [I]f the FISA court has reason to doubt that the government has any real non-prosecutorial purpose in seeking foreign intelligence information it can demand further inquiry into the certifying officer's purpose — or perhaps even the Attorney General's or Deputy Attorney General's reasons for approval."[3948]

The Court of Review also considered whether FISA, as amended, passed constitutional muster under the Fourth Amendment. It deemed the procedures and government showings required under FISA to come close to the minimum requirements for a warrant under the Fourth Amendment, if not meeting such requirements. Assuming arguendo that a FISA order was not a warrant for Fourth Amendment purposes, the Court of Review found FISA constitutional because the surveillances authorized thereunder were reasonable.

[3946] *Id.*

[3947] *Id.*

[3948] *Id.* at 736.

Probable Cause, Reasonable Suspicion, and Reasonableness Standards in the Context of the Fourth Amendment and the Foreign Intelligence Surveillance Act (Memorandum January 30, 2006)

AMERICAN LAW DIVISION, CONGRESSIONAL RESEARCH SERV., PROBABLE CAUSE, REASONABLE SUSPICION, AND REASONABLENESS STANDARDS IN THE CONTEXT OF THE FOURTH AMENDMENT AND THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (2006), *available at* http://www.intelligencelaw.com/library/secondary/crs/pdf/memo_1-30-2006.pdf.

Memorandum January 30, 2006

TO: Senate Select Committee on Intelligence
Attention: Mike Davidson

FROM: American Law Division

SUBJECT: Probable Cause, Reasonable Suspicion, and Reasonableness Standards in the Context of the Fourth Amendment and the Foreign Intelligence Surveillance Act

This is in response to your request for a brief description of the Fourth Amendment's probable cause, reasonable suspicion, and reasonableness standards. In over simplified terms, probable cause "exist[s] where the known facts and circumstances are sufficient to warrant a man of reasonable prudence in the belief that contraband or evidence of a crime will be found," *Ornelas v. United States*, 517 U.S. 690, 696 (1996); *Illinois v. Gates*, 462 U.S. 213, 238 (1983).

Under a similar gloss, reasonable suspicion is a standard, more than a hunch but considerably below preponderance of the evidence, which justifies an officer's investigative stop of an individual upon the articulable and particularized belief that criminal activity is afoot, *Ornelas v. United States*, 517 U.S. at 695; *Illinois v. Gates*, 462 U.S. at 235.

And Fourth Amendment reasonableness is that point at which the government's interest advanced by a particular search or seizure outweighs the loss of individual privacy or freedom of movement that attends the government's action, *Illinois v. Lidster*, 540 U.S. 419, 427 (2004)("in judging reasonableness, we look to the gravity of the public concerns served by the seizure, the degree to which the seizure advances the public interest, and the severity of the interference with individual liberty").

Again in summary and to add further complication, the Supreme Court has speculated that in national security cases the "probable cause" may be less demanding or at least different than it is in the context of a traditional criminal investigation, *United States v. United States District Court*, 407 U.S. 297, 322 (1972)("the gathering of security intelligence is often long range and involves the interrelation of various sources and types of information. . . . Thus, the focus of domestic surveillance may be less precise than that directed against more conventional types of crime"). FISA permits recourse to this reduced application of the probable cause standard in spy cases but not in terrorism cases, *In re Sealed Case*, 310 F.3d 717, 739 (F.I.S.Ct.Rev. 2002)("Congress allowed this lesser showing for clandestine intelligence activities – but not, notably, for other activities, including terrorism . . ."). Yet it is focus and not the standard that is different in FISA cases. The standard is the same; the certainty of the predicate is different: probable cause to believe that evidence of a crime *will be* found versus probable cause to believe that spying *may* occur.

Each of the standards is a means of judging official conduct against the demands of the Fourth Amendment which provides that, "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized," U.S. Const. Amend. IV. The question of which standard applies and whether a particular search passes muster is fact driven.

On a number occasions, the Court has pointed out that probable cause is the description of a degree of probability that cannot be easily defined out of context:

> *The probable-cause standard is incapable of precise definition or quantification into percentages because it deals with probabilities and depends on the totality of the circumstances. We have stated, however, that the substance of all the definitions of probable cause is a reasonable ground for belief of guilt, and that the belief of guilt must be particularized with respect to the person to be searched or seized. Maryland v. Pringle, 540 U.S. 366, 371 (2003)(citations omitted).*

An earlier case had made the same point for both the probable cause and reasonable suspicion standards:

> *Articulating precisely what "reasonable suspicion" and "probable cause" mean is not possible. They are commonsense, nontechnical conceptions that deal with the factual and practical considerations of everyday life on which reasonable and prudent men, not legal technicians act. As such, the standards are not really, or even usefully, reduced to a neat set of legal rules. We have described reasonable suspicion simply as a particularized and objective*

> *basis for suspecting the person stopped of criminal activity, and probable cause to search as existing where the known facts and circumstances are sufficient to warrant a man of reasonable prudence in the belief that contraband or evidence of a crime will be found. We have cautioned that these two legal principles are not "finely-tuned standards" comparable to the standards of proof beyond a reasonable doubt or of proof by a preponderance of the evidence. They are instead fluid concepts that take their substantive content from the particular contexts in which the standards are being assessed. The principal components of a determination of reasonable suspicion or probable cause will be the events which occurred leading up to the stop or search, and then the decision whether these historical facts, viewed from the standpoint of an objectively reasonable police officer amount to reasonable suspicion or to probable cause. Ornelas v. United States, 517 U.S. at 695-96 (citations omitted).*

While *Ornelas* finds "probable cause where the known facts and circumstances are sufficient to warrant a man of reasonable prudence in the belief that contraband or evidence of a crime will be found," id. at 695, *Pringle*, 540 U.S. at 371, 372 n,2, refers to the comparable but more detailed earlier treatment in *Brinegar v. United States*. *Brinegar* begins with Chief Justice Marshall's observation that probable cause "means less than evidence which would justify condemnation or conviction," *Brinegar v. United States*, 338 U.S. 160, 175 (1949), quoting, *Locke v. United States*, 7 Cranch (11 U.S.) 339, 348 (1813). *Brinegar* then adds, "[s]ince, Marshall's time, at any rate, it has come to mean more than bare suspicion: Probable cause exists where the facts and circumstances within . . . the officers' knowledge and of which they had reasonably trustworthy information are sufficient in themselves to warrant a man of reasonable caution in the belief that an offense has been or is being committed," 338 U.S. at 175-76 (citations omitted).

The Court has supplied illustrations of what constitutes probable cause and what does not. *Pringle* found probable cause to arrest the passenger in a small car on a charge of possessing the five "baggies" of cocaine found in the back seat of the car, 540 U.S. at 372. An officer had stopped the car for speeding at 3 in the morning. *Id*. at 371. Pringle was the front seat passenger and the officer saw a large roll of cash in the glove compartment when it was opened to retrieve the car's registration. *Id*. at 371-72. To these the Court added the inference that a trained, experienced officer might draw: "Here we think it was reasonable for the officer to infer a common enterprise among the three men [in the car]. The quantity of drugs and cash in the car indicated the likelihood of drug dealing, an enterprise to which a dealer would be unlikely to admit an innocent person with the potential to furnish evidence against him," *id*. at 373.

Ybarra, in contrast, found no probable cause for officers to search a bar patron present when they executed a warrant authorizing the search of the bartender

based upon probable cause to believe the bartender would be selling heroin at the time, *Ybarra v. Illinois*, 444 U.S. 85, 91 (1979). *Ybarra* listed a series of factors that might have but did not contribute to a finding of probable cause: "[T]he police did not recognize Ybarra and had no reason to believe that he had committed, was committing, or was about to commit any offense under state or federal law. Ybarra made no gestures indicative of criminal conduct, made no movements that might suggest an attempt to conceal contraband, and said nothing of a suspicious nature to the police officers. In short, the agents knew nothing in particular about Ybarra, except that he was present, along with several other customers in a public tavern at a time when the police had reason to believe that the bartender would have heroin for sale. It is true that the police possessed a warrant based on probable cause to search the tavern in which Ybarra happened to be at the time the warrant was executed. But, a person's mere propinquity to others independently suspected of criminal activity does not, without more, give rise to probable cause to search that person," *id.*

Some years later, the *Royer* plurality opinion noted a list of arguably suspicious factors that nevertheless did not add up to probable cause: "[A] nervous young man with two American Tourister bags paid cash for an airline ticket to a 'target' city. These facts led to inquiry, which in turn revealed that the ticket had been bought under an assumed name. The proffered explanation did not satisfy the officers," *Florida v. Royer*, 460 U.S. 491, 507 (1983).

The reasonable suspicion standard is of relatively recent origins. Although never expressly mentioned there, it comes from *Terry*, which recognized that under certain exigencies of time and place police officers may conduct a limited seizure and search with less than probable cause, *Terry v. Ohio*, 392 U.S. 1 (1968).[3949] Reasonable suspicion has been described as "something more than an inchoate and unparticularized suspicion or hunch. . . . [as a] level of suspicion . . . considerable less than proof of wrongdoing by a preponderance of the evidence. .

[3949] "At the time he seized petitioner and searched him for weapons, Officer McFadden had reasonable grounds to believe that petitioner was armed and dangerous, and it was necessary for the protection of himself and others to take swift measures to discover the true facts and neutralize the threat of harm if it materialized. The policeman carefully restricted his search to what was appropriate to the discovery of the particular items which he sought. Each case of this sort will, of course, have to be decided on its own facts. We merely hold today that where a police officer observes unusual conduct which leads him reasonably to conclude in light of his experience that criminal activity may be afoot and that the persons with whom he is dealing may be armed and presently dangerous, where in the course of investigating this behavior he identifies himself as a policeman and makes reasonable inquiries, and where nothing in the initial stages of the encounter serves to dispel his reasonable fear for his own or others' safety, he is entitled for the protection of himself and others in the area to conduct a carefully limited search of the outer clothing of such persons in an attempt to discover weapons which might be used to assault him. Such a search is a reasonable search under the Fourth Amendment, and any weapons seized may properly be introduced in evidence against the person from whom they were taken," 392 U.S. at 30-31.

. . [as a] . . . level of suspicion . . . obviously less demanding than that for probable cause. . . [but a level of] suspicion supported by articulable facts that criminal activity "may be afoot," even if the officer lacks probable cause," *United States v. Sokolow*, 490 U.S. 1, 7 (1989); as "a particularized and objective basis for suspecting legal wrongdoing," *United States v. Arvizu*, 534 U.S. 266, 273 (2002); and as "a particularized and objective basis for suspecting the person stopped of criminal activity," *Ornelas v. United States*, 517 U.S. at 690, citing, *United States v. Cortez*, 449 U.S. 411, 417-18 (1981).

It is a standard that may be invoked for a warrantless search or seizure at less than probable cause when in the totality of the circumstances at hand substantial public interests outweigh the minimal loss of personal freedom of movement and privacy imposed in a manner limited in time and nature. For example, *Brignoni-Ponce* acknowledged the substantial public interest in preventing foreign nationals from entering this country illegally, yet it refused approve even a limited detention by roving patrols near but not at the border when officers' suspicions were aroused solely by the Mexican ancestry of the detainees, *United States v. Brignoni-Ponce*, 422 U.S. 873, 883-84 (1975). *Brignoni-Ponce* explained, however, that

> *"[a]ny number of factors may be taken into account in deciding whether there is reasonable suspicion to stop a car in the border area. Officers may consider the characteristics of the area in which they encounter a vehicle. Its proximity to the border, the usual patterns of traffic on the particular road, and previous experience with alien traffic are all relevant. They also may consider information about recent illegal border crossings in the area. The driver's behavior may be relevant, as erratic driving or obvious attempts to evade officers can support a reasonable suspicion. Aspects of the vehicle itself may justify suspicion. For instance, officers say that certain station wagons, with large compartments for fold-down seats or spare tires are frequently used for transporting concealed aliens. The vehicle may appear to be heavily loaded, it may have an extraordinary number of passengers, or the officers may observe persons trying to hide," Id. at 884-85.*

Arvizu found reasonable suspicion in a border patrol case involving such circumstances:

It was reasonable for [Agent] Stoddard to infer from his observations, his registration check [of the minivan registered to an address in an area of the border town of Douglas, notorious for smuggling], and his experience as a border patrol agent that respondent had set out from Douglas along a little-traveled route used by smugglers to avoid the [route] 191 checkpoint. Stoddard's knowledge further supported a commonsense inference that respondent intended to pass through the area at a time when officers would be leaving their backroads

patrols to change shifts. The likelihood that respondent and his family were on a picnic outing was diminished by the fact that the minivan had turned away from the known recreational areas . . . . Corroborating this inference is the fact that recreational areas farther to the north would have been easier to reach by taking 191, as opposed to the 40-to-50 mile trip on unpaved and primitive roads [the minivan had taken]. The children's elevated knees [as they rode in the backs at of the van] suggested the existence of concealed cargo in the passenger compartment. Finally, for the reason we have given, Stoddard's assessment of respondent's reactions upon seeing him [slowing down dramatically, stiffening behind the wheel, and pretending to ignore the officer], and the children's mechanical-like waving [as if under instructions to allay suspicions], which continued for a full four to five minutes, were entitled to some weight. *United States v. Arvizu*, 534 U.S. 266, 277 (2002).

Sokolow and *Reid* illustrate the dividing line between facts that reflect reasonable suspicion and those that do not. *Sokolow* declared that

> *Paying $2,100 in cash for two airplane tickets is out of the ordinary, and it is even more out of the ordinary to pay that sum from a roll of $20 bills containing nearly twice that amount of cash. We also think the agents had a reasonable ground to believe that respondent was traveling under an alias. . . . While a trip from Honolulu to Miami, standing alone, is not a cause for any sort of suspicion, here there was more: surely few residents of Honolulu travel from that city for 20 hours to spend 48 hours in Miami during the month of July. Any one of these factors is not by itself proof of any illegal conduct and is quite consistent with innocent travel. But we think taken together they amount to reasonable suspicion. United States v. Sokolow, 490 U.S. 1, 8-9 (1989).*

This, *Sokolow* contrasted with the *Reid* conclusion under similar circumstances that no reasonable suspicion existed:

> *In Reid [v. Georgia, 448 U.S. 438, 441 (1980)], the Court held that a DEA agent stopped the defendant without reasonable suspicion. At the time of the stop, the agent knew that (1) the defendant flew into Atlanta from Fort Lauderdale, a source city for cocaine; (2) he arrived early in the morning, when police activity was believed to be at a low ebb; (3) he did not check his luggage; and (4) the defendant and his companion appeared to be attempting to hide the fact that they were together. 490 U.S. at 9-10 n.5.*

The Supreme Court's reasonable suspicion cases have generally involved situations like those in *Terry, Brignoni-Ponce, Ornelas, Arvizu, Sokolow*, and *Reid*, essentially stop and frisk or stop and question cases. *Knights* indicates that

the classification is coincidental not required. Citing *Terry* and *Brignoni-Ponce*, *Knights* reasoned that

> *Although the Fourth Amendment ordinarily requires the degree of probability embodied in the term probable cause, a lesser degree satisfies the Constitution when the balance of governmental and private interest makes such a standard reasonable. . . . When an officer has reasonable suspicion that a probationer subject to a search condition is engaged in criminal activity, there is enough likelihood that criminal conduct is occurring that an intrusion on the probationer's significantly diminished privacy interest is reasonable. United States v. Knights, 534 U.S. 112, 121 (2001).*

The utility company with whom Knights had a running dispute had experienced a rash of vandalism, *id*. at 114-15. The incidents occurred in close proximity to Knights' judicial appearances to answer company charges, *id*. at 115. In one instance, brass locks had been pried from a telecommunications vault and the contents burned using gasoline and ignited by a pipe bomb, *id*. Prior to the arson, officers had stopped Knights and an associate and observed pipes and gasoline in the truck in which they were riding, *id*. After the arson, officers approached the parked truck and saw a Molotov cocktail, gas can, and brass locks similar to those pried from the vandalized vault in the truck, *id*. Moreover, Knights was on probation hence might more reasonably be suspected of criminal involvement than an unconvicted individual, *id*. at 120. He had also agreed to warrantless, suspicionless searches as a condition of his probation thus supporting a reasonable inference that he would more readily and more quickly destroy incriminating evidence than might other offenders, *id*. This created a reasonable suspicion that Knights had engaged in criminal activity and justified the warrantless search of his apartment, *id*. at 121.

As to the third standard, the Supreme Court has found certain "special needs" may render a search reasonable for Fourth Amendment purposes notwithstanding the want of a warrant or probable cause. The special needs standard has been invoked in drug testing cases and a comparable standard applied in highway check point cases. In such instances, "[w]hen special needs, beyond the normal need for law enforcement, make the warrant and probable cause requirement impractical. . . the reasonableness of a search [is determined] by balancing the nature of the intrusion on the individual's privacy against the promotion of legitimate governmental interests," *Board of Education v. Earls*, 536 U.S. 822, 829 (2002). *Earls* found the testing of high school participants in extracurricular activities a reasonable means of protecting school children from drug use given the children's reduced privacy interests as students and the negligible intrusion associated with the search procedures, id. at 830-38. *Acton* came to the same conclusion after applying the same standard to assess the reasonableness of a drug testing program for student athletes, *Vernonia School District v. Acton*, 515 U.S. 646, 653-65 (1995). Using the same standard – "balanc[ing] the governmental and privacy interests to assess the practicality of

the warrant and probable cause requirements in the particular context" – *Skinner* found reasonable by Fourth Amendment standards the drug testing program for railroad employees given the public interest in railway safety, the reduced privacy interests reflected in the extensive safety regulation under which the railroad industry operates, and the minimally intrusive manner in which the searches were conducted, *Skinner v. Railway Labor Executives' Assoc.*, 489 U.S. 602, 619-33 (1989). Under the same standard, a drug testing program for Customs Service employees met Fourth Amendment reasonableness standards, given the public interest in the integrity as well as the unimpaired perception and judgment of those armed to enforce our drug laws balanced against the reduced privacy expectations of public employees occupying such positions and the minimally intrusive methods of search, *Treasury Employees v. Von Raab*, 489 U.S. 656, 670-72 (1989). The availability of the special needs reasonableness standard is not boundless. *Chandler* rejected a drug testing program imposed as a qualification to run for elective state office on the grounds that the need was symbolic not special, *Chandler v. Miller*, 520 U.S. 305, 322 (1997). The state had failed to show a public interest sufficient to outweigh the privacy interests at issue or to justify departure from ordinarily applicable Fourth Amendment warrant and probable cause requirements, *id.* at 318-22. There was no evidence of drug use among the state's elected officials, *id.* at 318-19. Nor was the candidate arranged and controlled testing procedure likely to address the problem if any existed, *id.* at 319-20.

Chandler makes it clear that the reasonableness standard, available "when special needs, beyond the normal need for law enforcement, make the warrant and probable cause requirement impractical" is inappropriate when the government's needs are not "special." Ferguson suggests that the reasonableness standard is inappropriate when the need is not beyond the normal need for law enforcement, *Ferguson v. City of Charleston*, 532 U.S. 67, (2001). The standard is inappropriate when the purpose for the challenged search is one not "divorced from the state's general interest in law enforcement. . . [but] ultimately indistinguishable from the general interest in crime control," that is, when "the immediate objective of the searches was to generate evidence for law enforcement purposes," *id.* at 80-81, 83.[3950]

In highway checkpoint cases, *Martinez-Fuerte* and *Sitz* apply a Fourth Amendment reasonable balancing test similar to that used in special needs cases. *Martinez-Fuerte* balanced the substantial public interest served in terms of smuggling and illegal entry by permanent highway checkpoints located

---

[3950] Ferguson involved a law enforcement initiated hospital drug testing program for pregnant patients under which those who tested positive were given the option of drug treatment or prosecution, id. at 71-73. It may appear from Lidster, discussed infra, which applies a special needs analysis to a highway checkpoint designed to secure evidence for law enforcement purposes, that Ferguson should be to understood to apply only when the evidence is to be used against the person searched.

proximate to the border against the reduced expectation of privacy associated with automobile use and the "quite limited" and "minimal" intrusion upon private interests, *United States v. Martinez-Fuerte*, 428 U.S. 543, 556-62 (1976). *Sitz* uses a similar standard for highway drunk-driving checkpoints – "balanc[ing] the state's interest in preventing drunken driving, the extent to which this system [of highway checkpoints] can reasonably be said to advance that interest, [against] the degree of intrusion upon individual motorists who are briefly stopped," *Michigan Department of State Police v. Sitz*, 496 U.S. 444, 455 (1990).

Faced with a drug interdiction highway checkpoint in which motorists were stopped while drug sniffing dogs circled their vehicles, *Edmond* distinguished *Martinez-Fuerte* as a "border" case and refused to abandon the probable cause or reasonable suspicion standards in favor of a reasonableness test:

> *[T]he Indianapolis checkpoints are far removed from the border context that was crucial in Martinez-Fuerte . . . . The primary purpose of the Indianapolis narcotics checkpoint is in the end to advance the general interest in crime control. We decline to suspend the usual requirement of individualized suspicion where the police seek to employ a checkpoint primarily for the ordinary enterprise of investigating crime. Indianapolis v. Edmond, 531 U.S. 32, 45-46 (2000).*

Lidster appears to limit the force of *Edmond* and perhaps of *Ferguson*. *Lidster* applied a balancing test to a highway checkpoint maintained for ordinary law enforcement, evidence gathering purposes, albeit probably not in anticipation that the evidence would be used against any of the motorists stopped:

> *[A]n Edmond-type presumptive rule of unconstitutionality does not apply here. That does not mean the stop is automatically, or even presumptively, constitutional. It simply means that we must judge its reasonableness, hence, its constitutionality, on the basis of individual circumstances. . . . [I]n judging reasonableness, we look to the gravity of the public concerns served by the seizure, the degree to which the seizure advances the public interest, and the severity of the interference with individual liberty.*
>
> *We now consider the reasonableness of the checkpoint stop before us in light of the factors just mentioned . . . . We hold that the stop was constitutional. The relevant public concern was grave. Police were investigating a crime that had resulted in a human death. . . .And the stop's objective was to help find the perpetrator of a specific and known crime, not of unknown crimes of a general sort. The stop advanced this grave public concern to a significant degree [by asking motorist if they had any relevant information and distributing a flyer]. . . . The stop took place about one week*

> *after the hit-and-run accident, on the same highway near the location of the accident, and at about the same time of night. And the police used the stops to obtain information from drivers, some of whom might well have been in the vicinity of the crime at the time it occurred. Most importantly, the stops interfered only minimally with the liberty of the sort the Fourth Amendment seeks to protect. Illinois v. Lidster, 540 U.S. 419, 426-27 (2004) (citations and accompanying parentheticals omitted).*

Probable cause is bit different under FISA. Ordinarily, probable cause speaks to the probability of the existence of a certain fact, *e.g.*, probable cause to believe a crime has been, is, or is about to be committed and that the search will result in the discovery of evidence or contraband. FISA authorizes issuance of a surveillance or search order predicated upon the probability of a possibility; the probability to believe that the foreign target of the order may engage in spying, or the probability to believe that the American target of the order may engage in criminal spying activities, 50 U.S.C. 1805(a)(3)(A), 1824(a)(3)(A), 1801(b)(1)(B), (b)(2)(A).[3951] But it is the predicate not the standard that is changed. The probable cause *standard* is the same in FISA as in a criminal context: would a prudent individual believe that a fact is probably true. It is the focus that is different. Would a prudent individual believe that spying may occur.

Charles Doyle
Senior Specialist
7-6006

[3951] FISA permits recourse to this reduced application of the probable cause standard in spy cases but not in terrorism cases, In re Sealed Case, 310 F.3d 717, 739 (F.I.S.Ct.Rev. 2002)("Congress allowed this lesser showing for clandestine intelligence activities – but not, notably, for other activities, including terrorism . . .").

The U.S. Foreign Intelligence Surveillance Court and the U.S. Foreign Intelligence Surveillance Court of Review: An Overview, RL33833 (January 24, 2007)

ELIZABETH B. BAZAN, CONGRESSIONAL RESEARCH SERV., THE U.S. FOREIGN INTELLIGENCE SURVEILLANCE COURT AND THE U.S. FOREIGN INTELLIGENCE SURVEILLANCE COURT OF REVIEW: AN OVERVIEW (2007), *available at* http://www.intelligencelaw.com/library/secondary/crs/pdf/RL33833_1-24-2007.pdf.

Order Code RL33833

January 24, 2007

Elizabeth B. Bazan
Legislative Attorney
American Law Division

Summary

The national debate regarding the National Security Agency's Terrorist Surveillance Program (TSP) focused congressional attention on the U.S. Foreign Intelligence Surveillance Court and the U.S. Foreign Intelligence Surveillance Court of Review created by the Foreign Intelligence Surveillance Act. Congressional interest in these courts has been heightened by the January 17, 2007, letter from Attorney General Gonzales to Chairman Leahy and Senator Specter advising them that a Foreign Intelligence Surveillance Court judge had "issued orders authorizing the Government to target for collection international communications into or out of the United States where there is probable cause to believe that one of the communicants is a member or agent of al Qaeda or an associated terrorist organization," stating that all surveillance previously occurring under the TSP will now be conducted subject to the approval of the Foreign Intelligence Surveillance Court, and noting that the President has determined not to reauthorize the TSP when the current authorization expires. This report examines the creation, membership, structure, and jurisdiction of these courts. It will be updated as subsequent events may require.

Introduction

The Foreign Intelligence Surveillance Act of 1978 (FISA), P.L. 95-511, 50 U.S.C. § 1801 et seq., as amended, provides a statutory framework for the U.S. government to engage in electronic surveillance[3952] and physical searches[3953] to

---

[3952] Under subsection 101(f) of FISA, 50 U.S.C. § 1801(f), the term "electronic surveillance" means:

obtain foreign intelligence information.[3954] It also provides a statutory structure for the installation and use of pen registers and trap and trace devices[3955] for use

---

(1) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes;

(2) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States, but does not include the acquisition of those communications of computer trespassers that would be permissible under section 2511(2)(i) of Title 18;

(3) the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States; or

(4) the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.

The provisions dealing with such electronic surveillance are found in title I of FISA, 50 U.S.C. § 1801 et seq., while the provisions addressing physical searches are located in title III of FISA, 50 U.S.C. § 1821 et seq.

[3953] Subsection 301(5) of FISA, 50 U.S.C. § 1821(5) defines the term "physical search" to mean: any physical intrusion within the United States into premises or property (including examination of the interior of property by technical means) that is intended to result in a seizure, reproduction, inspection, or alteration of information, material, or property, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, but does not include (A) "electronic surveillance", as defined in section 1801(f) of this title, or (B) the acquisition by the United States Government of foreign intelligence information from international or foreign communications, or foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic communications system, utilizing a means other than electronic surveillance as defined in section 1801(f) of this title.

[3954] Subsection 101(e) of FISA, 50 U.S.C. § 1801(e), defines "foreign intelligence information" to mean:

(1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against —

(A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

(B) sabotage or international terrorism by a foreign power or an agent of a foreign power; or

in federal investigations to obtain foreign intelligence information not concerning a U.S. person or to protect against international terrorism or clandestine intelligence activities. Such an investigation of a U.S. person may not be conducted solely on the basis of activities protected by the First Amendment to the Constitution.[3956]

In addition, FISA provides statutory authority for the Director of the Federal Bureau of Investigation (FBI) or his designee to seek a U.S. Foreign Intelligence Surveillance Court (FISC) order authorizing the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information not concerning a U.S. person or to protect against international terrorism or clandestine intelligence activities. Again, such an investigation of a U.S. person may not conducted solely on the basis of First Amendment-protected activities.[3957] A production order for tangible things may be accompanied by a nondisclosure order. Under Section 501(d) of FISA, 50 U.S.C. § 1861(d), no person shall disclose to any other person that the FBI has sought or obtained tangible things pursuant to an order under this section, other than to those persons to whom disclosure is necessary to

---

(C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or

(2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to —

(A) the national defense or the security of the United States; or

(B) the conduct of the foreign affairs of the United States.

[3955] Pen registers and trap and trace devices are addressed in title IV of FISA, 50 U.S.C. § 1841 et seq. Subsection 401(2) of FISA, 50 U.S.C. § 1841(2) defines "pen register" and "trap and trace device" by cross-reference to 18 U.S.C. § 3127. Under 18 U.S.C. § 3127(3), "pen register" is defined to mean: a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication, but such term does not include any device or process used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device or process used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business.

The term "trap and trace device" is defined under 18 U.S.C. § 3127(4) to mean: a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication.

[3956] Section 402 of FISA, 50 U.S.C. § 1842.

[3957] Section 501 of FISA, 50 U.S.C. § 1861.

comply with such order, an attorney to obtain legal advice or assistance with respect to the production of things in response to the order, or other persons as permitted by the Director of the FBI or the designee of the Director. A person to whom a disclosure is made is also subject to the nondisclosure requirements. Any person making or intending to make a disclosure to a person to whom disclosure is necessary to comply with the order or to whom disclosure is permitted by the Director of the FBI or his designee must, at the request of the Director or his designee, identify the person to whom disclosure is to be or has been made.

With limited exceptions,[3958] electronic surveillance and physical searches may be conducted under FISA pursuant to court orders issued by a judge of the FISC, and pen registers and trap and trace devices may be installed and used pursuant to the order of a FISC judge or a U.S. Magistrate Judge authorized to act in that judge's behalf. In all instances in which the production of any tangible thing is required under FISA, an order from a FISC judge or a U.S. Magistrate Judge authorized to act in the judge's behalf must be obtained. Appeals from the denial of applications for FISC orders approving electronic surveillance, physical search, or production of tangible things may be made by the U.S. government to the U.S. Foreign Intelligence Court of Review (Court of Review). If the denial of an application is upheld by the Court of Review, a petition for certiorari may be filed to the U.S. Supreme Court.

[3958] In the case of FISA electronic surveillance, those exceptions may be found in sections 102 (electronic surveillance for foreign intelligence purposes of certain types of foreign powers, as defined under section 101(a)(1), (2), and (3), 50 U.S.C. §§ 1801(a)(1), (2), and (3), upon Attorney General certification), 105(f) (emergency authorization by the Attorney General for up to 72 hours, if specified criteria are met, while an application for a FISC order is pursued), and 111 of FISA (authority electronic surveillance without a court order for up to 15 calendar days following a congressional declaration of war), 50 U.S.C. §§ 1802, 1805(f) and 1811, respectively. The exceptions to the requirement for a court order for FISA physical searches may be found at sections 302 (physical searches for foreign intelligence purposes with respect to certain types of foreign powers, as defined under section 101(a)(1), (2), and (3), 50 U.S.C. §§ 1801(a)(1), (2), and (3), upon Attorney General certification), 304(e) (emergency authorization by the Attorney General for up to 72 hours, if specified criteria are met, while an application for a FISC order is pursued) and 309 (authority for physical searches for up to 15 calendar days following a congressional declaration of war) of FISA, 50 U.S.C. §§ 1822, 1824(e), and 1829, respectively. The exceptions with respect to FISA pen registers and trap and trace devices may be found at sections 403 (emergency authorization by the Attorney General for up to 48 hours, if specified criteria are met, while an application for a FISC order is pursued) and 404 (authority for installation and use of pen registers and trap and trace devices for up to 15 calendar days following a congressional declaration of war) of FISA, 50 U.S.C. §§ 1843 and 1844, respectively.

A "foreign power," as defined in subsection (a)(1), (2), or (3), 50 U.S.C. §§ 1801(a)(1), (2), or (3), means "(1) a foreign government or any component thereof, whether or not recognized by the United States;" "(2) a faction of a foreign nation or nations, not substantially composed of United States persons;" or "(3) an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments."

This report discusses the creation and structure of the Foreign Intelligence Surveillance Court and the Foreign Intelligence Court of Review and their respective jurisdictions.

Membership and Structure of the U.S. Foreign Intelligence Surveillance Court and the U.S. Foreign Intelligence Surveillance Court of Review

Section 103 of the Foreign Intelligence Surveillance Act, as amended, 50 U.S.C. § 1803, establishes the U.S. Foreign Intelligence Surveillance Court and the U.S. Foreign Intelligence Surveillance Court of Review. The FISC is composed of 11 U.S. district court judges publicly designated by the Chief Justice of the United States from seven circuits, at least three of whom must reside within 20 miles of the District of Columbia.[3959] The Chief Justice publicly designates one of the FISC judges to be presiding judge.

Although there is a procedure for the publication of FISC opinions, such publication is extremely rare. Only one opinion has been published since the court's inception in 1978*, In re All Matters Submitted to the Foreign Intelligence Surveillance Court*, 218 F. Supp. 2d 611 (U.S. Foreign Intell. Surveil. Ct. 2002). Under Foreign Intelligence Surveillance Court Rule 5(c),

> *[o]n request by a Judge, the Presiding Judge, after consulting with other Judges of the Court, may direct that an Opinion be published. Before publications, the Opinion must be reviewed by the Executive Branch and redacted, as necessary, to ensure that properly classified information is appropriately protected pursuant to Executive Order 12958 as amended by Executive Order 13292 (or its successor).*

Three of the FISC judges who reside within 20 miles of the District of Columbia, or, if all of those judges are unavailable, other FISC judges designated by the presiding judge of the FISC, comprise a petition review pool that has jurisdiction to review petitions filed pursuant to subsection 501(f)(1) of FISA, 50 U.S.C. § 1861(f)(1), to challenge a production order for tangible things in a foreign intelligence, international terrorism, or clandestine intelligence activities investigation under section 501 of FISA, or a nondisclosure order imposed in connection with such a production order.[3960]

[3959] Subsection 103(a) of FISA, 50 U.S.C. § 1803(a).

[3960] Subsection 103(e)(1) of FISA, 50 U.S.C. § 1803(e)(1). Under subsection 103(f)(2) of FISA, 50 U.S.C. § 1803(f)(2), within sixty days after March 9, 2006, the FISC was directed to adopt and, consistent with the protection of national security, publish procedures for the review of petitions filed pursuant to subsection 501(f)(1) of FISA, 50 U.S.C. § 1861(f)(1) the petition review pool. Subsection 501(f)(2) requires that such procedures provide that review of a petition shall be

The Court of Review is composed of three judges publicly designated by the Chief Justice from the United States district courts or courts of appeals. The Chief Justice also publicly designates one of the three judges as the presiding judge of the court.[3961] Only one opinion has been published by the Court of Review, *In re Sealed Case*, 310 F.3d 717 (U.S. Foreign Intell. Surveil. Ct. Rev. 2002), which is the first opinion the court has issued.

Each FISC and Court of Review judge serves for a maximum of seven years and is not eligible for redesignation.[3962]

Jurisdiction of the U.S. Foreign Intelligence Surveillance Court

Electronic Surveillance and Physical Searches

The FISC has jurisdiction to hear applications[3963] for and to grant court orders approving electronic surveillance or physical searches anywhere in the United States to obtain foreign intelligence information under FISA.[3964] No FISC judge may hear an application for electronic surveillance or a physical search under FISA that has been denied previously by another FISC judge.[3965] In general, such applications are either granted, granted as modified, or denied.[3966] If a FISC

---

conducted in camera and also provide for the designation of an acting presiding judge of the panel.

[3961] Subsection 103(b) of FISA, 50 U.S.C. § 1803(b).

[3962] Subsection 103(d) of FISA, 50 U.S.C. § 1803(d).

[3963] The requirements for an application for a court order authorizing electronic surveillance under FISA are set out in section 104 of FISA, 50 U.S.C. § 104. The requirements for an application authorizing a physical search under FISA are set out in section 303 of FISA, 50 U.S.C. § 1823.

[3964] Subsection 103(a) of FISA, 50 U.S.C. § 1803(a) (electronic surveillance); subsection 302(c) of FISA, 50 U.S.C. § 1822(c) (physical searches).

[3965] *Id.*

[3966] The number of applications for electronic surveillance and physical searches under FISA granted, modified, and denied each year are reported to the Congress and to the Administrative Office in reports which are publicly available at [http://www.usdoj.gov/ag/readingroom/ag_foia1.htm], listed under "Annual Foreign Intelligence Surveillance Act Reports." Annual reporting of electronic surveillance information is required by the congressional oversight requirements of sections 107 of FISA, 50 U.S.C. § 1807. There is no precisely parallel reporting requirement in FISA regarding physical searches, pen registers and trap and trace devices, or production of tangible things. Section 306 of FISA, 50 U.S.C. § 1826, requires such reports to on a semi-annual rather than an annual basis on physical searches. There are more detailed semi-annual congressional reporting requirements placed upon the Attorney General with respect to electronic surveillances, section 108 of FISA, 50 U.S.C. §

judge denies an application for an order authorizing electronic surveillance under FISA,[3967] such judge shall provide immediately for the record a written statement of each reason for his or her decision and, on motion of the United States, the record shall be transmitted, under seal, to the Court of Review. Proceedings in the FISC, conducted pursuant to procedures adopted under subsection 103(f)(1) of FISA, 50 U.S.C. § 1803(f)(1),[3968] and proceedings of the Court of Review, are to be conducted as expeditiously as possible. The record of such proceedings, including applications made and orders granted, must be maintained under security measures established by the Chief Justice in consultation with the Attorney General and the Director of National Intelligence.[3969]

Pen Registers and Trap and Trace Devices

Either a FISC judge or a U.S. Magistrate Judge publicly designated by the Chief Justice to act on behalf of such judge may hear applications[3970] for and grant orders[3971] approving installation and use of pen registers and trap and trace

---

1808; physical searches, section 306 of FISA, 50 U.S.C. § 1826; and pen registers and trap and trace devices, section 406 of FISA, 50 U.S.C. § 1846; and annual reporting requirements with respect to production of tangible things, section 502 of FISA, 50 U.S.C. § 1862. Additional reporting requirements were added by the Intelligence Reform and Terrorism Prevention Act, P.L. 108-458, and codified as a new section 601 of FISA, 50 U.S.C. § 1871.

[3967] The requirements for issuance of a FISC order granting an application for electronic surveillance under FISA are set out in section 105 of FISA, 50 U.S.C. § 1805, while the requirements for issuance of a FISC order granting an application for a physical search under FISA are set out in section 304 of FISA, 50 U.S.C. § 1824.

[3968] *Id.* Under subsection 103(f)(1), 50 U.S.C. § 1803(f)(1), the FISC and the Court of Review may establish such rules and procedures, and take such actions, as are reasonably necessary to administer their responsibilities under FISA. Subsection 103(f)(2), 50 U.S.C. § 1803(f)(2), requires that rules and procedures so established, and any modifications thereto, must be recorded and must be transmitted to all of the judges on the FISC, all of the judges on the Court of Review, the Chief Justice of the United States, the House and Senate Judiciary Committees, the Senate Select Committee on Intelligence, and the House Permanent Select Committee on Intelligence. Such transmissions are to be submitted in unclassified form, but may include a classified annex. The FOREIGN INTELLIGENCE SURVEILLANCE COURT RULES OF PROCEDURE and the PROCEDURES FOR REVIEW OF PETITIONS FILED PURSUANT TO SECTION 501(F) OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED are available at [http://www.uscourts.gov/rules/fisa.html]. No rules of procedure for the Court of Review have been identified, although section 103(f)(1)t also provides that court with authority to establish such rules.

[3969] Subsection 103(c) of FISA , 50 U.S.C. § 1803(c) (electronic surveillance); subsection 302(e), 50 U.S.C. § 1822(e) (physical searches).

[3970] The requirements for an application for a pen register or trap and trace device under FISA are set forth in subsection 402(a)-(c) of FISA, 50 U.S.C. § 1842(a)-(c).

[3971] The requirements for issuance of a FISC order authorizing a pen register or trap and trace device under FISA are set forth in subsection 402(d) of FISA, 50 U.S.C. § 1842(d).

devices[3972] for an investigation to obtain foreign intelligence information not concerning a U.S. person[3973] or to protect against international terrorism[3974] or clandestine intelligence activities, provided that such investigation of a U.S. person is not conducted solely on the basis of activities protected by the First Amendment to the Constitution.

Production of Tangible Things

As in the case of pen registers and trap and trace devices, either a FISC judge or a U.S. Magistrate Judge publicly designated by the Chief Justice to act on behalf of such judge may hear applications[3975] for and grant orders[3976] approving production of any tangible thing[3977] for an investigation to obtain foreign intelligence information not concerning a U.S. person or to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a U.S. person is not conducted solely upon the basis of activities protected by the First Amendment to the Constitution.

[3972] Subsections 402(b) or (d), 50 U.S.C. §§ 1842(b) or (d).

[3973] Under subsection 101(i) of FISA, 50 U.S.C. § 1801(i), a "United States person" is defined to mean "a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 1101(a)(20) of Title 8), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in subsection (a)(1), (2), or (3) of this section." As noted above, a "foreign power," as defined in subsection (a)(1), (2), or (3), 50 U.S.C. §§ 1801(a)(1), (2), or (3), means "(1) a foreign government or any component thereof, whether or not recognized by the United States;" "(2) a faction of a foreign nation or nations, not substantially composed of United States persons;" or "(3) an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments."

[3974] Under subsection 101(c) of FISA, 50 U.S.C. § 1801(c), "international terrorism" means activities that "(1) involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or any State;" "(2) appear to be intended — (A) to intimidate or coerce a civilian population; (B) to influence the policy of a government by intimidation or coercion; or (C) to affect the conduct of a government by assassination or kidnapping;" and "(3) occur totally outside the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum."

[3975] The requirements for an application for a FISC order for production of tangible things under FISA are set forth in subsection 501(a) and (b) of FISA, 50 U.S.C. § 1861(a) and (b).

[3976] The requirements for issuance of a FISC order for production of tangible things under FISA are set forth in subsection 501(c) of FISA, 50 U.S.C. § 1861(c).

[3977] Subsections 501(b)(1) and (c), 50 U.S.C. §§ 1861(b)(1) and (c).

Review of Petitions Challenging Production Orders for Tangible Things or Related Nondisclosure Orders

A person who receives a production order may challenge that order by filing a petition with the petition review pool created by section 103(e) of FISA, 50 U.S.C. § 1803(e). The recipient of a production order must wait at least a year before challenging the nondisclosure order imposed in connection with that production order by filing a petition with the petition review pool to modify or set aside the nondisclosure order.[3978] If the judge denies a petition to modify or set aside a nondisclosure order, the recipient of such order must wait at least another year before filing another such petition with respect to such nondisclosure order. Any production or nondisclosure order not explicitly modified or set aside remains in full effect.[3979]

Judicial proceedings under this subsection are conducted under the PROCEDURES FOR REVIEW OF PETITIONS FILED PURSUANT TO SECTION 501(F) OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED, and are to be concluded as expeditiously as possible. The record of proceedings, including petitions filed, orders granted, and statements of reasons for decision, are maintained under security measures established by the Chief Justice of the United States, in consultation with the Attorney General and the Director of National Intelligence.[3980] All petitions under this subsection are filed under seal. In any proceedings under this subsection, the court shall, upon request of the government, review ex parte and in camera any government submission, or portions thereof, that may include classified information.[3981]

Motions to suppress information obtained by or derived from electronic surveillance, physical search, or pen registers or trap and trace devices under FISA are heard by U.S. district courts.

The procedure for challenging production or nondisclosure orders before the petition review pool of the FISC contrasts with that applicable to motions to suppress information obtained through or derived from electronic surveillance, physical search, or the installation and use of a pen register or trap and trace device under FISA, which a federal, state, or local government intends to use or disclose in a trial or other official proceeding. If a federal, state, or local government intends to use or disclose information obtained by or derived from a FISC order authorizing electronic surveillance, a physical search, or the use of a

---

[3978] Subsection 501(f)(2)(A)(i), 50 U.S.C. § 1861(f)(2)(A)(i).

[3979] Subsection 501(f)(2)(C) and (D), 50 U.S.C. § 1861(f)(2)(C) and (D).

[3980] Subsection 501(f)(4), 50 U.S.C. § 1861(f)(4).

[3981] Subsection 501(f)(5), 50 U.S.C. § 1861(f)(5).

pen register or trap and trace device, any challenges to the use or disclosure of that information must be made in the U.S. district court in which the motion or request is made, or, if the motion or request is made before another federal, state, or local authority, in the United States district court in the same district as that authority. Such challenges may include motions to suppress made under FISA by an "aggrieved person"[3982] against whom such information is intended to be used or disclosed; and any motion or request made by an aggrieved person pursuant to any other statute or rule of the United States or any state before any court or other authority of the United States or any state to discover or obtain applications or orders or other materials relating to FISA electronic surveillance, physical search, or use of a pen register or trap and trace device or to discover, obtain, or suppress evidence or information obtained or derived from the use of such investigative techniques under FISA.[3983]

Similar, but not identical, to the proceedings before the petition review panel regarding production orders or nondisclosure orders, the U.S. district court proceedings addressing motions to suppress information obtained by or derived from a FISA electronic surveillance, physical search, or pen register or trap and trace device, or seeking to discover or obtain related materials may be considered ex parte and in camera if the Attorney General files an affidavit under oath that disclosure or any adversary hearing would harm the national security of the United States.

If the United States district court determines that the electronic surveillance, physical search, or installation and use of the pen register or trap and trace device in regard to the aggrieved person was not lawfully authorized or conducted, it shall, in accordance with the requirements of law, suppress the evidence that was unlawfully obtained or derived therefrom or otherwise grant the motion of the aggrieved person. If the court determines that the electronic surveillance, physical search, or installation and use of a pen register or trap and trace device

---

[3982] The term "aggrieved person" is defined with respect to the use of electronic surveillance under FISA in subsection 101(k), 50 U.S.C. § 1801(k) to mean "a person who is the target of an electronic surveillance or any other person whose communications or activities were subject to electronic surveillance." When defined with respect to the use of physical searches under FISA, the term is defined by subsection 301(2) of FISA, 50 U.S.C. § 1821(2), to mean "a person whose premises, property, information, or material is the target of physical search or any other person whose premises, property, information, or material was subject to physical search." In connection with the use of a pen register or trap and trace device pursuant to FISA, the term is defined under subsection 401(3) of FISA, 50 U.S.C. § 1841(3) to mean any person "whose telephone line was subject to the installation or use of a pen register or trap and trace device authorized by this subchapter;" or "whose communication instrument or device was subject to the use of a pen register or trap and trace device authorized [under title IV of FISA] to capture incoming electronic or other communications impulses." The term is not used in connection with production of tangible things under title V of FISA, 50 U.S.C. § 1861-1862.

[3983] *See* subsection 106(c)-(h) of FISA, 50 U.S.C. § 1806(c)-(h) (electronic surveillance); subsection 305(d)-(i), 50 U.S.C. § 1825(d)-(i) (physical searches); 406(c)-(h) of FISA, 50 U.S.C. § 1846(c)-(h) (pen registers or trap and trace devices).

was lawfully authorized or conducted, it shall deny the motion of the aggrieved person except to the extent that due process requires discovery or disclosure.

Orders granting such motions or requests, decisions that a FISA electronic surveillance, physical search, or installation and use of a pen register or trap and trace device was not lawfully authorized or conducted, and orders of the United States district court requiring review or granting disclosure of applications, orders, or other materials relating thereto shall be final orders and binding upon all courts of the United States and the several states except a United States Court of Appeals or the Supreme Court.

Jurisdiction of the Court of Review

The government may seek review of a denial of an application for a court order under FISA authorizing electronic surveillance, physical search, or production of any tangible thing before the Court of Review.[3984] If the denial is upheld by the Court of Review, the government may seek U.S. Supreme Court review of the decision by a petition for certiorari.[3985]

In addition, the Court of Review has jurisdiction over petitions for review of a decision under section 501(f)(2) of FISA, 50 U.S.C. § 1861(f)(2), to affirm, modify, or set aside a production order or nondisclosure order filed by the government or any person receiving such an order.[3986] Upon the request of the government, any order setting aside a nondisclosure order shall be stayed pending such review.[3987]

The Court of Review shall provide for the record a written statement of the reasons for its decision and, on petition by the government or any person receiving such order for writ of certiorari, the record shall be transmitted under seal to the Supreme Court of the United States, which shall have jurisdiction to review such decision.

U.S. Supreme Court Jurisdiction

The U.S. Supreme Court has jurisdiction, on a petition for certiorari, to review decisions of the Court of Review affirming a denial of an application for an order authorizing electronic surveillance, physical searches, production orders, or nondisclosure orders under FISA.

[3984] The Foreign Intelligence Surveillance Court of Review is established under subsection 103(b), 50 U.S.C. § 1803(b). The Chief Justice publicly designates one of the Court of Review judges to be the presiding judge.

[3985] The U.S. Supreme Court is given jurisdiction over denials of applications which have been upheld by the Court of Review in subsection 103(b), 50 U.S.C. § 1803(b).

[3986] Subsection 501(f)(3) of FISA, 50 U.S.C. § 1861(f)(3).

[3987] Subsection 501(f)(2)(C)(iii), 50 U.S.C. § 1861(f)(2)(C)(iii).

Intelligence Reform and Terrorism Prevention Act of 2004: "Lone Wolf" Amendment to the Foreign Intelligence Surveillance Act, RS22011 (December 29, 2004)

ELIZABETH B. BAZAN, CONGRESSIONAL RESEARCH SERV., INTELLIGENCE REFORM AND TERRORISM PREVENTION ACT OF 2004: "LONE WOLF" AMENDMENT TO THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (2004), *available at* http://www.intelligencelaw.com/library/secondary/crs/pdf/RS22011_12-29-2004.pdf.

Order Code RS22011
December 29, 2004

CRS Report for Congress

Elizabeth B. Bazan
Legislative Attorney
American Law Division

Summary

Section 6001 of the Intelligence Reform and Terrorism Prevention Act of 2004, P.L. 108-458, amended the definition of "agent of a foreign power" in the Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. § 1801(b)(1), to add a new category of covered individuals. Under the new "lone wolf" provision, a non-United States person who engages in international terrorism or activities in preparation for international terrorism is deemed to be an "agent of a foreign power" under FISA. The new provision does not change the procedures to be used to apply for a court order authorizing electronic surveillance or a physical search under FISA. If an order is sought under this definition of an "agent of a foreign power," however, the applicant is not required to demonstrate a connection between the target of the electronic surveillance or the physical search and a foreign nation, foreign group, or international terrorist group. Nor does the Foreign Intelligence Surveillance Court (FISC), in approving such an order, haveto find probable cause to believe that such a connection existed. Rather, if the court authorizes such a surveillance or physical search using this new definition of "agent of a foreign power," the FISC judge has to find, in pertinent part, that, based upon the information provided by the applicant for the order, the target had engaged in or was engaging in international terrorism or activities in preparation therefor.

Introduction

The Foreign Intelligence Surveillance Act of 1978 (FISA), as amended, 50 U.S.C. §§ 1801-1862, provides a statutory framework for the use of electronic surveillance or physical searches to acquire foreign intelligence information.[3988] It also provides a vehicle for the use of pen registers or trap and trace devices in investigations conducted by the FBI under guidelines approved by the Attorney General under E.O. 12333 or a successor order to acquire foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities. In permitting the use of pen registers and trap and trace devices, FISA provides that such an investigation of a United States person may not be conducted solely on the basis of activities protected under the First Amendment of the U.S. Constitution. In addition, FISA provides a means for the government to obtain access to certain business records or other tangible things for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities, again provided that such investigation of a United States person may not be conducted solely based upon First Amendment protected activities.

An applicant for a court order under FISA authorizing electronic surveillance or a physical search must include in the application, among other information, a statement of the facts or circumstances relied upon by the applicant to justify his or her belief that the target of the electronic surveillance or the physical search is a "foreign power" or an "agent of a foreign power" as those terms are defined in Section 101 of the act, 50 U.S.C. § 1801. Section 6001 of the Intelligence Reform and Terrorism Prevention Act of 2004,

P.L. 108-458, amended the definition of "agent of a foreign power" under Section 101(b)(1) of FISA, 50 U.S.C. § 1801(b)(1), to add a new category of non-United States persons covered under this definition. The amendment added a new subparagraph 101(b)(1)(C), 50 U.S.C. § 1801(b)(1)(C) (as reflected in italics below). As amended by Section 6001, "agent of a foreign power" under FISA means:

(1) any person other than a United States person, who–

[3988] As part of the application process for a Foreign Intelligence Surveillance Court order authorizing electronic surveillance or a physical search, the Assistant to the President for National Security Affairs or an executive branch national security or defense official or officials designated by the President must certify, among other things, that the he or she deems the information sought to be foreign intelligence information, that a significant purpose of the electronic surveillance or physical search is to obtain foreign intelligence information, and that such information cannot reasonably be obtained by normal investigative techniques. The certification that "a significant purpose" of the electronic surveillance or physical search is obtaining foreign intelligence information has been interpreted to provide latitude for such investigative techniques to be used for law enforcement purposes as well, so long as a significant foreign intelligence purpose also exists. *See* In re Sealed Case, 310 F.3d 717, 732-736 (U.S. Foreign Intell. Surveil. Ct. Rev. 2002).

(A) acts in the United States as an officer or employee of a foreign power, or as a member of a foreign power as defined in subsection (a)(4) of this section;[3989]
(B) acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of the United States, when the circumstances of such person's presence in the United States indicate that such person may engage in such activities in the United States, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities;
(C) engages in international terrorism or activities in preparation therefore [sic]; or[3990]
(2) any person who–
(A) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States;
(B) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States;

[3989] "Foreign power" is defined for purposes of FISA in Section 101(a) of the act, 50 U.S.C. § 1801(a), to mean: (1) a foreign government or any component thereof, whether or not recognized by the United States; (2) a faction of a foreign nation or nations, not substantially composed of United States persons; (3) an entity that is openly acknowledged by a foreign government or governments to be directed or controlled by such foreign government or governments; (4) a group engaged in international terrorism or activities in preparation therefor; (5) a foreign-based political organization, not substantially composed of United States persons; or (6) an entity that is directed and controlled by a foreign government or governments.

[3990] In light of the phrasing in the definition of "foreign power" in 50 U.S.C. § 1801(a)(4) and of the definition of "agent of a foreign power" in 50 U.S.C. § 1801(b)(2)(C), "therefore" as it appears in the new subsection (C) added to 50 U.S.C. § 1801(b)(1) seems likely to have been intended to read "therefor." "International terrorism" is defined in 50 U.S.C. § 1801(c) to mean activities that:

(1) involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or any State;

(2) appear to be intended–

(A) to intimidate or coerce a civilian population;

(B) to influence the policy of a government by intimidation or coercion; or

(C) to affect the conduct of a government by assassination or kidnaping; and

(3) occur totally outside the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum.

(C) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power;
(D) knowingly enters the United States under a false or fraudulent identity for or on behalf of a foreign power or, while in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power; or
(E) knowingly aids or abets any person in the conduct of activities described in subparagraph (A), (B), or (C) or knowingly conspires with any person to engage in activities described in subparagraph (A), (B), or (C).

The term "United States person" in FISA is used to describe a citizen of the United States, a permanent resident alien, an unincorporated association a substantial number of the members of which are U.S. citizens or permanent resident aliens, or a corporation which is incorporated in the United States. This term does not include a corporation or association which is a foreign power as that term is defined in Section 101(a)(1), (2), or (3) of FISA, 50 U.S.C. § 1801(a)(1), (2), or (3).[3991] Thus, under the new subsection added by Section 6001 of P.L. 108-458, a non-U.S. person who engages in international terrorism or in activities in preparation for international terrorism may be considered an "agent of a foreign power" for purposes of FISA. An applicant for a FISA court order using this definition of "agent of a foreign power" need not provide facts and circumstances justifying a belief that the target of the electronic surveillance or physical search is connected to a foreign nation, foreign group, or international terrorist organization. Nor does the Foreign Intelligence Surveillance Court (FISC), in granting such an application, have to find probable cause, based on the facts submitted by the applicant, to believe that such a connection to a foreign nation, foreign group, or international terrorist group exists in order to find probable cause to believe that the target of the electronic surveillance or physical search is a foreign power or an agent of a foreign power.[3992]

[3991] 50 U.S.C. § 1801(i).
[3992] If a FISC judge is to enter an ex parte order granting an application for electronic surveillance under 50 U.S.C. § 1805, he or she must find that:

(1) the President has authorized the Attorney General to approve applications for electronic surveillance for foreign intelligence information;
(2) the application has been made by a Federal officer and approved by the Attorney General;
(3) on the basis of the facts submitted by the applicant there is probable cause to believe that–
(A) the target of the electronic surveillance is a foreign power or an agent of a foreign power; Provided, That no United States person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States; and
(B) each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used by a foreign power or an agent of a foreign power;
(4) the proposed minimization procedures meet the definition of minimization procedures under section 1801(h) of this title; and
(5) the application which has been filed contains all statements and certifications required by section 1804 of this title and, if the target is a United States person, the certification or

This amendment does not change the procedures to be followed by an applicant seeking a FISA order for electronic surveillance or for a physical search. However, the facts and circumstances used by the applicant to demonstrate the basis of his or her belief that the target of the electronic surveillance or physical search is a "foreign power or an agent of a foreign power" will vary depending upon the definition of "foreign power" or "agent of a foreign power" relied upon in the application. Nor does the amendment alter the requirements for such a court order except to the extent that the factual underpinnings for the probable cause determination will also vary depending upon definition of "foreign power" or "agent of a foreign power" relied upon in a given case.

The amendment to the definition of "agent of a foreign power" in Section 6001 of P.L. 108-458 is made subject to the sunset provisions of Section 224 of the USA PATRIOT Act, P.L. 107-56, including the exception provided in subsection (b) of Sec. 224. Therefore, the new Section 101(b)(1)(C) of FISA, 50 U.S.C. § 1801(b)(1)(C), would sunset on December 31, 2005, except with respect to any foreign intelligence investigation begun before that date or any criminal offense or potential offense that began or occurred before that date. Thus, where a foreign intelligence investigation was underway before December 31, 2005, or a criminal offense or potential offense began or was committed[3993] before that date, the definition of "agent of a foreign power" added by Section 6001 of P.L. 108-458 would still be available. Under those circumstances, an application for a FISA court order for electronic surveillance or a physical search involving a "lone wolf" target could still be pursued after December 31, 2005, and a court order issued authorizing such surveillance or search. Section 6002 of P.L. 108-458 expanded the semi-annual reporting requirements under FISA.[3994] As part of these

---

certifications are not clearly erroneous on the basis of statements made under section 1804(a)(7)(E) of this title and any other information furnished under section 1804(d) of this title.

50 U.S.C. § 1805(a). In making a determination of probable cause under Section 1805(a)(3), the FISC judge may consider past activities of the target as well as facts and circumstances relating to current or future activities of the target. 50 U.S.C. § 1805(b). Similar findings must be made by a FISC judge issuing an order granting an application for a physical search under FISA, 50 U.S.C. § 1824(a), (b). Each provision also requires that a judge approving electronic surveillance or a physical search, respectively, under FISA must include certain specifications and directions in the orders issued. 50 U.S.C. §§ 1805(c), 1824(c).

[3993] As discussed in greater depth in footnote 1, supra, FISA may be used for law enforcement purposes so long as "a significant purpose" of the investigation is to obtain foreign intelligence information.

[3994] Section 6002 of P.L. 108-458 redesignated the existing Title VI of FISA as Title VII and former Section 601 as Section 701. A new Section 601 of FISA was added, which required the Attorney General, on a semiannual basis, to submit to the House Permanent Select Committee on Intelligence, the Senate Select Committee on Intelligence and the House and Senate Judiciary Committees, in a manner consistent with the protection of the national security, reports setting forth with respect to the preceding six month period:

requirements, starting within six months of the date of enactment of P.L. 108-458, the Attorney General must submit semiannual reports, each covering the previous six month period, to the House Permanent Select Committee on Intelligence, the Senate Select Committee on Intelligence, the House Judiciary Committee, and the Senate Judiciary Committee, in a manner consistent with protection of national security, including, among other things, the number of individuals covered by an order issued pursuant to the new definition of "agent of a foreign power" in Section 101(b)(1)(C), 50 U.S.C. § 1801(b)(1)(C).

---

(1) the aggregate number of persons targeted for orders issued under this Act, including a breakdown of those targeted for–

(A) electronic surveillance under section 105 [50 U.S.C. § 1805];

(B) physical searches under section 304 [50 U.S.C. § 1824];

(C) pen registers under section 402 [50 U.S.C. § 1842]; and

(D) access to records under section 501 [50 U.S.C. § 1861];

(2) the number of individuals covered by an order issued pursuant to section 101(b)(1)(C) [50 U.S.C. § 1801(b)(1)(C)];

(3) the number of times that the Attorney General has authorized that information obtained under this Act may be used in a criminal proceeding or any information derived therefrom may be used in a criminal proceeding;

(4) a summary of significant legal interpretations of this Act involving matters before the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review, including interpretations presented in applications or pleadings filed with the Foreign Intelligence Surveillance Court or the Foreign Intelligence Court of Review by the Department of Justice; and

(5) copies of all decisions (not including orders) or opinions of the Foreign Intelligence Surveillance Court or Foreign Intelligence Surveillance Court of Review that include significant construction or interpretation of the provisions of this Act.

Amendments to the Foreign Intelligence Surveillance Act Set to Expire in 2009, R40138 (March 16, 2009).

EDWARD C. LIU, CONGRESSIONAL RESEARCH SERV., AMENDMENTS TO THE FOREIGN INTELLIGENCE SURVEILLANCE ACT SET TO EXPIRE IN 2009 (2009), , *available at* http://www.intelligencelaw.com/library/secondary/crs/pdf/R40138_3-16-2009.pdf.

Edward C. Liu
Legislative Attorney
eliu@crs.loc.gov, 7-9166
March 16, 2009

Congressional Research Service

7-5700
www.crs.gov
R40138

Summary

Several recent amendments to the Foreign Intelligence Surveillance Act (FISA) will sunset on December 31, 2009. H.R. 1467, introduced in the 111th Congress, would extend these three provisions until December 31, 2019.

Section 6001(a) of the Intelligence Reform and Terrorism Protection Act (IRTPA), also known as the "lone wolf" provision, changed the rules regarding the types of individuals that could be targets of FISA-authorized searches. It permits surveillance of non-U.S. persons engaged in international terrorism, without requiring evidence linking those persons to an identifiable foreign power or terrorist organization.

Section 206 of the USA PATRIOT ACT amended FISA to permit multipoint, or "roving," wiretaps by adding flexibility to the degree of specificity with which the location or facility subject to electronic surveillance under FISA must be identified.

Section 215 of the USA PATRIOT ACT enlarged the scope of documents that could be sought under FISA, and lowered the standard required before issuance of a court order compelling the production of documents.

While these provisions will cease to be prospectively effective on December 31, 2009, a grandfather clause permits them to remain effective with respect to investigations that began, or potential offenses that took place, before the sunset date.

Overview

The Foreign Intelligence Surveillance Act (FISA) provides a statutory framework for government agencies to seek a court order from a specialized Foreign Intelligence Surveillance Court (FISC) authorizing the collection of foreign intelligence information via electronic surveillance[3995] or physical searches.[3996] FISA also provides procedures governing the use of pen registers and trap and trace devices,[3997] and access to certain business records for foreign intelligence collection.[3998] The extent to which the Fourth Amendment's warrant requirement is applicable to the government's collection of foreign intelligence is unclear.[3999] But, FISA's statutory requirements arguably provide a minimum standard that must be met before foreign intelligence searches or surveillance may be conducted by the government.[4000]

A substantial purpose of a FISA court order must be the collection of foreign intelligence information.[4001] Therefore, the procedures for obtaining a court

---

[3995] 50 U.S.C. §§ 1801-1808 (2008).

[3996] 50 U.S.C. §§ 1822-1826 (2008).

[3997] 50 U.S.C. §§ 1841-1846 (2008). Pen registers capture the numbers dialed on a telephone line; trap and trace devices identify the originating number of a call on a particular phone line. See 18 U.S.C. § 3127(3)-(4) (2008).

[3998] 50 U.S.C. §§ 1861-1862 (2008).

[3999] The Supreme Court has held that the Fourth Amendment's warrant requirement applies in instances of domestic security surveillance. U.S. v. U.S. District Court, 407 U.S. 297, 323-4 (1972) (also referred to as the Keith case, so named for the District Court judge that initially ordered disclosure of unlawful warrantless electronic surveillance to the defendants). But, see In re Directives, 2008 U.S. App. LEXIS 27417 (U.S. Foreign Intell. Survellance Ct. Rev. 2008) (holding that the foreign intelligence surveillance of targets reasonably believed to be outside of the U.S. qualifies for the "special needs" exception to the warrant requirement). See, also, CRS Report WD00002, Presidential Authority to Conduct Warrantless Electronic Surveillance to Gather Foreign Intelligence Information, by Elizabeth B. Bazan and Jennifer K. Elsea, at 9-12 (discussing courts' differing application of the Fourth Amendment to searches for the purpose of foreign intelligence collection).

[4000] *But, see* CRS Report WD00002, Presidential Authority to Conduct Warrantless Electronic Surveillance to Gather Foreign Intelligence Information, by Elizabeth B. Bazan and Jennifer K. Elsea, at 29-33 ("While the congressional intent to cabin the President's exercise of any inherent constitutional authority to engage in foreign intelligence electronic surveillance may be clear from the exclusivity provision in FISA and from the legislative history of the measure, some support may be drawn from the [Foreign Intelligence Surveillance] Court of Review's decision in In re Sealed Case for the position that the President continues to have the power to authorize warrantless electronic surveillance to gather foreign intelligence outside the FISA framework").

[4001] See, e.g., 50 U.S.C. § 1804(a)(7)(B) (2008). Prior to 2001, the statute had required that "the purpose" of a FISA warrant be foreign intelligence collection.

order under FISA differ from the procedures used in the criminal law enforcement context. While both FISA orders and criminal warrants incorporate impartial judicial review to determine if probable cause exists, the propositions that must be supported by probable cause are substantially different in either case. In the case of a FISA court order, the FISC must find probable cause to believe both (1) that the person targeted by the order is a foreign power or its agent, and (2) that the subject of the search (i.e., the telecommunications or place to be searched) will be used by the target.[4002]

Three relatively recent amendments to FISA will expire on December 31, 2009. These provisions are:

- Section 6001(a) of the Intelligence Reform and Terrorism Protection Act (IRTPA), also known as the "lone wolf" provision, which simplified the evidentiary showing needed to obtain a FISA court order to target individuals, other than U.S. citizens or permanent residents, engaged in international terrorism;[4003]
- Section 206 of the USA PATRIOT Act, which permitted multipoint, or "roving," wiretaps in certain circumstances by adding flexibility to the manner in which the subject of a FISA court order is specified;[4004] and
- Section 215 of the PATRIOT Act, which broadened the types of records that could be made accessible to the government under FISA.[4005]

This report will discuss the state of the law prior to enactment of these provisions, the changes wrought by each of these provisions, and the expected state of the law after the pending sunset date.

"Lone Wolf" Terrorists

Commonly referred to as the "lone wolf" provision, § 6001(a) of IRTPA simplified the evidentiary standard used to determine whether an individual, other than a citizen or a permanent resident of the U.S., who was engaged in international terrorism, could be the target of a FISA court order. This amendment did not modify other standards used to determine the secondary question of whether the

---

[4002] 50 U.S.C. § 1805(a)(3) (2008). In contrast, federal criminal search warrants require probable cause to believe that instrumentalities, evidence, or fruits of a crime will be found in the place to be searched. See Fed. R. Crim. P. 41(c). Criminal warrants authorizing electronic surveillance additionally require probable cause to believe that the target is engaged in criminal activities, that normal investigative techniques are insufficient, and that the facilities that are the subject of surveillance will be used by the target. 18 U.S.C. § 2518(3) (2008).

[4003] P.L. 108-458, § 6001(a).

[4004] P.L. 107-56, § 206, codified at 50 U.S.C. § 1805(c)(2)(B) (2008).

[4005] P.L. 107-56, § 215, codified at 50 U.S.C. §§ 1861-2 (2008).

electronic surveillance or a physical search of the subject of a court order is justified in a specific situation.

Historical Context

The historical impetus behind enactment of the "lone wolf" provision came to light shortly after the terrorist attacks of September 11, 2001. During the examination of the events leading up to those attacks, it was reported that investigations into one of the individuals believed to be responsible for those attacks had been potentially hampered by the legal requirements governing FISA.[4006] Specifically, Federal Bureau of Investigations (FBI) agents investigating Zacarias Moussaoui suspected him of planning a terrorist attack involving piloting commercial airliners, and had detained him in October of 2001 based on a violation of immigration law.[4007] The FBI agents had then sought a court order under FISA to examine the contents of Moussaoui's laptop computer.[4008] But, the agency apparently concluded that it had insufficient information at that time to demonstrate that Moussaoui was an agent of a foreign power, as required by FISA.[4009]

FISA, as it then existed, would have authorized, among other things, physical searches of a laptop if probable cause existed to believe the laptop was owned or used by a foreign power or its agent.[4010] The definition of a "foreign power" included "groups engaged in international terrorism or activities in preparation therefor."[4011] Individuals involved in international terrorism for or on behalf of those groups were considered "agents of a foreign power."[4012] In the weeks leading up to the attacks, it appears that the FBI encountered an actual or perceived insufficiency of information demonstrating probable cause to believe

---

[4006] NAT'L COMM. ON TERRORIST ATTACKS UPON THE U.S., The 9/11 Commission Report, at 273-274 [hereinafter "9/11 Comm'n Rep."].

[4007] Id. at 273. Moussaoui, a French national, was present in the United States with an expired visa.

[4008] Id. at 273-274.

[4009] Id. at 274. Based upon this conclusion, the FBI "declined to submit a FISA application" to the FISC.

[4010] 50 U.S.C. § 1821-1824 (2001).

[4011] 50 U.S.C. § 1801(a)(4) (2001). At the time, foreign powers also included foreign governments, entities controlled by those governments, and factions of foreign nations and foreign-based political organizations that are not substantially composed of United States persons. Id. at § (a)(1-6).

[4012] 50 U.S.C. § 1801(b)(2)(C) (2001).

that Moussaoui was acting for or on behalf of an identifiable group engaged in international terrorism.[4013]

Legislative Responses

Following these revelations, a number of legislative proposals were put forth to amend the definition of "agents of a foreign power" under FISA so that individuals engaged in international terrorism did not need to be linked to a specific foreign power.[4014] One such amendment was ultimately enacted with passage of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA).[4015] This "lone wolf" provision provides that persons, other than citizens or permanent residents of the U.S., that are engaged in international terrorism are presumptively considered to be agents of a foreign power.[4016] Enactment of this provision obviated any need to provide an evidentiary connection between that individual and a foreign government or terrorist group.

Critics of the "lone wolf" provision argued that the laptop in the Moussaoui case could have been lawfully searched under FISA or the laws governing generic criminal warrants.[4017] Critics also expressed concern that the simplified "lone wolf" standard would lead to "FISA serving as a substitute for some of our most important criminal laws."[4018]

On the other hand, proponents of the "lone wolf" provision note that the increased self-organization among terror networks has made proving connections to identifiable groups more difficult, and that a "lone wolf" provision is necessary to combat terrorists who use a modern organizational structure.[4019]

Sunset

[4013] See 9/11 Comm'n Rep. at 274. It is unclear whether a search of Moussaoui's laptop before September 11, 2001, would have provided enough information to prevent or minimize those attacks.

[4014] S. 2586, 107th Cong. (2002); S. 113, 108th Cong. (2003).

[4015] P.L. 108-458, § 6001(a).

[4016] 50 U.S.C. § 1801(b)(1)(3) (2008).

[4017] See S.Rept. 108-40 at 33-41 (additional views of Sen. Leahy and Sen. Feingold on a similar "lone wolf" provision in S. 113).

[4018] Id. at 73 (additional views of Sen. Feingold).

[4019] S.Rept. 108-40 at 4-6.

The "lone wolf" provision was originally scheduled to sunset on December 31, 2005.[4020] However, § 103 of the USA PATRIOT Improvement and Reauthorization Act of 2005 extended the sunset date of the "lone wolf" provision until December 31, 2009.[4021] The original sunset provision also included a grandfather clause which allowed it to continue to be effective with respect to investigations that began, or potential offenses that took place, before the provision's sunset date.[4022] For example, if an individual is engaged in international terrorism on December 30, 2009, he may still be considered a "lone wolf" for FISA court orders sought after the provision has expired. This grandfather clause is unaffected by the extension of the sunset date to December 31, 2009.

Roving Wiretaps

Section 206 of the USA PATRIOT ACT amended FISA to permit multipoint, or "roving," wiretaps by adding flexibility to the degree of specificity with which the location or facility subject to electronic surveillance under FISA must be identified.[4023] It is often colloquially described as allowing FISA wiretaps to target persons rather than places.

Background

Prior to enactment of § 206, the scope of electronic surveillance authorized by a court order was limited in two ways. First, the location or facility that was the subject of surveillance had to be identified.[4024] Second, only identifiable third-parties could be directed to facilitate electronic surveillance by the government.[4025] Conducting electronic surveillance frequently requires the assistance of telecommunications providers, landlords, or other third-parties. Furthermore, telecommunications providers are generally prohibited from assisting in electronic surveillance for foreign intelligence purposes, except as authorized by FISA.[4026] In cases where the location or facility was unknown, the identity of the person who would need to assist the government could not be specified in the order. Therefore, limiting the class of persons who could be

---

[4020] P.L. 108-458, § 6001(b).

[4021] P.L. 109-177, § 103.

[4022] P.L. 108-458, § 6001(b) (referencing PATRIOT Act sunset provision in P.L. 107-56, § 224(b)).

[4023] P.L. 107-56, § 206, codified at 50 U.S.C. § 1805(c)(2)(B) (2008).

[4024] See 50 U.S.C. § 1805(c)(1)(B) (2001) (requiring FISA warrants to specify the "nature and location of each of the facilities or places at which electronic surveillance will be directed").

[4025] See 50 U.S.C. § 1805(c)(2)(B) (2001).

[4026] See 50 U.S.C. §§ 1809(a) and 1810 (2008).

directed to assist the government by a FISA court order effectively limited the reach of FISA court orders to known and identifiable locations.

Section 206 and "Other Persons"

Section 206 of the USA PATRIOT ACT amended § 105(c)(2)(B) of FISA to provide that "in circumstances where the Court finds, based on specific facts provided in the application, that the actions of the target of the application may have the effect of thwarting the identification of a specified person" a FISA order may direct "other persons" to assist with the electronic surveillance.[4027] In a technical amendment later that year, the requirement that the order specify the location of the surveillance was also changed so that this requirement only applied if the facilities or places were known.[4028] These modifications had the effect of permitting FISA orders to direct unspecified individuals to assist the government in performing electronic surveillance, thus permitting court orders to authorize surveillance of places or locations that were unknown at the time the order was issued.

This section was further amended by the USA PATRIOT Improvement and Reauthorization Act of 2005 to require that the FISC be notified within 10 days after "surveillance begins to be directed at any new facility or place."[4029] In addition, the FISC must be told the nature and location of each new facility or place, the facts and circumstances relied upon to justify the new surveillance, a statement of any proposed minimization procedures that differ from those contained in the original application or order, and the total number of facilities or places subject to surveillance under the authority of the present order.[4030]

Particularity Requirement of the Fourth Amendment

The Fourth Amendment imposes specific requirements upon the issuance of warrants authorizing searches of "persons, houses, papers, and effects."[4031] One of the requirements, referred to as the particularity requirement, states that warrants shall "particularly describ[e] the place to be searched."[4032] Under FISA,

---

[4027] P.L. 107-56, § 206, codified at 50 U.S.C. § 1805(c)(2)(B) (2008).

[4028] P.L. 107-108, § 314(a)(2)(A).

[4029] P.L. 109-177, § 108(b)(4), codified at 50 U.S.C. § 1805(c)(3) (2008). This deadline for notification can be extended to up to 60 days by the FISC upon a showing of good cause.

[4030] Id.

[4031] U.S. CONST. amend. IV. The Supreme Court has held that electronic surveillance of private conversations qualifies as a search for purposes of the Fourth Amendment.

[4032] Id.

roving wiretaps are not required to identify the location that may be subject to surveillance. Therefore, some may argue that roving wiretaps do not comport with the particularity requirement of the Fourth Amendment. Initially, it is not clear that the Fourth Amendment would require that searches for foreign intelligence information be supported by a warrant,[4033] but prior legal challenges to similar provisions of Title III of the Omnibus Crime Control and Safe Streets Act (Title III) may be instructive in the event that challenges to § 206 are brought alleging violations of the particularity requirement of the Fourth Amendment.

Similar roving wiretaps have been permitted under Title III since 1986, in cases where the target of the surveillance takes actions to thwart such surveillance.[4034] The procedures under Title III are similar to those currently used under FISA, but two significant differences exist. First, a roving wiretap under Title III must definitively identify the target of the surveillance.[4035] Fixed wiretaps under Title III and all wiretaps under FISA need only identify the target if the target's identity is known. FISA permits roving wiretaps via court orders that only provide a specific description of the target.[4036] Second, Title III requires that the surveilled individuals be notified of the surveillance, generally 90 days after surveillance terminates.[4037] FISA contains no similar notification provision.

In *United States v. Petti*, the Ninth Circuit was presented with a challenge to a roving wiretap under Title III alleging that roving wiretaps do not satisfy the particularity requirement of the Fourth Amendment.[4038] The Ninth Circuit initially noted that

> *the test for determining the sufficiency of the warrant description is whether the place to be searched is described with sufficient particularity to enable the executing officer to locate and identify the premises with reasonable effort, and whether there is any reasonable probability that another premise might be mistakenly searched.*[4039]

[4033] See supra footnote 5.

[4034] Electronic Communications Privacy Act of 1986, P.L. 99-508, § 106(d)(3), codified at 18 U.S.C. § 2518(11) (2008).

[4035] 18 U.S.C. § 2518(11)(b)(ii) (2008).

[4036] See 50 U.S.C. §§ 1804(a)(3), 1805(c)(1)(A) (2008).

[4037] 18 U.S.C. § 2518(8)(d) (2008). This notification may be postponed upon an ex parte showing of good cause.

[4038] U.S. v. Petti, 973 F.2d 1441, 1443-5 (9th Cir. 1992).

[4039] Id. at 1444 (internal quotation marks omitted).

Applying this test, the Ninth Circuit held that roving wiretaps under Title III satisfied the particularity clause of the Fourth Amendment.[4040] The court in this case relied upon the fact that targets of roving wiretaps had to be identified and that they were only available where the target's actions indicated an intent to thwart electronic surveillance.[4041]

Critics of roving wiretaps under FISA may argue that § 206 increases the likelihood that innocent conversations will be the subject of electronic surveillance. They may further argue that the threat of these accidental searches of innocent persons is precisely the type of injury sought to be prevented by the particularity clause of the Fourth Amendment. Such a threat may be particularly acute in this case given the fact that there is no requirement under FISA that the target of a roving wiretap be identified, although the target must be specifically described.[4042]

Sunset

Section 206 of the USA PATRIOT ACT was initially set to sunset on December 31, 2005.[4043] But, it was extended by the USA PATRIOT Improvement and Reauthorization Act of 2005 until December 31, 2009. After this date, § 105(c)(2) of FISA will read as it read on October 25, 2001,[4044] eliminating the authority for FISA court orders to direct other unspecified persons to assist with electronic surveillance.[4045]

The original sunset provision also provided a grandfather clause for investigations that began, or potential offenses that took place, before the date of

---

[4040] Id. at 1445.

[4041] Id. See also, United States v. Bianco, 998 F.2d 1112, 1124 (2nd Cir. 1993) (similarly holding that a similar provision authorizing roving bugs under Title III was constitutional).

[4042] 50 U.S.C. §§ 1804(a)(3), 1805(c)(1)(B) (2008).

[4043] P.L. 107-56, § 224(a).

[4044] P.L. 109-177, § 102(b). The relevant section of FISA will then provide that, upon the request of the applicant, a specified communication or other common carrier, landlord, custodian, or other specified person furnish the applicant forthwith all information, facilities, or technical assistance necessary to accomplish the electronic surveillance in such a manner as will protect its secrecy and produce a minimum of interference with the services that such carrier, landlord, custodian, or other person is providing that target of electronic surveillance. 50 U.S.C. § 1805(c)(2) (2001).

[4045] The sunset will not repeal the provision of FISA that permits a FISA warrant to fail to identify facilities or places that will be subject to electronic surveillance. However, the authority for most new roving wiretaps may be effectively repealed because new orders may not direct unspecified persons to assist with surveillance.

the provision's expiration.[4046] For example, if an individual is engaged in international terrorism on December 30, 2009, he may be the target of a roving wiretap under FISA even after authority for new roving wiretaps has expired. This grandfather clause is unaffected by the extension of the sunset date to December 31, 2009.

Access to Business Records Under FISA

Section 215 of the USA PATRIOT ACT enlarged the scope of documents that could be sought under FISA, as well as lowered the standard required before a court order could be issued compelling the production of documents.

Background

In 1976, the Supreme Court held that an individual's bank account records did not fall within the protection of the Fourth Amendment's prohibition on unreasonable searches and seizures.[4047] Subsequently, Congress passed laws protecting various types of transactional information, but built in exceptions providing some access to statutorily protected records for counter intelligence purposes.[4048] Similar statutory protections were also enacted for electronic communications records and credit bureau records.[4049] As with financial records, these later statutes also included exceptions for access to records relevant to counter intelligence investigations. These exceptions comprise the authority for so-called national security letters (NSL), which can be used to compel the production of certain types of records.

In 1998, Congress amended FISA to provide access to certain records that were not available through NSL's.[4050] Specifically, it created a mechanism for federal investigators to compel the production of records from common carriers, public accommodation facilities, storage facilities, and vehicle rental facilities.[4051] Applications for orders under this section had to be made by FBI agents with a rank of Assistant Special Agent in Charge or higher and investigations could not be conducted solely on the basis of activities protected by the First

---

[4046] P.L. 107-56, § 224(b).

[4047] U.S. v. Miller, 425 U.S. 435 (1976).

[4048] See CRS Report RL33320, National Security Letters in Foreign Intelligence Investigations: Legal Background and Recent Amendments, by Charles Doyle, at 3.

[4049] Id. at 3-4.

[4050] P.L. 105-272, tit. VI, § 602.

[4051] 50 U.S.C. § 1862(a) (2001).

Amendment.[4052] Under these procedures the FISC would issue an order if, inter alia, the application contained "specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or an agent of a foreign power."[4053] Recipients of an order under this section were required to comply with it, and were also prohibited from disclosing to others that an order had been issued.[4054]

Expansion of Scope of Documents Subject to FISA

In 2001, § 215 of the USA PATRIOT ACT made several changes to the procedures under FISA for obtaining business records.[4055] Among these was an expansion of the scope of records that were subject to compulsory production. Whereas, prior to enactment of the USA PATRIOT ACT, only records from four explicit categories of businesses could be obtained, § 215 applied to "any tangible things."[4056]

This expanded scope drew strong opposition from the library community, so much so that § 215 came to be known as the "library provision" despite the fact that the original text of the provision did not mention libraries.[4057] Opposition from this group appears to have been primarily based upon the chilling effect such access could have on the exercise of First Amendment rights and purported intrusions into areas protected by the Fourth Amendment.[4058] Opposition from library advocates may have also been a residual response to prior attempts by the FBI to gather foreign intelligence information from library staff and records during the Cold War.[4059]

[4052] 50 U.S.C. § 1862(a)(1) (2001).

[4053] 50 U.S.C. § 1862(b)(2)(B) (2001).

[4054] 50 U.S.C. § 1862(d)(1)-(2) (2001).

[4055] P.L. 107-56, § 215 codified at 50 U.S.C. § 1862(a)-(b) (2008).

[4056] 50 U.S.C. § 1861(a)(1) (2008).

[4057] E.g. Richard B. Schmitt, House Weakens Patriot Act's 'Library Provision', L.A. TIMES, June 16, 2005, at A-1.

[4058] See, e.g., AMERICAN LIBRARY ASSOCIATION, Resolution on the USA Patriot Act and Related Measures That Infringe on the Rights of Library Users, Jan. 29, 2003, available at http://www.ala.org; Judith King, Director ALA Office for Intellectual Freedom, Letter to the Editor, FBI 'Fishing Expeditions' Librarians' Biggest Worry, WALL ST. J., May 24, 2004, at A15; David Mehegan, Reading Over Your Shoulder: The Push Is On To Shelve Part Of The Patriot Act, BOSTON GLOBE, Mar. 9, 2004, at E5.

[4059] See Ulrika Ekman Ault, The FBI's Library Awareness Program: Is Big Brother Reading Over Your Shoulder?, 65 N.Y.U. L. REV. 1532 (1990).

In response to these concerns, a library-specific amendment was made to the § 215 procedures by the USA PATRIOT Improvement and Reauthorization Act of 2005. Under this amendment, if the records sought were "library circulation records, library patron lists, book sales records, book customer lists, firearms sales records, tax return records, educational records, or medical records containing information that would identify a person," the application has to be approved by one of three high-ranking FBI officers.[4060]

Changes to the Standard of Review

Section 215 of the USA PATRIOT ACT also modified the standard that had to be met before an order compelling production of documents could issue from the FISC. Prior to enactment of § 215, an applicant had to have "specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or an agent of a foreign power."[4061] In contrast, under § 215 as originally enacted, the applicant only needed to "specify that the records concerned [were] sought for a [foreign intelligence investigation.]"[4062]

Subsequently, in 2005, Congress further amended FISA procedures for obtaining business records as part of the USA PATRIOT Improvement and Reauthorization Act of 2005. The applicable standard was again changed to require "a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to a [foreign intelligence investigation.]"[4063] Records are presumptively relevant if they pertain to

- a foreign power or an agent of a foreign power;
- the activities of a suspected agent of a foreign power who is the subject of such authorized investigation; or
- an individual in contact with, or known to, a suspected agent of a foreign power who is the subject of such authorized investigation;

Nondisclosure and Judicial Review

Orders issued under § 215 are accompanied by nondisclosure orders prohibiting the recipients from disclosing that the FBI has sought or obtained any tangible

---

[4060] Applications for these records could be made only by the Director of the Federal Bureau of Investigation, the Deputy Director of the Federal Bureau of Investigation, or the Executive Assistant Director for National Security. This authority cannot be further delegated. 50 U.S.C. § 1861(a)(3) (2008).

[4061] 50 U.S.C. § 1862(b)(2)(B) (2001).

[4062] P.L. 107-56, § 215.

[4063] P.L. 109-177, § 106(b).

things pursuant to a FISA order. However, the recipient may discuss the order with other persons as necessary to comply with the order, with an attorney to obtain legal advice or assistance, or with other persons as permitted by the FBI.[4064] The recipient must identify persons to whom disclosure has been made, or is intended to be made, if the FBI requests, except that attorneys with whom the recipient has consulted do not need to be identified.[4065]

The USA PATRIOT Improvement and Reauthorization Act of 2005 also provided procedures for recipients of § 215 orders to challenge the judicial review of orders compelling the production of business records.[4066] Once a petition for review is submitted by a recipient, a FISC judge must determine whether the petition is frivolous within 72 hours.[4067] If the petition is frivolous, it must be denied and the order affirmed.[4068] Otherwise the order may be modified or set aside if it does not meet the requirements of FISA or is otherwise unlawful.[4069] Appeals by either party may be heard by the Foreign Intelligence Court of Review and the Supreme Court.[4070]

Judicial review of nondisclosure orders operates under a similar procedure,[4071] but such orders are not reviewable for one year after they are initially issued.[4072] If the petition is not determined to be frivolous, a nondisclosure order may be set aside if there is no reason to believe that disclosure may endanger the national security of the United States, interfere with a criminal, counterterrorism, or counterintelligence investigation, interfere with diplomatic relations, or endanger the life or physical safety of any person.[4073]

A petition to set aside a nondisclosure order may be defeated if the government certifies that disclosure would endanger the national security or interfere with

---

[4064] 50 U.S.C. § 1861(d)(1) (2008).

[4065] 50 U.S.C. § 1861(d)(2)(C) (2008).

[4066] 50 U.S.C. § 1861(f)(2)(A)(i) (2008).

[4067] 50 U.S.C. § 1861(f)(2)(A)(ii) (2008).

[4068] Id.

[4069] 50 U.S.C. § 1861(f)(2)(B) (2008).

[4070] 50 U.S.C. § 1861(f)(3) (2008).

[4071] Judicial review of nondisclosure orders was added by P.L. 109-178, § 3.

[4072] 50 U.S.C. § 1861(f)(2)(A)(i) (2008).

[4073] 50 U.S.C. § 1861(f)(2)(C)(i) (2008).

diplomatic relations.[4074] Absent any finding of bad faith, such a certification is to be treated as conclusive by the FISC. If a petition is denied, either due to a certification described above, frivolity, or otherwise, the petitioner may not challenge the nondisclosure order for another year.[4075] Appeals by either party may be heard by the Foreign Intelligence Court of Review and the Supreme Court.[4076]

DOJ OIG Report

The USA PATRIOT Improvement and Reauthorization Act of 2005 directed the Inspector General of the Department of Justice (OIG) to audit the FBI's use of § 215 authority and report its findings to Congress.[4077] The OIG's most recent audit for calendar year 2006 was released in March of 2008.[4078] According to that report, 21 applications for § 215 orders were made in 2006, of which six were withdrawn and 15 granted. The report also indicates that one of the six applications was withdrawn because the FISC indicated that it would not sign the order due to First Amendment concerns.[4079]

Sunset

Section 215 of the USA PATRIOT ACT was initially set to sunset on December 31, 2005.[4080] But, it was extended by the USA PATRIOT Improvement and Reauthorization Act of 2005 until December 31, 2009. After this date, § 501 and 502 of FISA will read as they read on October 25, 2001,[4081] restricting the types of business records that are subject to FISA and reinstating the requirement for

---

[4074] Such certifications must be made by the Attorney General, Deputy Attorney General, an Assistant Attorney General, or the Director of the Federal Bureau of Investigation. 50 U.S.C. § 1861(f)(2)(C)(ii) (2008).

[4075] 50 U.S.C. § 1861(f)(2)(C)(iii) (2008).

[4076] 50 U.S.C. § 1861(f)(3) (2008).

[4077] P.L. 109-177, § 106A.

[4078] OFFICE OF THE INSPECTOR GENERAL, DEP'T OF JUSTICE, A Review of the FBI's Use of Section 215 Orders for Business Records in 2006, Mar. 2008, available at http://www.usdoj.gov/oig/special/s0803a/final.pdf.

[4079] Id. at 33. In indicating that it would deny the application, the FISC appears to have decided that "the facts were too 'thin' and that this request implicated the target's First Amendment rights." Id. at 68.

[4080] P.L. 107-56, § 224(a).

[4081] P.L. 109-177, § 102(b). Access will then be limited to records held by common carriers, public accommodation facilities, physical storage facilities, and vehicle rental facilities. 50 U.S.C. § 1862(c)(2) (2001).

"specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or an agent of a foreign power."[4082]

The original sunset provision also provided a grandfather clause for investigations that began, or potential offenses that took place, before the date of the provision's expiration.[4083] For example, in the case of investigations that had already begun before December 30, 2009, a broader scope of records could be made accessible to the government under FISA even after the expiration date. This grandfather clause is unaffected by the extension of the sunset date to December 31, 2009.

Proposed Legislation in the 111th Congress

H.R. 1467, the Safe and Secure America Act of 2009, would extend all three provisions for ten years, creating a new sunset date of December 31, 2019. This bill would not otherwise change any of the procedures or legal standards relevant to these three provisions.

[4082] 50 U.S.C. § 1862(b)(2)(B) (2001).

[4083] P.L. 107-56, § 224(b).

The Foreign Intelligence Surveillance Act: A Sketch of Selected Issues, RL34566 (July 7, 2008)

ELIZABETH B. BAZAN, CONGRESSIONAL RESEARCH SERV., THE FOREIGN INTELLIGENCE SURVEILLANCE ACT: A SKETCH OF SELECTED ISSUES (2008), *available at* http://www.intelligencelaw.com/library/secondary/crs/pdf/RL34566_7-7-2008.pdf.

Order Code RL34566

July 7, 2008
Elizabeth B. Bazan
Legislative Attorney
American Law Division

Summary

The current legislative and oversight activity with respect to electronic surveillance under the Foreign Intelligence Surveillance Act (FISA) has drawn national attention to several overarching issues. This report briefly outlines three such issues and touches upon some of the perspectives reflected in the ongoing debate. These issues include the inherent and often dynamic tension between national security and civil liberties, particularly rights of privacy and free speech; the need for the intelligence community to be able to efficiently and effectively collect foreig intelligence information from the communications of foreign persons located outside the United States in a changing, fast-paced, and technologically sophisticated international environment or from United States persons abroad, and the differing approaches suggested to meet this need; and limitations of liability for those electronic communication service providers who furnish aid to the federal government in its foreign intelligence collection. Two constitutional provisions, in particular, are implicated in this debate — the Fourth and First Amendments. This report briefly examines these issues and sets them in context.

The 110th Congress has been very active in developing and considering measures to amend FISA to address these issues. On August 5, 2007, the Protect America Act, P.L. 110-55, was enacted into law. It expired on February 16, 2008, after passage of a fifteen-day extension to its original sunset date. See P.L. 110-182. On November 15, 2007, the House of Representatives passed H.R. 3773, the RESTORE Act of 2007. On February 12, 2008, the Senate passed S. 2248, as amended, then struck all but the enacting clause of H.R. 3773, and inserted the text of S. 2248, as amended, in its stead. On March 14, 2008, the House passed an amendment to the Senate amendment to H.R. 3773. After months of intensive negotiations, on June 19, 2008, a compromise bill, H.R. 6304, was introduced in the House. It was passed by the House the following day. On June 26, 2008, a cloture motion on the measure was presented in the Senate. Further activity on

H.R. 6304 is anticipated after the Senate returns from the July 4th recess. Each of these bills differ somewhat in content and approach from one another.

This report consists of the text of CRS Report RL34279, The Foreign Intelligence Surveillance Act: An Overview of Selected Issues, by Elizabeth B. Bazan, without the accompanying footnotes. It will be updated as needed.

Introduction

The Foreign Intelligence Surveillance Act of 1978, P.L. 95-511, 92 Stat. 1783 (October 25, 1978), 50 U.S.C. §§ 1801 et seq. (hereinafter FISA), was enacted in response both to the Committee to Study Government Operations with Respect to Intelligence Activities (otherwise known as the Church Committee) revelations regarding past abuses of electronic surveillance for national security purposes and to the somewhat uncertain state of the law on the subject. While FISA now provides a statutory framework for gathering foreign intelligence information through the use of electronic surveillance, physical searches, and pen registers or trap and trace devices, and access to business records and other tangible things, the 1978 Act dealt only with electronic surveillance. The provisions passed almost 30 years ago became Title I of FISA. As originally enacted, the measure provided a statutory framework for collection of foreign intelligence information through the use of electronic surveillance of communications of foreign powers or agents of foreign powers, as those terms were defined in the act. The act has been amended repeatedly in the intervening years in an effort to address changing circumstances. Then, as now, the Congress sought to strike a balance between national security interests and civil liberties.

A number of FISA bills have received recent attention in the 110th Congress. On August, 5, 2007, the Protect America Act, P.L. 110-55 was enacted into law. This measure, in part, construed the term "electronic surveillance" under FISA not to include surveillance directed at a person reasonably believed to be located outside of the United States, and provided authority for warrantless acquisition of foreign intelligence information concerning persons reasonably believed to be located outside the United States where certain criteria were satisfied. As originally enacted, the measure was to sunset on February 1, 2008. On January 29, 2008, both the House and the Senate passed H.R. 5104, a 15-day extension to the sunset for the Protect America Act, to allow further time to consider, pass, and go to conference on proposed legislation to amend FISA, while ensuring that the intelligence community would have the authority it needed in the intervening period. It was enacted into law as P.L. 110-182.

The House of Representatives passed H.R. 3773, the Responsible Electronic Surveillance That is Overseen, Reviewed, and Effective Act of 2007 or the RESTORE Act of 2007 on November 15, 2007, while S. 2248 was reported out of the Senate Select Committee on Intelligence on October 26, 2007, and an amendment in the nature of a substitute to S. 2248, the Foreign Intelligence

Surveillance Amendments Act of 2007 or the FISA Amendments Act of 2007, was reported out of the Senate Judiciary Committee on November 16, 2007. A modified version of the Senate Judiciary Committee's amendment in the nature of a substitute to S. 2248 was tabled.

The Senate passed S. 2248, the FISA Amendments Act of 2008, as amended, on February 12, 2008. After striking all but the enacting clause of H.R. 3773 and inserting the text of S. 2248 as amended, the Senate then passed H.R. 3773, the FISA Amendments Act of 2008.

On March 14, 2008, the House passed an amendment to the Senate amendment to H.R. 3773. After intensive negotiations, a compromise bill, H.R. 6304, was introduced in the House on June 19, 2008. The measure passed the House the following day. A cloture motion on the measure was presented in the Senate on June 26, 2008. Further activity on H.R. 6304 is anticipated after the Senate returns from the July 4th recess.

The current legislative and oversight activity with respect to electronic surveillance under FISA has drawn national attention to several overarching issues. This report briefly outlines three such issues and touches upon some of the perspectives reflected in the ongoing debate. These issues include the inherent and often dynamic tension between national security and civil liberties, particularly rights of privacy and free speech; the need identified by the Director of National Intelligence (DNI), Admiral Mike McConnell, for the intelligence community to be able to efficiently and effectively collect foreign intelligence information from the communications of foreign persons located outside the United States in a changing, fast-paced, and technologically sophisticated international environment, and the differing approaches suggested to meet this need; and limitations of liabilityfor those electronic communication service providers who furnish aid to the federal government in its foreign intelligence collection. This report briefly examines these issues and sets them in context.

Tension Between National Security and Civil Liberties

Two constitutional provisions, in particular, are implicated in this debate — the Fourth and First Amendments. The Fourth Amendment to the U.S. Constitution provides:

> *The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrant shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.*

The First Amendment to the U.S. Constitution provides:

> *Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.*

As the Fourth Amendment protects the people's privacy rights, so the First Amendment reflects a recognition of the value of free expression of ideas and lawful political dissent to the preservation of a free society.

In introducing S. 1566, the bill that became the Foreign Intelligence Surveillance Act of 1978, P.L. 95-511, Senator Edward Kennedy addressed the challenge of striking an appropriate balance between the legitimate government need to safeguard the nation against the intelligence activities of foreign agents and the concomitant need to protect civil liberties, stating:

> *The complexity of the problem must not be underestimated. Electronic surveillance can be a useful tool for the Government's gathering of certain kinds of information; yet, if abused, it can also constitute a particularly indiscriminate and penetrating invasion of the privacy of our citizens. My objective over the past six years has been to reach some kind of fair balance that will protect the security of the United States without infringing on our citizens' human liberties and rights.*

This sentiment was echoed in a hearing before the Senate Judiciary Committee on S. 1566 when Attorney General Griffin Bell testified for the Carter Administration in favor of the measure:

> *I believe this bill is remarkable not only in the way it has been developed, but also in the fact that for the first time in our society the clandestine intelligence activities of our government shall be subject to the regulation and receive the positive authority of a public law for all to inspect. President Carter stated it very well in announcing this bill when he said that "one of the most difficult tasks in a free society like our own is the correlation between adequate intelligence to guarantee our nation's security on the one hand, and the preservation of basic human rights on the other." It is a very delicate balance to strike, but one which is necessary in our society, and a balance which cannot be achieved by sacrificing either our nation's security or our civil liberties. . . .*

In providing background for its report on H.R. 7308, the House FISA bill then under consideration, the House Permanent Select Committee on Intelligence noted:

The history and law relating to electronic surveillance for "national security" purposes have revolved around the competing demands of the President's constitutional powers to gather intelligence deemed necessary to the security of the nation and the requirements of the fourth amendment. The U.S. Supreme Court has never expressly decided the issue of whether the President has the constitutional authority to authorize warrantless electronic surveillance for foreign intelligence purposes. Whether or not the President has an "inherent power" to engage in or authorize warrantless electronic surveillance and, if such power exists, what limitations, if any, restrict the scope of that power, are issues that have troubled constitutional scholars for decades.

Electronic surveillance can provide vital information needed to identify those who are acting or preparing to act against U.S. interests for the benefit of foreign powers, including those engaged in espionage, sabotage, or terrorist acts or who otherwise pose a threat to the nation or its citizens, and to uncover their plans or activities. This information may not be readily uncovered by other investigative means. Thus, surveillance can provide a valuable tool for protecting the security of the nation and its citizens. However, this investigative technique, by its nature, can intrude into the privacy of both the target of the surveillance and those with whom the target communicates. It also has the potential of chilling political discussion and lawful dissent.

The framing of the current debate on this issue flows, in part, from questions arising with respect to the Terrorist Surveillance Program (TSP), first revealed in press accounts in December 2005. While little information regarding the details of this NSA program is publicly available, the President has indicated that, "since shortly after September 11, 2001, he had authorized the National Security Agency (NSA) to intercept international communications into and out of the United States of persons linked to al Queda or related terrorist organizations. The purpose of the intercepts is to establish an early warning system to detect and prevent another catastrophic terrorist attack on the United States." Concerns surrounding the TSP have led to continuing congressional oversight and a number of legislative proposals focused upon providing the intelligence community with the tools it needs for foreign intelligence collection to protect the United States and its citizens, while also protecting the civil liberties of those impacted by such collection.

The current level of complexity and sophistication of global communications technology can provide both increased opportunities for lawful private communications and public debate, and increased means for communications between those engaged in criminal wrongdoing or plans or actions which pose a threat to U.S. national security. While this presents challenges to intelligence collection for foreign intelligence purposes, the government has moved to utilize these new technologies for both law enforcement and intelligence purposes. The balance between these important governmental needs and protections of

constitutionally protected privacy interests and First Amendment protected activities is dynamic, and there can be differences of opinion as to where the appropriate balance point between them may be found.

Collection of Foreign Intelligence Information from Foreign Persons and United States Persons Located Abroad

A second, related issue in the current debate concerns the appropriate circumstances or standards for collection of foreign intelligence information from foreign persons and United States persons abroad. This issue can best be understood when set in the context of recent developments, to the extent that pertinent information is publicly available.

In July 2007, an unclassified summary of the National Intelligence Estimate (NIE) on "The Terrorist Threat to the US Homeland" was released. The NIE expressed the judgement, in part, that the U.S. Homeland will face a persistent and evolving threat over the next three years, the main threat coming from Islamic terrorist groups and cells, particularly al Qaeda.

In a January 17, 2007, letter to Chairman Leahy and Ranking Member Specter of the Senate Judiciary Committee, then Attorney General Gonzales advised them that, on January 10, 2007, a Foreign Intelligence Surveillance Court judge "issued orders authorizing the Government to target for collection international communications into or out of the United States where there is probable cause to believe that one of the communicants is a member or agent of al Qaeda or an associated terrorist organization." The Attorney General stated that, in light of these orders, which "will allow the necessary speed and agility," all surveillance previously occurring under the Terrorist Surveillance Program (TSP) would now be conducted subject to the approval of the FISC. He indicated further that, under these circumstances, the President had determined not to reauthorize the TSP when the then current authorization expired. The Attorney General also noted that the Intelligence Committees had been briefed on the highly classified details of the FISC orders and advised Chairman Leahy and Senator Specter that he had directed the Acting Assistant Attorney General for the Office of Legal Counsel and the Assistant Attorney General for National Security to provide them a classified briefing on the details of the orders. Because the contents of these orders remain classified, the scope of or limitations with respect to any authority that may have been provided remain unknown.

On April 13, 2007, the Administration announced that it had submitted draft legislation to the Congress regarding modernization of FISA. This draft legislation included a proposed new section 102A of FISA which would authorize the President, acting through the Attorney General, to permit acquisition of foreign intelligence information for up to one year concerning persons reasonably

believed to be outside the United States if the Attorney General certifies in writing under oath that he has made four specific determinations.

On August 2, 2007, the DNI released a statement on "Modernization of the Foreign Intelligence Surveillance Act." In his statement, Admiral McConnell regarded such modernization as necessary to respond to technological changes and to meet the Nation's current intelligence collection needs. He viewed it as essential for the intelligence community to provide warning of threats to the United States. One of two critically needed changes perceived by the DNI was his view that a court order should not be required for gathering foreign intelligence from foreign targets located overseas. Admiral McConnell did, however, indicate that he would be willing to agree to court review, after commencement of needed collection, of the procedures by which foreign intelligence is gathered through classified methods directed at foreigners outside the United States.

Some news accounts suggest that a FISC court ruling this Spring may have limited the authority of the United States, in certain circumstances, to engage in surveillance of foreign conversations taking place outside the United States. Admiral McConnell stated in remarks included in the transcript of an interview published in the El Paso Times on August 22, 2007, that on or about May of this year, when another judge of the FISC considered an application for renewal or extension of the surveillance approved under the January 10 orders, that judge interpreted the requirements of FISA differently from the judge who had issued the January 10 orders, and deemed a FISA warrant necessary for surveillance of wire communications of a foreign person in a foreign country.

Views differ as to the scope of the need and the means by which this need may be met. Can this concern be addressed by solutions directed solely at electronic surveillance or acquisitions without a court order from the FISC of communications between foreign persons in communication with other foreign persons all located outside the United States, whether or not those communications are routed through the United States at some point in their transmission? Or must the solution be crafted in such a way as to permit such surveillance or acquisitions of the communications of foreign persons located abroad, whether they may be in communication only with other non-U.S. persons, or both non-U.S. persons and U.S. persons, located outside the United States? What is required if some of the communications of the foreign person targeted in the surveillance or acquisition are with U.S. persons or non-U.S. persons located in the United States? May such foreign intelligence be collected from U.S. persons abroad without a Foreign Intelligence Surveillance Court order pursuant to a certification by the Attorney General or the Attorney General and the DNI jointly or whether a court order is required prudentially or constitutionally under the Fourth Amendment?

<u>Legislative Response: Foreign Intelligence Surveillance of Foreign Persons Abroad</u>

On August 5, 2007, the Protect America Act of 2007 was enacted into law, P.L. 110-55, which provided that "[n]othing in the definition of electronic surveillance under section 101(f) [of FISA] shall be construed to encompass surveillance directed at a person reasonably believed to be located outside of the United States." It also created a new procedure under section 105B(a) of FISA under which the Attorney General and the DNI, for periods of up to one year, may authorize acquisition of foreign intelligence information concerning persons reasonably believed to be outside the United States, if the Attorney General and the DNI determine, based on the information provided to them, that five criteria have been met. This authority was similar, but not identical to, the proposed section 102A of FISA in the Administration's draft bill. P.L. 110-55 expired on February 16, 2008, after passage of a fifteen-day extension to its original sunset date. Under the transitional provisions in Section 6 of the Protect America Act, the acquisitions authorized while the act was in force may continue until their expiration.

H.R. 3773 as originally passed by the House provides that no court order is needed for electronic surveillance directed at acquisition of the contents of communications between persons not known to be U.S. persons who are reasonably believed to be located outside the United States, without regard to whether the communication is transmitted through the United States or the surveillance device is located in the United States. If the communications of a U.S. person are inadvertently intercepted, stringent constraints upon retention, disclosure, dissemination, or use would apply. However, the bill provides for a FISC order for acquisitions for up to one year of communications of non-U.S. persons reasonably believed to be outside the U.S. to collect most types of foreign intelligence information by targeting those persons, where those persons may be communicating with persons inside the United States. It also establishes requirements for such acquisitions.

The Senate amendment to H.R. 3773 would permit the Attorney General and the DNI to jointly authorize, for up to one year, targeting of persons reasonably believed to be outside the U.S. to acquire foreign intelligence information if certain statutory criteria are met. The Senate bill does not require prior approval by the FISC of applicable certifications, targeting procedures and minimization procedures in connection with the acquisition of communications of non-U.S. persons abroad, nor does it require adoption and submission of compliance guidelines. Rather, it requires submission of a certification or a targeting or minimization procedure, or an amendment thereto, to the Foreign Intelligence Surveillance Court (FISC) within five days of making or amending the certification or adopting or amending the procedure. Where the Attorney General and the DNI determine that immediate action is required and time does not permit preparation of a certification prior to initiation of an acquisition, the Senate bill requires the Attorney General and the DNI to prepare the certification, including such determination, within seven days after the determination is made. If the FISC finds that a certification meets statutory

requirements and targeting and minimization procedures are consistent with statutory requirements and meet constitutional standards under the Fourth Amendment, the FISC would enter an order approving continued use of the procedures involved. If the court finds that the required standards are not met, then the FISC would enter an order directing the government, at the government's election and to the extent required by the FISC order, to correct any deficiencies within 30 days or cease the acquisition.

In the absence of an emergency authorization, the House amendment to the Senate amendment to H.R. 3773 requires prior approval by the FISC of the applicable targeting procedures, minimization procedures, and certification before the Attorney General and the Director of National Intelligence (DNI) may authorize acquisition of the contents of communications of non-U.S. persons reasonably believed to be located outside the United States. The FISC would have 30 days after a certification is submitted to review the certification and the targeting and minimization procedures and to approve or deny an order regarding such an acquisition.

The House amendment also requires the Attorney General, in consultation with the DNI, to adopt guidelines to ensure compliance with limitations imposed by the bill on such acquisitions and to ensure that an application is filed under section 104 or 303 of FISA, if required by that act. The guidelines are to be submitted to the FISC, the congressional intelligence committees, and the House and Senate Judiciary Committees.

H.R. 6304 would amend FISA to permit the Attorney General and the DNI to jointly authorize targeting of persons reasonably believed to be non-U.S. persons located outside the United States for periods of up to one year. Proposed section 702 of FISA contains explicit limitations, including protections against reverse targeting in connection with the acquisition of the communications of such persons. A certification by the Attorney General and the DNI that certain statutory criteria have been met, applicable targeting procedures, and minimization procedures would be subject to judicial review by the FISC. The certification would attest, in part, that procedures are in place that have been approved, have been submitted for approval, or will be submitted with the certification for approval by the FISC that are reasonably designed to ensure that an acquisition is limited to targeting persons reasonably believed to be located outside the United States, and to prevent the intentional acquisition of any communication where the sender and all intended recipients are known at the time of the acquisition to be located in the United States. Generally, if the certification and targeting and minimization procedures meet the statutory requirements and are consistent with the Fourth Amendment, a FISC order approving them would be issued prior to implementation of the acquisition of the communications at issue. If the FISC finds deficiencies in the certification, targeting procedures, or minimization procedures, the court would issue an order directing the government to, at the government's election and to the extent required by the court's order, correct any such deficiency within 30 days or cease,

or not begin, the implementation of the authorization for which the certification was submitted.

Legislative Response: Foreign Intelligence Surveillance of U.S. Persons Outside the United States

Generally, the full extent of Fourth Amendment protections attach to the privacy interests of U.S. persons within the United States. Fourth Amendment protections also attach to U.S. citizens abroad. However, the operation of its protections outside the United States may differ from that in the United States due to the fact that a citizen abroad may not have the same expectation of privacy. In addition, the Warrant Clause of the Fourth Amendment may not apply outside the United States where U.S. magistrates have no jurisdiction. A determination whether interception of a communication abroad is lawful turns upon the law of the country where the interception occurs, so, depending upon location, the rights available may differ significantly. In addition, the availability of Fourth Amendment protections are affected by whom the search was executed, and the extent of any U.S. role. If the U.S. plays no role, then the Fourth Amendment does not attach, and the exclusionary rule does not apply to evidence obtained by or derived from such a search unless the foreign conduct "shocks the conscience." On the other hand, if warrantless electronic surveillance targeted at a U.S. citizen's communications is conducted abroad for the purpose of gathering foreign intelligence by U.S. officials, the U.S. district court in *United States v. Bin Laden*, 126 F. Supp. 2d 264, 277 (S.D.N.Y. 2000), has held that it will be deemed reasonable if it is authorized by the President, or the Attorney General pursuant to the President's delegation, and the surveillance was conducted "primarily for foreign intelligence purposes and . . . targets foreign powers or their agents."

In addition to considering the scope of constitutional privacy protections available to U.S. citizens or U.S. persons abroad, the 110th Congress, in FISA legislation before it, is also considering what it deems the appropriate level of privacy protection to be afforded such persons while outside the United States. In addition to the Protect America Act of 2007, P.L. 110-55 (August 5, 2007), the Senate-passed amendment to H.R. 3773, the House-passed amendment to the Senate amendment to H.R. 3773, and H.R. 6304 each addresses procedures for targeting U.S. persons reasonably believed to be located outside the United States to collect foreign intelligence information.

The Senate amendment to H.R. 3773, the House amendment to the Senate amendment to H.R. 3773, and H.R. 6304 each provide for targeting of U.S. persons reasonably believed to be located outside the United States for up to 90 days pursuant to a FISC order if statutory criteria are met. Such an order could be renewed for additional 90-day periods upon submission of renewal applications meeting the same standards. In the case of an emergency authorization by the Attorney General of an acquisition, each bill requires notice to a FISC judge by the Attorney General or his designee at the time the decision is made to conduct such an acquisition and requires the filing of an application for a FISC order

within seven days of the Attorney General's authorization of the emergency acquisition. Minimization procedures would apply to such an acquisition.

Under each of these bills, in the absence of a judicial order approving an acquisition originally authorized by the Attorney General on an emergency basis, the acquisition would terminate when the information sought is obtained, when an application for the order is denied, or when seven days have elapsed, whichever is earliest. Without a FISC order, no information acquired or evidence derived from an emergency acquisition, except under circumstances where the target of the acquisition is determined not to be a U.S. person, may be received in evidence or disclosed in federal, state, or local proceedings; nor could any information concerning a U.S. person acquired from such acquisition subsequently be used or disclosed in any other manner by federal officers or employees without the consent of such person, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person.

Limitations on Liability for Telecommunications Providers Furnishing Aid to the Government

The second of the two critical needs identified by the DNI in his August 2nd statement was a need for liability protection for those who furnish aid to the Government in carrying out its foreign intelligence collection efforts. He sought both retrospective relief from liability for those who are alleged to have aided the Government from September 11, 2001 to the present in connection with electronic surveillance or collection of other communications related information, and prospective liability protection for those telecommunications providers who furnish aid to the government in the future whether pursuant to a court order or a certification by the Attorney General or the Attorney General and the DNI that the acquisition or electronic surveillance involved is lawful and that all statutory requirements have been met.

Under current law, there are a number of statutory sections which provide some limitation on liability for telecommunication providers who furnish aid to the government in connection with electronic surveillance or a physical search, or the installation of a pen register or trap and trace device pursuant to a court order under FISA. In addition, 18 U.S.C. § 2511(2)(a) bars suit in any court against any provider of wire or electronic communication service, its officers, employees, or agents, landlord, custodian, or other specified person for providing information, facilities, or assistance in accordance with the terms of a court order, statutory authorization, or a certification in writing by the Attorney General or a person specified under 18 U.S.C. § 2518(7) that no warrant or court order is required by law, that all statutory requirements have been met, and that the specified assistance is required.

Prospective relief from liability for those furnishing aid to the government pursuant to a court order or certification or a directive pursuant to statute

requiring compliance with government demands for assistance is contemplated in a number of bills, including H.R. 3773 as originally passed, the Senate Amendment to H.R. 3773, the House amendment to the Senate amendment to H.R. 3773, and H.R. 6304. All three versions of H.R. 3773, and H.R. 6304 authorize the FISC to compel compliance through the contempt power, as did P.L. 110-55 while it was in force.

Retroactive immunity presents more difficult issues. There are currently pending a substantial number of law suits against the telecommunications providers who are alleged to have furnished aid to the government in connection with its warrantless surveillance programs since September 11, 2001, and other programs. Approximately 40 of these suits are currently pending in the Northern District of California under an order of the Judicial Panel on Multidistrict Litigation. On August 9, 2006, pursuant to 28 U.S.C. § 1407, the Judicial Panel on Multidistrict Litigation transferred 17 civil actions that were pending throughout the country to the Northern District of California, and assigned them to Judge Vaughn Walker for coordinated or consolidated pretrial proceedings in *In Re: National Security Agency Telecommunications Records Litigation*, MDL-1791. Another 26 cases were treated as potential tag-along actions under the multidistrict litigation rules. The panel of five federal trial and appellate court judges found that all these class actions share "factual and legal questions regarding alleged Government surveillance of telecommunications activity and the participation in (or cooperation with) that surveillance by individual telecommunications companies," and thus centralization of the cases "is necessary in order to eliminate duplicative discovery, prevent inconsistent pretrial rulings (particularly with respect to matters involving national security), and conserve the resources of the parties, their counsel and the judiciary."

Arguments may be made on both sides with respect to whether retroactive immunity should be granted telecommunications providers who are alleged to have assisted the government in such programs. For example, the cooperation of such providers is critical to the government's capacity to pursue electronic surveillance to gather foreign intelligence information, and is also essential for collection of communications records for pattern analysis. If the telecommunication providers who responded to the government's requests or demands for assistance did so in good faith reliance upon assertions by the government that the demand was lawful and that a court order was not required, it may be argued that the providers should be immunized from ill effects flowing from such good faith reliance. Some have argued that the unique factual context militates in favor of such relief from liability, to the extent those who responded to the government's requests for assistance in the wake of 9/11 did so in response to government assertions that their cooperation was necessary to protect against further attacks.

In many of the suits filed, the government has asserted states secrets privilege with respect to the programs involved and the role of any of the telecommunications carriers with respect thereto. This is a common law

evidentiary privilege, which may only be asserted by the government, that protects information from discovery when its disclosure would be inimical to the national security. The privilege can come into play in three ways. If the very subject matter of the case is a state secret, an assertion of the privilege can cause the case to be immediately dismissed and the action barred. If, however, this prong of the state secrets privilege does not apply, the privilege may operate to bar admission into evidence of information which will damage the security of the United States. The plaintiff then goes forward on the basis of evidence not covered. If the plaintiff cannot prove a prima facie case with nonprivileged evidence, then the case may be dismissed. On the other hand, if the privilege deprives a defendant of information that would otherwise give the defendant a valid defense to the claim, then the court may grant summary judgment to the defendant. In the current context, to the extent that a defendant telecommunications providers may have a valid claim of immunity under 18 U.S.C. § 2511(2)(a), but for the application of the state secrets privilege to the identities of any providers who may have furnished aid to the government, an argument may be made that the telecommunications providers so impacted should be afforded immunity from suit.

On the other hand, such suits may be the only means by which those who may have been adversely impacted by such government activities may obtain any remedy for any injuries incurred. These injuries may have impacted First and Fourth Amendment protected interests, and there may be no other means of vindicating those rights. In addition, the telecommunications providers provide the front line of defense of those rights against governmental abuse if the government demand or request is unlawful. In some instances, it may be argued that a telecommunications provider has a statutory obligation to protect customer records from unlawful access. Such arguments militate against affording relief from liability to any providers who may have permitted unlawful access.

In addition to these arguments, some have argued that, because the Administration has not shared information repeatedly sought by some committees of jurisdiction with respect to the role of the telecommunications providers in the TSP or other pertinent intelligence activities, the Congress does not have adequate information to determine whether relief for the telecommunications carriers is warranted.

Legislative Response

Under proposed section 802(a) of FISA in Title II of H.R. 6304, a civil action may not lie or be maintained in a federal or state court against any person for providing assistance to an element of the intelligence community, and must be dismissed promptly, if the Attorney General certifies to the U.S. district court in which the action is pending that:

(1) any assistance by that person was provided pursuant to an order of the court established under section 103(a) directing such assistance;
(2) any assistance by that person was provided pursuant to a certification in writing under section 2511(2)(a)(ii)(B) or 2709(b) of title 18, United States Code;
(3) any assistance by that person was provided pursuant to a directive under section 102(a)(4), 105B(e), as added by section 2 of the Protect America Act of 2007 (Public Law 110-55), or 702(h) directing such assistance;
(4) in the case of a covered civil action, the assistance alleged to have been provided by the electronic communication service provider was —
    (A) in connection with an intelligence activity involving communications that was —
        (i) authorized by the President during the period beginning on September 11, 2001, and ending on January 17, 2007; and
        (ii) designed to detect or prevent a terrorist attack, or activities in preparation for a terrorist attack, against the United States; and
    (B) the subject of a written request or directive, or a series of written requests or directives, from the Attorney General or the head of an element of the intelligence community (or the deputy of such person) to the electronic communication service provider indicating that the activity was —
        (i) authorized by the President; and
        (ii) determined to be lawful; or
(5) the person did not provide the alleged assistance.

Under proposed subsection 802(b) of FISA, such a certification shall be given effect unless the court finds that it is not supported by substantial evidence provided to the court under that section. In the course of its judicial review, the U.S. district court may examine the court order, certification, written request, or directive described in proposed subsection 802(a) and any relevant court order, certification, written request, or directive submitted to the court by the parties under proposed subsection 802(d). Any such party would be permitted to participate in briefing or argument of any legal issue in a judicial proceeding under this section to the extent that such participation does not require disclosure of classified information to that party. Any relevant classified information would be reviewed in camera and ex parte. Any portion of the court's written order that would reveal classified information would be issued in camera and ex parte and maintain it under seal. Upon filing of a declaration by the Attorney General under 28 U.S.C. § 1746 that disclosure of such a certification or of the supplemental materials provided pursuant to proposed subsections 802 (b) or (d) would harm the national security of the United States, the U.S. district court would be required to review such certification and the supplemental materials in camera and ex parte. Any public disclosure of such certification and supplemental materials would be limited to a statement as to whether the case is dismissed and a description of the legal standards that govern the order, without

disclosing the paragraph of subsection (a) that is the basis for the certification. If H.R. 6304 were to be enacted into law, proposed Section 802 of FISA would apply to a civil action pending on or filed after the date of the enactment.

The Senate amendment to H.R. 3773 bars covered civil actions in a federal or state court and requires that such an action must be dismissed promptly if the Attorney General or above certifies to the court that the assistance alleged to have been provided by the electronic communication service provider was in connection with an intelligence activity involving communications that was authorized by the President during the period beginning on September 11, 2001, and ending on January 17, 2007; and designed to detect or prevent a terrorist attack, or activities in preparation for a terrorist attack, against the United States; and described in a written request or directive from the Attorney General or the head of an element of the intelligence community (or the deputy of such person) to the electronic communication service provider indicating that the activity was authorized by the President and determined to be lawful. A covered civil action in federal or state court would also be barred and should be dismissed promptly if the Attorney General certifies to the court that the electronic communication service provider did not provide the alleged assistance. The Attorney General's certification would be subject to judicial review under an abuse of discretion standard. If the Attorney General files a declaration under 28 U.S.C. § 1746 that disclosure of a certification made under subsection 202(a) of the bill would harm United States national security, the court shall review the certification in camera and ex parte, and limit public disclosure concerning such certification, including any public order following such ex parte review, to a statement that the conditions of subsection 202(a) of the bill have been met, without disclosing the subparagraph of subsection 202(a)(1) that is the basis for the certification. The authorities of the Attorney General under section 202 are to be performed by the Attorney General, or the Acting Attorney General, or a designee in a position not lower than the Deputy Attorney General.

The House-passed amendment to the Senate Amendment took a different approach. Proposed section 802, in part, provides authority for the government to intervene in any covered civil action. Any party may submit to the court evidence, briefs, arguments, or other information on any matter with respect to which a state secrets privilege has been asserted. The section also authorizes the court to review any such submissions in accordance with procedures set forth in section 106(f) of FISA; and permits the court, on motion of the Attorney General, to take additional steps to protect classified information. The court, to the extent practicable and consistent with national security would be permitted to request any party to present briefs and arguments on any legal question the court finds raised by such submission, regardless of whether that party has access to the submission. Under new subsection 802(e) of FISA, for any covered civil action alleging that a person provided assistance to an element of the intelligence community pursuant to a request or directive during the period from September 11, 2001 through January 17, 2007, the Attorney General would be required to

provide to the court any request or directive related to the allegations under the procedures set forth in new subsection 802(b).

H.R. 6304, therefore, differs from prior House and Senate amendments to H.R. 3773 in a number of respects, while having similarities to them in others. Both H.R. 6304 and the Senate amendment would bar civil actions in federal or state court against persons providing assistance to an element of the intelligence community if the Attorney General certifies that certain statutory criteria are met. They differ to some degree as to the criteria involved.

H.R. 6304 provides for judicial review of the Attorney General's certification under a substantial evidence standard, while the Senate amendment to H.R. 3773 provides for review of the Attorney General's certification using an abuse of discretion standard. The House amendment to the Senate amendment to H.R. 3773 provides for judicial review of any submissions by any party relating any matter as to which state secrets privilege has been asserted, but does not specify the standard of review.

H.R. 6304 expressly permits the district court, in its review, to examine any court order, certification, written request, or directive described in proposed subsection 802(a) or submitted to the court by the parties, and, permits party participation in briefs and arguments on any legal issue in the judicial proceeding to the extent that such participation does not require disclosure of classified information to that party. This does not have a parallel in the Senate amendment. However, it has some points of similarity with the House amendment, which permits submissions by the parties of evidence, briefs, arguments, or other information relating to any matter with respect to which state secrets privilege has been asserted, while providing protections for classified information. For any covered civil action alleging that a person provided assistance to an element of the intelligence community pursuant to a request or directive during the September 11, 2001 to January 17, 2007 period, the House amendment requires the Attorney General to provide the court with any request or directive related to the allegations.

All three bills make provision for ex parte, in camera review of classified information. H.R. 6304 and the Senate amendment both place restrictions on public disclosure of information regarding the certification and the court's order.

The Foreign Intelligence Surveillance Act: An Overview of Selected Issues, RL34279 (July 7, 2008)

ELIZABETH B. BAZAN, CONGRESSIONAL RESEARCH SERV., THE FOREIGN INTELLIGENCE SURVEILLANCE ACT: AN OVERVIEW OF SELECTED ISSUES (2008), *available at* http://www.intelligencelaw.com/library/secondary/crs/pdf/RL34279_7-7-2008.pdf.

Order Code RL34279
Updated July 7, 2008

Elizabeth B. Bazan
Legislative Attorney
American Law Division

Summary

The current legislative and oversight activity with respect to electronic surveillance under the Foreign Intelligence Surveillance Act (FISA) has drawn national attention to several overarching issues. This report briefly outlines three such issues and touches upon some of the perspectives reflected in the ongoing debate. These issues include the inherent and often dynamic tension between national security and civil liberties, particularly rights of privacy and free speech; the need for the intelligence community to be able to efficiently and effectively collect foreign intelligence information from the communications of foreign persons located outside the United States in a changing, fast-paced, and technologically sophisticated international environment or from United States persons abroad, and the differing approaches suggested to meet this need; and limitations of liability for those electronic communication service providers who furnish aid to the federal government in its foreign intelligence collection. Two constitutional provisions, in particular, are implicated in this debate — the Fourth and First Amendments. This report briefly examines these issues and sets them in context.

The 110th Congress has been very active in developing and considering measures to amend FISA to address these issues. On August 5, 2007, the Protect America Act, P.L. 110-55, was enacted into law. It expired on February 16, 2008, after passage of a 15-day extension to its original sunset date, P.L. 110-182. On November 15, 2007, the House of Representatives passed H.R. 3773, the RESTORE Act of 2007. On February 12, 2008, the Senate passed S. 2248, as amended, then struck all but the enacting clause of H.R. 3773, and inserted the text of S. 2248, as amended, in its stead. On March 14, 2008, the House passed an amendment to theSenate amendment to H.R. 3773. After months of intensive negotiations, on June 19, 2008, a compromise bill, H.R. 6304, was introduced in the House. It was passed by the House the following day. On June 26, 2008, a cloture motion on the measure was presented in the Senate. Further activity on

H.R. 6304 is anticipated after the Senate returns from the July 4th recess. Each of these bills differs somewhat in content and approach from one another. This report also briefly explores legislative responses to the issues addressed. It will be updated as needed.

Introduction

The Foreign Intelligence Surveillance Act of 1978, P.L. 95-511, 92 Stat. 1783 (October 25, 1978), 50 U.S.C. §§ 1801 *et seq*. (hereinafter FISA), was enacted in response both to the Committee to Study Government Operations with Respect to Intelligence Activities (otherwise known as the Church Committee) revelations regarding past abuses of electronic surveillance for national security purposes and to the somewhat uncertain state of the law on the subject.[4084] While FISA now provides

---

[4084] The U.S. Supreme Court originally held that the Fourth Amendment only applied to tangible things, Olmstead v. United States, 277 U.S. 438 (1928). but later held that intangible things, such as conversations, were also protected. In its 1967 decision in Katz v. United States, 389 U.S. 347, 353, 359 n. 23 (1967), the Court, overturning its previous holding in Olmstead v. United States, held that the Fourth Amendment covered electronic surveillance of oral communications without physical intrusion. The *Katz* Court stated, however, that its holding did not extend to cases involving national security. In United States v. United States District Court, 407 U.S. 297, 313-14 (1972) (the Keith case), the Court regarded Katz as "implicitly recogniz[ing] that the broad and unsuspected governmental incursions into conversational privacy which electronic surveillance entails necessitate the application of Fourth Amendment safeguards." Mr. Justice Powell, writing for the *Keith* Court, framed the matter before the Court as follows:

The issue before us is an important one for the people of our country and their Government. It involves the delicate question of the President's power, acting through the Attorney General, to authorize electronic surveillance in internal security matters without prior judicial approval. Successive Presidents for more than one-quarter of a century have authorized such surveillance in varying degrees, without guidance from the Congress or a definitive decision of this Court. This case brings the issue here for the first time. Its resolution is a matter of national concern, requiring sensitivity both to the Government's right to protect itself from unlawful subversion and attack and to the citizen's right to be secure in his privacy against unreasonable Government intrusion.

407 U.S. at 299. The Court held that, in the case of intelligence gathering involving domestic security surveillance, prior judicial approval was required to satisfy the Fourth Amendment. Justice Powell emphasized that the case before it "require[d] no judgment on the scope of the President's surveillance power with respect to the activities of foreign powers, within or without the country." *Id*., at 308 The Court expressed no opinion as to "the issues which may be involved with respect to activities of foreign powers or their agents." *Id*., at 321-22. However, the guidance which the Court provided in Keith with respect to national security surveillance in a domestic context to some degree presaged the approach Congress was to take in foreign intelligence surveillance. *Id*. at 323-24.

Court of appeals decisions following *Keith* met more squarely the issue of warrantless electronic surveillance in the context of foreign intelligence gathering. In United States v. Brown, 484 F.2d

a statutory framework for gathering foreign intelligence information through the use of electronic surveillance, physical searches, and pen registers or trap and trace devices, and access to business records and other tangible things, the 1978 Act dealt only with electronic surveillance. The provisions passed almost 30 years ago became Title I of FISA. As originally enacted, the measure provided a statutory framework for collection of foreign intelligence information through the use of electronic surveillance of communications of foreign powers or agents of foreign powers, as those terms were defined in the act. The act has been amended repeatedly in the intervening years in an effort to address changing circumstances. Then, as now, the Congress sought to strike a balance between national security interests and civil liberties.

A number of FISA bills have received recent attention in the 110th Congress. On August, 5, 2007, the Protect America Act, P.L. 110-55 was enacted into law. This measure, in part, construed the term "electronic surveillance" under FISA not to include surveillance directed at a person reasonably believed to be located outside of the United States, and provided authority for warrantless acquisition of foreign intelligence information concerning persons reasonably believed to be located outside the United States where certain criteria were satisfied. As originally enacted, the measure was to sunset on February 1, 2008.[4085] On January 29, 2008, both the House and the Senate passed H.R. 5104, a 15-day extension to the sunset for the Protect America Act, to allow further time to consider, pass, and go to conference on proposed legislation to amend FISA, while ensuring that the intelligence community would have the authority it needed in the intervening period. It was enacted into law as P.L. 110-182.

---

418 (5th Cir. 1973), *cert. denied*, 415 U.S. 960 (1974), the Fifth Circuit upheld the legality of a warrantless wiretap authorized by the Attorney General for foreign intelligence purposes where the conversation of Brown, an American citizen, was incidentally overheard. The Third Circuit in United States v. Butenko, 494 F.2d 593 (3rd Cir. 1974), *cert. denied sub nom*, Ivanov v. United States, 419 U.S. 881 (1974), concluded that warrantless electronic surveillance was lawful, violating neither Section 605 of the Communications Act nor the Fourth Amendment, if its primary purpose was to gather foreign intelligence information. In its plurality decision in Zweibon v. Mitchell, 516 F.2d 594, 613-14 (D.C. Cir. 1975), *cert. denied*, 425 U.S. 944 (1976), the District of Columbia Circuit took a somewhat different view in a case involving a warrantless wiretap of a domestic organization that was not an agent of a foreign power or working in collaboration with a foreign power. Finding that a warrant was required in such circumstances, the plurality also noted that "an analysis of the policies implicated by foreign security surveillance indicates that, absent exigent circumstances, all warrantless electronic surveillance is unreasonable and therefore unconstitutional." For more information on the background of FISA, see CRS Report RL30465, *The Foreign Intelligence Surveillance Act: An Overview of the Statutory Framework and U.S. Foreign Intelligence Surveillance Court and U.S. Foreign Intelligence Surveillance Court of Review Decisions*, by Elizabeth B. Bazan (February 15, 2007).

[4085] For more information on the Protect America Act of 2007, see CRS Report RL34143, *P.L. 110-55, the Protect America Act of 2007: Modifications to the Foreign Intelligence Surveillance Act*, by Elizabeth B. Bazan.

The House of Representatives passed H.R. 3773, the Responsible Electronic Surveillance That is Overseen, Reviewed, and Effective Act of 2007, or the RESTORE Act of 2007, on November 15, 2007,[4086] while S. 2248 was reported out of the Senate Select Committee on Intelligence on October 26, 2007, and an amendment in the nature of a substitute to S. 2248, the Foreign Intelligence Surveillance Amendments Act of 2007, or the FISA Amendments Act of 2007, was reported out of the Senate Judiciary Committee on November 16, 2007. A modified version of the Senate Judiciary Committee's amendment in the nature of a substitute to S. 2248 was tabled.

The Senate passed S. 2248, the FISA Amendments Act of 2008, as amended, on February 12, 2008.[4087] After striking all but the enacting clause of H.R. 3773 and inserting the text of S. 2248 as amended, the Senate then passed H.R. 3773, the FISA Amendments Act of 2008.

On March 14, 2008, the House passed an amendment to the Senate amendment to H.R. 3773.[4088] After intensive negotiations, a compromise bill, H.R. 6304, was introduced in the House on June 19, 2008. The measure passed the House the following day.[4089] A cloture motion on the measure was presented in the Senate on June 26, 2008. Further activity on H.R. 6304 is anticipated after the Senate returns from the July 4th recess.

The current legislative and oversight activity with respect to electronic surveillance under FISA has drawn national attention to several overarching issues. This report briefly outlines three such issues and touches upon some of the perspectives reflected in the ongoing debate. These issues include the inherent and often dynamic tension between national security and civil liberties, particularly rights of privacy and free speech; the need identified by the Director of National Intelligence (DNI), Admiral Mike McConnell, for the intelligence community to be able to efficiently and effectively collect foreign intelligence information from the communications of foreign persons located outside the United States in a changing, fast-paced, and technologically sophisticated international environment,[4090] and the differing approaches suggested to meet

---

[4086] Roll no. 1120, 227 - 189.

[4087] Record Vote No. 20, 68 - 29.

[4088] Roll no. 145, 213 - 197, 1 Member voting Present. Passage of S. 2248 was then vitiated and the bill was returned to the Senate calendar.

[4089] Roll no. 437, 293 - 129.

[4090] *See* Statement of the Director of National Intelligence, Subject: Modernization of the Foreign Intelligence Surveillance Act (FISA) (August 2, 2007), stating in pertinent part:

this need; and limitations of liability for those electronic communication service providers who furnish aid to the federal government in its foreign intelligence collection. This report briefly examine these issues and sets them in context.

Tension Between National Security and Civil Liberties

Two constitutional provisions, in particular, are implicated in this debate — the Fourth and First Amendments. The Fourth Amendment to the U.S. Constitution provides:

> *The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrant shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.*

The First Amendment to the U.S. Constitution provides:

> *Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.*

As the Fourth Amendment protects the people's privacy rights, so the First Amendment reflects a recognition of the value of free expression of ideas and lawful political dissent to the preservation of a free society.

In introducing S. 1566, the bill that became the Foreign Intelligence Surveillance Act of 1978, P.L. 95-511, Senator Edward Kennedy addressed the challenge of

---

First, the Intelligence Community should not be required to obtain court orders to effectively collect foreign intelligence from foreign targets located overseas. Simply due to technology changes since 1978, court approval should not now be required for gathering intelligence from foreigners located overseas. This was not deemed appropriate in 1978 and it is not appropriate today. . . .

The Intelligence Community should not be restricted to effective collection of only certain categories of foreign intelligence when the targets are located overseas. We must ensure that the Intelligence Community can be effective against all who seek to do us harm. The bill must not require court approval before urgently needed intelligence collection can begin against a foreign target located overseas. The delays of a court process that requires judicial determinations in advance to gather vital intelligence from foreign targets overseas can in some cases prevent the rapid gathering of intelligence necessary to provide warning of threats to the country. This process would also require in practice that we continue to divert scarce intelligence experts to compiling these court submissions. Similarly, critical intelligence gathering on foreign targets should not be halted while court review is pending. . . . .

This statement may be found at [http://www.odni.gov/press_releases/20070802_release.pdf].

striking an appropriate balance between the legitimate government need to safeguard the nation against the intelligence activities of foreign agents and the concomitant need to protect civil liberties, stating:

> *The complexity of the problem must not be underestimated. Electronic surveillance can be a useful tool for the Government's gathering of certain kinds of information; yet, if abused, it can also constitute a particularly indiscriminate and penetrating invasion of the privacy of our citizens. My objective over the past six years has been to reach some kind of fair balance that will protect the security of the United States without infringing on our citizens' human liberties and rights.*[4091]

This sentiment was echoed in a hearing before the Senate Judiciary Committee on S. 1566 when Attorney General Griffin Bell testified for the Carter Administration in favor of the measure:

> *I believe this bill is remarkable not only in the way it has been developed, but also in the fact that for the first time in our society the clandestine intelligence activities of our government shall be subject to the regulation and receive the positive authority of a public law for all to inspect. President Carter stated it very well in announcing this bill when he said that "one of the most difficult tasks in a free society like our own is the correlation between adequate intelligence to guarantee our nation's security on the one hand, and the preservation of basic human rights on the other." It is a very delicate balance to strike, but one which is necessary in our society, and a balance which cannot be achieved by sacrificing either our nation's security or our civil liberties. . . .*[4092]

In providing background for its report on H.R. 7308, the House FISA bill then under consideration, the House Permanent Select Committee on Intelligence noted:

> *The history and law relating to electronic surveillance for "national security" purposes have revolved around the competing*

[4091] Report of the Senate Committee on the Judiciary to accompany S. 1566, S.Rept. 95-604, Part I, 95th Cong., 1st Sess. 8 (1977); 1978 U.S.C.C.A.N. 3904, 3910. FISA was enacted in the wake of revelations of abuses of warrantless surveillance in the name of national security revealed in the 1973 investigation of the Watergate break-ins and later explored in greater detail by Church Committee. *Id.* at 7, 1978 U.S.C.C.A.N. at 3908. See also, Foreign Intelligence Surveillance Act of 1978, H.Rept. 95-1283, Part I, 95th Cong., 2d Sess. 14 (1978).

[4092] Hearing before the Subcommittee on Criminal Laws and Procedures of the Senate Committee on the Judiciary, Foreign Intelligence Surveillance Act of 1977, 95th Cong., 1st Sess. 23 (1977).

demands of the President's constitutional powers to gather intelligence deemed necessary to the security of the nation and the requirements of the fourth amendment. The U.S. Supreme Court has never expressly decided the issue of whether the President has the constitutional authority to authorize warrantless electronic surveillance for foreign intelligence purposes. Whether or not the President has an "inherent power" to engage in or authorize warrantless electronic surveillance and, if such power exists, what limitations, if any, restrict the scope of that power, are issues that have troubled constitutional scholars for decades.[4093]

Electronic surveillance can provide vital information needed to identify those who are acting or preparing to act against U.S. interests for the benefit of foreign powers, including those engaged in espionage, sabotage, or terrorist acts or who otherwise pose a threat to the nation or its citizens, and to uncover their plans or activities. This information may not be readily uncovered by other investigative means. Thus, surveillance can provide a valuable tool for protecting the security of the nation and its citizens. However, this investigative technique, by its nature, can intrude into the privacy of both the target of the surveillance and those with whom the target communicates. It also has the potential of chilling political discussion and lawful dissent.[4094]

[4093] Report of the House Permanent Select Committee on Intelligence to accompany H.R. 7308, the Foreign Intelligence Surveillance Act of 1978, H.Rept. 95-1283, Part I, 95th Cong., 2d Sess. 15 (1978).

[4094] *See*, S.Rept. 95-604, at 8, 1978 U.S.C.C.A.N. 3909-3910. The Senate Judiciary Committee noted that "[i]n summarizing its conclusion that surveillance was "often conducted by illegal or improper means," the Church committee wrote:

Since the 1930's, intelligence agencies have frequently wiretapped and bugged American citizens without the benefit of judicial warrant. . . . [P]ast subjects of these surveillances have included a United States Congressman, Congressional staff member, journalists and newsmen, and numerous individuals and groups who engaged in no criminal activity and who posed no genuine threat to the national security, such as two White House domestic affairs advisers and an anti-Vietnam War protest group. (vol 2, p. 12)

* * * *

The application of vague and elastic standards for wiretapping and bugging has resulted in electronic surveillances which, by any objective measure, were improper and seriously infringed the Fourth Amendment Rights of both the targets and those with whom the targets communicated. The inherently intrusive nature of electronic surveillance, moreover, has enabled the Government to generate vast amounts of information — unrelated to any legitimate government interest — about the personal and political lives of American citizens. The collection of this type of information has, in turn, raised the danger of its use for partisan political and other improper ends by senior administration officials. (vol. 3, p. 32)

The Senate Judiciary Committee observed further:

The framing of the current debate on this issue flows, in part, from questions arising with respect to the Terrorist Surveillance Program (TSP), first revealed in press accounts in December 2005.[4095] While little information regarding the details of this NSA program is publicly available, the President has indicated that, "since shortly after September 11, 2001, he had authorized the National Security Agency (NSA) to intercept international communications into and out of the United States of persons linked to al Queda or related terrorist organizations. The purpose of the intercepts is to establish an early warning system to detect and prevent another catastrophic terrorist attack on the United States."[4096] Concerns surrounding the TSP have led to continuing congressional oversight and a number of legislative proposals focused upon providing the intelligence community with the tools it needs for foreign intelligence collection to protect the United States and its citizens, while also protecting the civil liberties of those impacted by such collection.

Also formidable — although incalculable — is the "chilling effect" which warrantless electronic surveillance may have on the constitutional rights of those who were not targets of the surveillance, but who perceived themselves, whether reasonably or unreasonably, as potential targets. Our Bill of Rights is concerned not only with direct infringements on constitutional rights, but also with government activities which effectively inhibit the exercise of these rights. The exercise of political freedom depends in large measure on citizens' understanding that they will be able to be publicly active and dissent from official policy, within lawful limits, without having to sacrifice the expectation of privacy that they rightfully hold. Arbitrary or uncontrolled use of warrantless electronic surveillance can violate that understanding and impair that public confidence so necessary to an uninhibited political life.

See also, *Keith*, 407 U.S. at 391-321, where Justice Powell observed that,

National security cases . . . often reflect a convergence of First and Fourth Amendment values not present in cases of "ordinary" crime. Though the investigative duty of the executive may be stronger in such cases, so also is there greater jeopardy to constitutionally protected speech. "Historically the struggle for freedom of speech and press in England was bound up with the issue of the scope of the search and seizure power," *Marcus v. Search Warrant*, 367 U.S. 717, 724 (1961). . . . Fourth Amendment protections become the more necessary when the targets of official surveillance may be those suspected of unorthodoxy in their political beliefs. The danger to political dissent is acute where the Government attempts to act under so vague a concept as the power to protect "domestic security." . . . .

[4095] See, e.g., James Risen and Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, December 16, 2005, at 1, 22 (citing anonymous government officials to report that the executive order, which allows some warrantless eavesdropping on persons inside the United States, "is based on classified legal opinions that assert that the president has broad powers to order such searches, derived in part from the September 2001 Congressional resolution authorizing him to wage war on Al Qaeda and other terrorist groups").

[4096] "Legal Authorities Supporting the Activities of the National Security Agency Described by the President," U.S. Department of Justice (January 19, 2006). This may be found at [http://www.usdoj.gov/ag/readingroom/surveillance9.pdf].

The current level of complexity and sophistication of global communications technology can provide both increased opportunities for lawful private communications and public debate, and increased means for communications between those engaged in criminal wrongdoing or plans or actions which pose a threat to U.S. national security. While this presents challenges to intelligence collection for foreign intelligence purposes, the government has moved to utilize these new technologies for both law enforcement and intelligence purposes. The balance between these important governmental needs and protections of constitutionally protected privacy interests and First Amendment protected activities is dynamic, and there can be differences of opinion as to where the appropriate balance point between them may be found.

Collection of Foreign Intelligence Information from Foreign Persons and United States Persons Located Abroad

A second, related issue in the current debate concerns the appropriate circumstances or standards for collection of foreign intelligence information from foreign persons and United States persons abroad. This issue can best be understood when set in the context of recent developments, to the extent that pertinent information is publicly available.

In July 2007, an unclassified summary of the National Intelligence Estimate (NIE) on "The Terrorist Threat to the US Homeland" was released. The NIE expressed the judgement, in part, that the U.S. Homeland will face a persistent and evolving threat over the next three years, the main threat coming from Islamic terrorist groups and cells, particularly al Qaeda.[4097]

In a January 17, 2007, letter to Chairman Leahy and Ranking Member Specter of the Senate Judiciary Committee, then Attorney General Gonzales advised them that, on January 10, 2007, a Foreign Intelligence Surveillance Court judge "issued orders authorizing the Government to target for collection international communications into or out of the United States where there is probable cause to believe that one of the communicants is a member or agent of al Qaeda or an associated terrorist organization." The Attorney General stated that, in light of these orders, which "will allow the necessary speed and agility," all surveillance previously occurring under the Terrorist Surveillance Program (TSP) would now be conducted subject to the approval of the FISC. He indicated further that, under these circumstances, the President had determined not to reauthorize the TSP when the then current authorization expired. The Attorney General also noted that the Intelligence Committees had been briefed on the highly classified details of the FISC orders and advised Chairman Leahy and Senator Specter that he had directed the Acting Assistant Attorney General for the Office of Legal

[4097] National Intelligence Estimate on "The Terrorist Threat to the US Homeland," at 6-7 (July 2007). This may be found at [http://www.odni.gov/press_releases/20070717_release.pdf].

Counsel and the Assistant Attorney General for National Security to provide them a classified briefing on the details of the orders. Because the contents of these orders remain classified, the scope of or limitations with respect to any authority that may have been provided remain unknown.

On April 13, 2007, the Administration announced that it had submitted draft legislation to the Congress regarding modernization of FISA. This draft legislation included a proposed new section 102A of FISA which would authorize the President, acting through the Attorney General, to permit acquisition of foreign intelligence information for up to one year concerning persons reasonably believed to be outside the United States if the Attorney General certifies in writing under oath that he has made four specific determinations.[4098]

On August 2, 2007, the DNI released a statement on "Modernization of the Foreign Intelligence Surveillance Act." In his statement, Admiral McConnell regarded such modernization as necessary to respond to technological changes and to meet the Nation's current intelligence collection needs. He viewed it as essential for the intelligence community to provide warning of threats to the United States. One of two critically needed changes perceived by the DNI was his view that a court order should not be required for gathering foreign intelligence from foreign targets located overseas. Admiral McConnell did, however, indicate that he would be willing to agree to court review, after commencement of needed collection, of the procedures by which foreign intelligence is gathered through classified methods directed at foreigners outside the United States.

Some news accounts suggest that a FISC court ruling this Spring may have limited the authority of the United States, in certain circumstances, to engage in surveillance of foreign conversations taking place outside the United States. Admiral McConnell stated in remarks included in the transcript of an interview published in the *El Paso Times* on August 22, 2007, that on or about May of this year, when another judge of the FISC considered an application for renewal or

---

[4098] These include: that "the acquisition does not constitute electronic surveillance; that the acquisition involves obtaining foreign intelligence information from or with the assistance of a communications service provider, custodian, or other person (including any officer, employee, agent, or other specified person of such service provider, custodian, or other person) who has access to communications, either as they are transmitted or while they are stored, or equipment that is being or may be used to transmit or store such communications;" that "a significant purpose of the acquisition is to obtain foreign intelligence information;" and that "the minimization procedures to be used with respect to the acquisition activity meet the definition of minimization procedures under section 101(h)" of FISA. The Fact Sheet on the draft legislation may be found at [http://www.usdoj.gov/opa/pr/2007/April/07_nsd_247.html]. The text of the draft bill may be found at [http://www.lifeandliberty.gov/docs/text-of-dni-proposed.pdf]. For further information about the proposed draft legislation regarding modernization of FISA, see the April 23, 2007, CRS Congressional Distribution Memorandum entitled, "Overview of 'FISA Modernization Provisions of the Proposed Fiscal Year 2008 Intelligence Authorization,'" by Elizabeth B. Bazan.

extension of the surveillance approved under the January 10 orders, that judge interpreted the requirements of FISA differently from the judge who had issued the January 10 orders, and deemed a FISA warrant necessary for surveillance of wire communications of a foreign person in a foreign country.[4099]

Views differ as to the scope of the need and the means by which this need may be met. Can this concern be addressed by solutions directed solely at electronic surveillance or acquisitions without a court order from the FISC of communications between foreign persons in communication with other foreign persons all located outside the United States, whether or not those communications are routed through the United States at some point in their transmission? Or must the solution be crafted in such a way as to permit such surveillance or acquisitions of the communications of foreign persons located abroad, whether they may be in communication only with other non-U.S. persons, or both non-U.S. persons and U.S. persons,[4100] located outside the United States? What is required if some of the communications of the foreign person targeted in the surveillance or acquisition are with U.S. persons or non-U.S. persons located in the United States? May such foreign intelligence be collected from U.S. persons abroad without a Foreign Intelligence Surveillance Court[4101] order pursuant to a certification by the Attorney General or the Attorney General and the DNI jointly or whether a court order is required prudentially or constitutionally under the Fourth Amendment.[4102]

Legislative Response: Foreign Intelligence Surveillance of Foreign Persons Abroad

---

[4099] The transcript of the interview with the DNI may be found at [http://www.elpasotimes.com/news/ci_6685679]. *See also*, "Greg Miller, Court Puts Limits on Surveillance Abroad: The ruling raises concerns that U.S. anti-terrorism efforts might be impaired at a time of heightened risk," *L.A. Times*, August 2, 2007, quoting a Member of Congress that "[t]here's been a ruling, over the last four or five months, that prohibits the ability of our intelligence services and our counterintelligence people from listening in to two terrorists in other parts of the world where the communication could come through the United States."

[4100] "United States person" is defined in section 101(I) of FISA to mean:
a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 1101(a)(20) of Title 8), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in subsection (a)(1), (2), or (3) of this section.

[4101] As a general matter, the proposals contemplate that any such court order would be issued by the Foreign Intelligence Surveillance Court, created under section 103(a) of FISA, 50 U.S.C. § 1803(a).

[4102] For a more in depth discussion of the application of the Fourth Amendment to U.S. citizens abroad, see CRS Congressional Distribution Memorandum entitled "U.S. Citizens' Fourth Amendment Rights Abroad and the Interception of Electronic Communications," by Jennifer K. Elsea (November 13, 2007).

On August 5, 2007, the Protect America Act of 2007 was enacted into law, P.L. 110-55, which provided that "[n]othing in the definition of electronic surveillance under section 101(f) [of FISA] shall be construed to encompass surveillance directed at a person reasonably believed to be located outside of the United States." It also created a new procedure under section 105B(a) of FISA under which the Attorney General and the DNI, for periods of up to one year, may authorize acquisition of foreign intelligence information concerning persons reasonably believed to be outside the United States, if the Attorney General and the DNI determine, based on the information provided to them, that five criteria have been met. This authority was similar, but not identical to, the proposed section 102A of FISA in the Administration's draft bill. P.L. 110-55 expired on February 16, 2008, after passage of a 15-day extension to its original sunset date.[4103] Under the transitional provisions in Section 6 of the Protect America Act, the acquisitions authorized while the act was in force may continue until their expiration.

H.R. 3773 as originally passed by the House provides that no court order is needed for electronic surveillance directed at acquisition of the contents of communications between persons not known to be U.S. persons who are reasonably believed to be located outside the United States, without regard to whether the communication is transmitted through the United States or the surveillance device is located in the United States. If the communications of a U.S. person are inadvertently intercepted, stringent constraints upon retention, disclosure, dissemination, or use would apply. However, the bill provides for a FISC order for acquisitions for up to one year of communications of non-U.S. persons reasonably believed to be outside the U.S. to collect most types of foreign intelligence information by targeting those persons, where those persons may be communicating with persons inside the United States. It also establishes requirements for such acquisitions.

The Senate amendment to H.R. 3773 would permit the Attorney General and the DNI to jointly authorize, for up to one year, targeting of persons reasonably believed to be outside the U.S. to acquire foreign intelligence information if certain statutory criteria are met. The Senate bill does not require prior approval by the FISC of applicable certifications, targeting procedures and minimization procedures in connection with the acquisition of communications of non-U.S. persons abroad, nor does it require adoption and submission of compliance guidelines. Rather, it requires submission of a certification or a targeting or minimization procedure, or an amendment thereto, to the Foreign Intelligence Surveillance Court (FISC) within five days of making or amending the certification or adopting or amending the procedure. Where the Attorney General and the DNI determine that immediate action is required and time does not permit preparation of a certification prior to initiation of an acquisition, the

[4103] P.L. 110-182.

Senate bill requires the Attorney General and the DNI to prepare the certification, including such determination, within seven days after the determination is made. If the FISC finds that a certification meets statutory requirements and targeting and minimization procedures are consistent with statutory requirements and meet constitutional standards under the Fourth Amendment, the FISC would enter an order approving continued use of the procedures involved. If the court finds that the required standards are not met, then the FISC would enter an order directing the government, at the government's election and to the extent required by the FISC order, to correct any deficiencies within 30 days or cease the acquisition.

In the absence of an emergency authorization, the House amendment to the Senate amendment to H.R. 3773 requires prior approval by the FISC of the applicable targeting procedures, minimization procedures, and certification before the Attorney General and the Director of National Intelligence (DNI) may authorize acquisition of the contents of communications of non-U.S. persons reasonably believed to be located outside the United States. The FISC would have 30 days after a certification is submitted to review the certification and the targeting and minimization procedures and to approve or deny an order regarding such an acquisition.

The House amendment also requires the Attorney General, in consultation with the DNI, to adopt guidelines to ensure compliance with limitations imposed by the bill on such acquisitions and to ensure that an application is filed under section 104 or 303 of FISA, if required by that act. The guidelines are to be submitted to the FISC, the congressional intelligence committees, and the House and Senate Judiciary Committees.

H.R. 6304 would amend FISA to permit the Attorney General and the DNI to jointly authorize targeting of persons reasonably believed to be non-U.S. persons located outside the United States for periods of up to one year. Proposed section 702 of FISA contains explicit limitations, including protections against reverse targeting[4104] in connection with the acquisition of the communications of such persons. A certification by the Attorney General and the DNI that certain statutory criteria have been met, applicable targeting procedures, and

---

[4104] Under proposed subsection 702(b) of FISA, such an acquisition is subject to several limitations, including those designed to protect against reverse targeting. Under these limitations, an acquisition may not intentionally target any person known at the time of acquisition to be located in the United States; may not intentionally target a person reasonably believed to be located outside the United States if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States; may not intentionally target a United States person reasonably believed to be located outside the United States; and may not intentionally acquire any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States. The acquisition must be conducted in a manner consistent with the Fourth Amendment to the Constitution of the United States.

minimization procedures would be subject to judicial review by the FISC. The certification would attest, in part, that procedures are in place that have been approved, have been submitted for approval, or will be submitted with the certification for approval by the FISC that are reasonably designed to ensure that an acquisition is limited to targeting persons reasonably believed to be located outside the United States, and to prevent the intentional acquisition of any communication where the sender and all intended recipients are known at the time of the acquisition to be located in the United States. Generally, if the certification and targeting and minimization procedures meet the statutory requirements and are consistent with the Fourth Amendment, a FISC order approving them would be issued prior to implementation of the acquisition of the communications at issue. If the FISC finds deficiencies in the certification, targeting procedures, or minimization procedures, the court would issue an order directing the government to, at the government's election and to the extent required by the court's order, correct any such deficiency within 30 days or cease, or not begin, the implementation of the authorization for which the certification was submitted.

Legislative Response: Foreign Intelligence Surveillance of U.S. Persons Outside the United States

Generally, the full extent of Fourth Amendment protections attach to the privacy interests of U.S. persons within the United States. Fourth Amendment protections also attach to U.S. citizens abroad.[4105] However, the operation of its protections outside the United States may differ from that in the United States due to the fact that a citizen abroad may not have the same expectation of privacy. In addition, the Warrant Clause of the Fourth Amendment may not apply outside the United States where U.S. magistrates have no jurisdiction.[4106] A determination whether interception of a communication abroad is lawful turns upon the law of the country where the interception occurs, so, depending upon

[4105] United States v. Verdugo-Urquidez, 494 U.S. 259 (1990), suggests that the Fourth Amendment may have some applicability to aliens, such as permanent resident aliens, who have accepted societal obligations and made a significant voluntary commitment to the United States.

[4106] United States v. Verdugo-Urquidez, 494 U.S. 259, 278 (Kennedy, J., concurring)("The absence of local judges or magistrates available to issue warrants, the differing and perhaps unascertainable conceptions of reasonableness and privacy that prevail abroad, and the need to cooperate with foreign officials all indicate that the Fourth Amendment's warrant requirement should not apply in Mexico as it does in this country"); *id.* at 279 (Stevens, J., concurring in the judgment)("I do agree, however, with the Government's submission that the search conducted by the United States agents with the approval and cooperation of the Mexican authorities was not 'unreasonable' as that term is used in the first Clause of the Amendment. I do not believe the Warrant Clause has any application to searches of noncitizens' homes in foreign jurisdictions because American magistrates have no power to authorize such searches").

location, the rights available may differ significantly.[4107] In addition, the availability of Fourth Amendment protections are affected by whom the search was executed, and the extent of any U.S. role.[4108] If the U.S. plays no role, then the Fourth Amendment does not attach, and the exclusionary rule does not apply to evidence obtained by or derived from such a search unless the foreign conduct "shocks the conscience."[4109] On the other hand, if warrantless electronic surveillance targeted at a U.S. citizen's communications is conducted abroad for the purpose of gathering foreign intelligence by U.S. officials, the U.S. district court in *United States v. Bin Laden*, 126 F. Supp. 2d 264, 277 (S.D.N.Y. 2000), has held that it will be deemed reasonable if it is authorized by the President, or the Attorney General pursuant to the President's delegation, and the surveillance was conducted "primarily for foreign intelligence purposes and . . . targets foreign powers or their agents."[4110]

In addition to considering the scope of constitutional privacy protections available to U.S. citizens or U.S. persons abroad, the 110th Congress, in FISA legislation before it, is also considering what it deems the appropriate level of privacy protection to be afforded such persons while outside the United States. In addition to the Protect America Act of 2007, P.L. 110-55 (August 5, 2007), the Senate-passed amendment to H.R. 3773, the House-passed amendment to the Senate amendment to H.R. 3773, and H.R. 6304 each addresses procedures for targeting U.S. persons reasonably believed to be located outside the United States to collect foreign intelligence information.

The Senate amendment to H.R. 3773, the House amendment to the Senate amendment to H.R. 3773, and H.R. 6304 each provide for targeting of U.S. persons reasonably believed to be located outside the United States for up to 90 days pursuant to a FISC order if statutory criteria are met. Such an order could be renewed for additional 90-day periods upon submission of renewal applications meeting the same standards. In the case of an emergency authorization by the

---

[4107] Stowe v. Devoy, 588 F.2d 336, 342 (2d Cir. 1978); United States v. Cotroni, 527 F.2d 708, 711 (2d Cir. 1975).

[4108] Stonehill v. United States, 405 F.2d 738, 743 (9th Cir. 1969)("Neither the Fourth Amendment to the United States Constitution nor the exclusionary rule of evidence, designed to deter federal officers from violating the Fourth Amendment, is applicable to the acts of foreign officials").

[4109] United States v. Callaway, 446 F.2d 753, 755 (3d Cir. 1971); United States v. Morrow, 537 F.2d 120, 139 (5th Cir. 1976); Stowe v. Devoy, 588 F.2d 336, 341 (2d Cir. 1978); United States v. Rose, 570 F.2d 1358, 1362 (9th Cir. 1978); United States v. Hensel, 699 F.2d 18, 25 (1st Cir. 1983); United States v. Delaplane, 778 F.2d 570, 573-74 (10th Cir. 1985); United States v. Rosenthal, 793 F.2d 1214, 1231-232 (11th Cir. 1986).

[4110] See CRS Congressional Distribution Memorandum entitled "U.S. Citizens' Fourth Amendment Rights Abroad and the Interception of Electronic Communications," by Jennifer K. Elsea (November 13, 2007).

Attorney General of an acquisition, each bill requires notice to a FISC judge by the Attorney General or his designee at the time the decision is made to conduct such an acquisition and requires the filing of an application for a FISC order within seven days of the Attorney General's authorization of the emergency acquisition. Minimization procedures would apply to such an acquisition. Under each of these bills, in the absence of a judicial order approving an acquisition originally authorized by the Attorney General on an emergency basis, the acquisition would terminate when the information sought is obtained, when an application for the order is denied, or when seven days have elapsed, whichever is earliest. Without a FISC order, no information acquired or evidence derived from an emergency acquisition, except under circumstances where the target of the acquisition is determined not to be a U.S. person, may be received in evidence or disclosed in federal, state, or local proceedings; nor could any information concerning a U.S. person acquired from such acquisition subsequently be used or disclosed in any other manner by federal officers or employees without the consent of such person, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person.

Limitations on Liability for Telecommunications Providers Furnishing Aid to the Government

The second of the two critical needs identified by the DNI in his August 2nd statement was a need for liability protection for those who furnish aid to the Government in carrying out its foreign intelligence collection efforts. He sought both retrospective relief from liability for those who are alleged to have aided the Government from September 11, 2001 to the present in connection with electronic surveillance or collection of other communications related information, and prospective liability protection for those telecommunications providers who furnish aid to the government in the future whether pursuant to a court order or a certification by the Attorney General or the Attorney General and the DNI that the acquisition or electronic surveillance involved is lawful and that all statutory requirements have been met.

Under current law, there are a number of statutory sections which provide some limitation on liability for telecommunication providers who furnish aid to the government in connection with electronic surveillance or a physical search,[4111] or the installation of a pen register or trap and trace device[4112] pursuant to a court order under FISA.[4113] In addition, 18 U.S.C. § 2511(2)(a) bars suit in any court against any provider of wire or electronic communication service, its officers,

---

[4111] 50 U.S.C. § 1805(I).

[4112] 50 U.S.C. § 1842(f).

[4113] Section 105B(1) of FISA as added by the Protect America Act, P.L. 110-55, barred causes of action in any court against any person for providing any information, facilities, or assistance in accordance with a directive under that section.

employees, or agents, landlord, custodian, or other specified person for providing information, facilities, or assistance in accordance with the terms of a court order, statutory authorization, or a certification in writing by the Attorney General or a person specified under 18 U.S.C. § 2518(7) that no warrant or court order is required by law, that all statutory requirements have been met, and that the specified assistance is required.[4114]

Prospective relief from liability for those furnishing aid to the government pursuant to a court order or certification or a directive pursuant to statute requiring compliance with government demands for assistance is contemplated in a number of bills, including H.R. 3773 as originally passed, the Senate Amendment to H.R. 3773, the House amendment to the Senate amendment to H.R. 3773, and H.R. 6304. All three versions of H.R. 3773, and H.R. 6304 authorize the FISC to compel compliance through the contempt power, as did P.L. 110-55 while it was in force.

Retroactive immunity presents more difficult issues. There are currently pending a substantial number of law suits against the telecommunications providers who are alleged to have furnished aid to the government in connection with its warrantless surveillance programs since September 11, 2001, and other programs.[4115] Approximately 40 of these suits are currently pending in the Northern District of California under an order of the Judicial Panel on Multidistrict Litigation. On August 9, 2006, pursuant to 28 U.S.C. § 1407, the Judicial Panel on Multidistrict Litigation transferred 17 civil actions that were pending throughout the country to the Northern District of California, and assigned them to Judge Vaughn Walker for coordinated or consolidated pretrial proceedings in *In Re: National Security Agency Telecommunications Records Litigation*, MDL-1791. Another 26 cases were treated as potential tag-along actions under the multidistrict litigation rules. The panel of five federal trial and appellate court judges found that all these class actions share "factual and legal questions regarding alleged Government surveillance of telecommunications activity and the participation in (or cooperation with) that surveillance by individual telecommunications companies," and thus centralization of the cases "is necessary in order to eliminate duplicative discovery, prevent inconsistent

---

[4114] *See also*, defenses against criminal liability in specified circumstances under 50 U.S.C. § 1809(b) (electronic surveillance) and 1827(b) (physical searches). *But see*, civil liability provisions under 50 U.S.C. §§ 1810 and 1828.

[4115] *Cf.*, CRS Report RL33424, *Government Access to Phone Calling Activity and Related Records: Legal Authorities*, by Elizabeth B. Bazan, Gina Marie Stevens, Brian T. Yeh (August 20, 2007). *Cf.*, American Civil Liberties Union v. National Security Agency, 438 F. Supp. 2d 754 (E.D. Mich. 2007), *vacated and remanded on other grounds*, 493 F.3d 644 (6th Cir. 2007), *cert. denied*, ___ U.S. ___, 128 S. Ct. 1334 (2008). The district court, in pertinent part, held the plaintiffs' "datamining" claim barred by application of the state secrets privilege, 438 F. Supp. 2d at 759, 763, 782. This case was brought against government agencies and officers rather than against the telecommunications providers who may have assisted the government in its efforts.

pretrial rulings (particularly with respect to matters involving national security), and conserve the resources of the parties, their counsel and the judiciary."[4116]

Arguments may be made on both sides with respect to whether retroactive immunity should be granted telecommunications providers who are alleged to have assisted the government in such programs. For example, the cooperation of such providers is critical to the government's capacity to pursue electronic surveillance to gather foreign intelligence information, and is also essential for collection of communications records for pattern analysis. If the telecommunication providers who responded to the government's requests or demands for assistance did so in good faith reliance upon assertions by the government that the demand was lawful and that a court order was not required, it may be argued that the providers should be immunized from ill effects flowing from such good faith reliance. Some have argued that the unique factual context militates in favor of such relief from liability, to the extent those who responded to the government's requests for assistance in the wake of 9/11 did so in response to government assertions that their cooperation was necessary to protect against further attacks.

In many of the suits filed, the government has asserted states secrets privilege with respect to the programs involved and the role of any of the telecommunications carriers with respect thereto. This is a common law evidentiary privilege, which may only be asserted by the government, that protects information from discovery when its disclosure would be inimical to the national security. The privilege can come into play in three ways. If the very subject matter of the case is a state secret, an assertion of the privilege can cause

---

[4116] Transfer Order, MDL Docket No. 1791, In Re: National Security Agency Telecommunications Records Litigation. In one of the consolidated suits, Al-Haramain Islamic Foundation, Inc. v. Bush, 507 F.3d 1190, 1206 (9th Cir. 2007), the appellate court remanded the case to the U.S. District Court for the Northern District of California "to consider whether FISA preempts the state secrets privilege and for any proceedings collateral to that determination." On July 2, 2008, in In re: National Security Agency Telecommunications Records Litigation, MDL Docket No. 06-1791 VRW, slip op. at 2, 28 (N.D. Cal. July 2, 2008) (pertaining to Al-Haramain Islamic Foundation v. Bush, C-07-0109 VRW), Judge Walker, having reviewed the pertinent statutory language and the related legislative history, *id*., slip op. at 10-28, held, in part, that FISA preempts the state secrets privilege in connection with electronic surveillance for intelligence purposes in connection with cases within its purview. The court stated the case before it was such a case, and that FISA therefore appeared "to displace the state secrets privilege for purposes of plaintiffs' claims." *Id.* However, the court observed that FISA's statutory structure does not appear to provide the plaintiffs with a viable remedy unless they are able to show that they are "aggrieved persons" within the meaning of FISA. *Id.*

Other actions have been initiated against telecommunications providers by a public utility commission to seek information from or impose sanctions upon those providers. *See, e.g*., State of Maine Public Utilities Commission, Request for Commission Investigation into Whether Verizon is Cooperating in Maine with the National Security Agency's Warrantless Surveillance Program, Docket No.2006-274.

the case to be immediately dismissed and the action barred. If, however, this prong of the state secrets privilege does not apply, the privilege may operate to bar admission into evidence of information which will damage the security of the United States. The plaintiff then goes forward on the basis of evidence not covered. If the plaintiff cannot prove a prima facie case with nonprivileged evidence, then the case may be dismissed.[4117] On the other hand, if the privilege deprives a defendant of information that would otherwise give the defendant a valid defense to the claim, then the court may grant summary judgment to the defendant.[4118] In the current context, to the extent that a defendant telecommunications providers may have a valid claim of immunity under 18 U.S.C. § 2511(2)(a), but for the application of the state secrets privilege to the identities of any providers who may have furnished aid to the government, an argument may be made that the telecommunications providers so impacted should be afforded immunity from suit.

On the other hand, such suits may be the only means by which those who may have been adversely impacted by such government activities may obtain any remedy for any injuries incurred. These injuries may have impacted First and Fourth Amendment protected interests, and there may be no other means of vindicating those rights. In addition, the telecommunications providers provide the front line of defense of those rights against governmental abuse if the government demand or request is unlawful. In some instances, it may be argued that a telecommunications provider has a statutory obligation to protect customer records from unlawful access.[4119] Such arguments militate against affording relief from liability to any providers who may have permitted unlawful access.

In addition to these arguments, some have argued that, because the Administration has not shared information repeatedly sought by some committees of jurisdiction with respect to the role of the telecommunications

---

[4117] This is the basis upon which the Sixth Circuit dismissed ACLU v. NSA, *supra*, on appeal, finding that the plaintiffs would be unable to demonstrate standing from nonprivileged evidence.

[4118] *See*, Hepting v. AT&T, 439 F. Supp. 2d 974, 984 (N.D. Cal. 2006), *citing* Kasza v. Browner, 133 F.3d 1159, 1166 (9th Cir. 1998). The *Hepting* court held that the case was not barred on the basis that its very nature was a state secret, but that there was insufficient information to determine whether the other two prongs applied. The other consolidated cases have been stayed pending the interlocutory appeal of the *Hepting* decision to the U.S. Court of Appeals for the Ninth Circuit, Hepting v. AT&T Corporation, Docket # 06-17132 consolidated with Docket # 06-17137. On appeal, the *Hepting* case was consolidated with Al-Haramain Islamic Foundation v. Bush, Docket # 06-36083. After argument, the court of appeals determined that the claimed facts and circumstances in the two cases were distinct and entered an order stating that the two cases were no longer consolidated for any purpose, Al-Haramain Islamic Foundation, Inc. v. Bush, 507 F.3d 1190, 1196 n. 3 (9th Cir. 2007).

[4119] *See, e.g.*, 47 U.S.C. § 222 (protection of customer proprietary network information).

providers in the TSP or other pertinent intelligence activities, the Congress does not have adequate information to determine whether relief for the telecommunications carriers is warranted.

Legislative Response

Under proposed section 802(a) of FISA in Title II of H.R. 6304, a civil action[4120] may not lie or be maintained in a federal or state court[4121] against any person[4122] for providing assistance[4123] to an element of the intelligence community, and must be dismissed promptly, if the Attorney General certifies to the U.S. district court in which the action is pending that:

> (1) any assistance by that person was provided pursuant to an order of the court established under section 103(a) directing such assistance;
> (2) any assistance by that person was provided pursuant to a certification in writing under section 2511(2)(a)(ii)(B) or 2709(b) of title 18, United States Code;
> (3) any assistance by that person was provided pursuant to a directive under section 102(a)(4), 105B(e), as added by section 2 of the Protect America Act of 2007 (Public Law 110-55), or 702(h) directing such assistance;
> (4) in the case of a covered civil action, the assistance alleged to have been provided by the electronic communication service provider was —
>
> > (A) in connection with an intelligence activity involving communications that was—

[4120] "Civil action" is defined in proposed subsection 801(2), to include a "covered civil action." The term "covered civil action" is defined under section 801(5) to mean a civil action filed in a federal or state court that "alleges that an electronic communication service provider furnished assistance to an element of the intelligence community;" and "seeks monetary or other relief from the electronic communication service provider related to the provision of such assistance."

[4121] Under proposed subsection 802(g), a civil action against a person for providing assistance to an element of the intelligence community that is brought in a state court shall be deemed to arise under the Constitution and laws of the United States and shall be removable under 28 U.S.C. § 1441.

[4122] "Person" is defined in proposed subsection 801(8) to mean an electronic communication service provider, as defined in proposed subsection 801(6); or a landlord, custodian, or other person who may be authorized or required to furnish assistance pursuant to an order of the court established under section 103(a) of FISA directing such assistance; a certification in writing under 18 U.S.C. §§ 2511(2)(a)(ii)(B) or 2709(b); or a directive under section 102(a)(4) of FISA, 105B(e) of FISA, as added by section 2 of the Protect America Act of 2007 (Public Law 110-55), or 702(h) of FISA.

[4123] "Assistance" is defined under proposed subsection 801(1) to mean "the provision of, or the provision of access to, information (including communication contents, communications records, or other information relating to a customer or communication), facilities, or another form of assistance."

(i) authorized by the President during the period beginning on September 11, 2001, and ending on January 17, 2007; and
(ii) designed to detect or prevent a terrorist attack, or activities in preparation for a terrorist attack, against the United States; and

(B) the subject of a written request or directive, or a series of written requests or directives, from the Attorney General or the head of an element of the intelligence community (or the deputy of such person) to the electronic communication service provider indicating that the activity was —

(i) authorized by the President; and
(ii) determined to be lawful; or

(5) the person did not provide the alleged assistance.

Under proposed subsection 802(b) of FISA, such a certification shall be given effect unless the court finds that it is not supported by substantial evidence provided to the court under that section. In the course of its judicial review, the U.S. district court may examine the court order, certification, written request, or directive described in proposed subsection 802(a) and any relevant court order, certification, written request, or directive submitted to the court by the parties under proposed subsection 802(d). Any such party would be permitted to participate in briefing or argument of any legal issue in a judicial proceeding under this section to the extent that such participation does not require disclosure of classified information to that party. Any relevant classified information would be reviewed in camera and exparte. Any portion of the court's written order that would reveal classified information would be issued in camera and ex parte and maintain it under seal. Upon filing of a declaration by the Attorney General under 28 U.S.C. § 1746 that disclosure of such a certification or of the supplemental materials provided pursuant to proposed subsections 802 (b) or (d) would harm the national security of the United States, the U.S. district court would be required to review such certification and the supplemental materials in camera and ex parte. Any public disclosure of such certification and supplemental materials would be limited to a statement as to whether the case is dismissed and a description of the legal standards that govern the order, without disclosing the paragraph of subsection (a) that is the basis for the certification. If H.R. 6304 were to be enacted into law, proposed Section 802 of FISA would apply to a civil action pending on or filed after the date of the enactment.

The Senate amendment to H.R. 3773 bars covered civil actions in a federal or state court and requires that such an action must be dismissed promptly if the Attorney General or above certifies to the court that the assistance alleged to have been provided by the electronic communication service provider was in connection with an intelligence activity involving communications that was authorized by the President during the period beginning on September 11, 2001, and ending on January 17, 2007; and designed to detect or prevent a terrorist attack, or activities in preparation for a terrorist attack, against the United States; and described in a written request or directive from the Attorney General or the

head of an element of the intelligence community (or the deputy of such person) to the electronic communication service provider indicating that the activity was authorized by the President and determined to be lawful. A covered civil action in federal or state court would also be barred and should be dismissed promptly if the Attorney General certifies to the court that the electronic communication service provider did not provide the alleged assistance. The Attorney General's certification would be subject to judicial review under an abuse of discretion standard. If the Attorney General files a declaration under 28 U.S.C. § 1746 that disclosure of a certification made under subsection 202(a) of the bill would harm United States national security, the court shall review the certification in camera and ex parte, and limit public disclosure concerning such certification, including any public order following such ex parte review, to a statement that the conditions of subsection 202(a) of the bill have been met, without disclosing the subparagraph of subsection 202(a)(1) that is the basis for the certification. The authorities of the Attorney General under section 202 are to be performed by the Attorney General, or the Acting Attorney General, or a designee in a position not lower than the Deputy Attorney General.

The House-passed amendment to the Senate Amendment took a different approach. Proposed section 802, in part, provides authority for the government to intervene in any covered civil action. Any party may submit to the court evidence, briefs, arguments, or other information on any matter with respect to which a state secrets privilege has been asserted. The section also authorizes the court to review any such submissions in accordance with procedures set forth in section 106(f) of FISA; and permits the court, on motion of the Attorney General, to take additional steps to protect classified information. The court, to the extent practicable and consistent with national security would be permitted to request any party to present briefs and arguments on any legal question the court finds raised by such submission, regardless of whether that party has access to the submission. Under new subsection 802(e) of FISA, for any covered civil action alleging that a person provided assistance to an element of the intelligence community pursuant to a request or directive during the period from September 11, 2001 through January 17, 2007, the Attorney General would be required to provide to the court any request or directive related to the allegations under the procedures set forth in new subsection 802(b).

H.R. 6304, therefore, differs from prior House and Senate amendments to H.R. 3773 in a number of respects, while having similarities to them in others. Both H.R. 6304 and the Senate amendment would bar civil actions in federal or state court against persons providing assistance to an element of the intelligence community if the Attorney General certifies that certain statutory criteria are met. They differ to some degree as to the criteria involved.

H.R. 6304 provides for judicial review of the Attorney General's certification under a substantial evidence standard, while the Senate amendment to H.R. 3773 provides for review of the Attorney General's certification using an abuse of discretion standard. The House amendment to the Senate amendment to H.R.

3773 provides for judicial review of any submissions by any party relating any matter as to which state secrets privilege has been asserted, but does not specify the standard of review.

H.R. 6304 expressly permits the district court, in its review, to examine any court order, certification, written request, or directive described in proposed subsection 802(a) or submitted to the court by the parties, and, permits party participation in briefs and arguments on any legal issue in the judicial proceeding to the extent that such participation does not require disclosure of classified information to that party. This does not have a parallel in the Senate amendment. However, it has some points of similarity with the House amendment, which permits submissions by the parties of evidence, briefs, arguments, or other information relating to any matter with respect to which state secrets privilege has been asserted, while providing protections for classified information. For any covered civil action alleging that a person provided assistance to an element of the intelligence community pursuant to a request or directive during the September 11, 2001 to January 17, 2007 period, the House amendment requires the Attorney General to provide the court with any request or directive related to the allegations.

All three bills make provision for ex parte, in camera review of classified information. H.R. 6304 and the Senate amendment both place restrictions on public disclosure of information regarding the certification and the court's order.

Presidential Authority to Conduct Warrantless Electronic Surveillance to Gather Foreign Intelligence Information, Memorandum (January 5, 2006).

ELIZABETH B. BAZAN & JENNIFER K. ELSEA, CONGRESSIONAL RESEARCH SERV., PRESIDENTIAL AUTHORITY TO CONDUCT WARRANTLESS ELECTRONIC SURVEILLANCE TO GATHER FOREIGN INTELLIGENCE INFORMATION, MEMORANDUM (2006), *available at* http://www.intelligencelaw.com/library/secondary/crs/pdf/memo_1-5-2006.pdf.

SUBJECT:
Presidential Authority to Conduct Warrantless Electronic Surveillance to Gather Foreign Intelligence Information

FROM:
Elizabeth B. Bazan and Jennifer K. Elsea
Legislative Attorneys
American Law Division

Introduction

Recent media revelations that the President authorized the National Security Agency (NSA) to collect signals intelligence[4124] from communications involving U.S. persons within the United States, without obtaining a warrant or court

---

[4124] "Signals intelligence" is defined in the DEPARTMENT OF DEFENSE DICTIONARY OF MILITARY AND ASSOCIATED TERMS, Joint Publication 1-02 (April 12, 2001), as follows:

1. A category of intelligence comprising either individually or in combination all communications intelligence, electronic intelligence, and foreign instrumentation signals intelligence, however transmitted. 2. Intelligence derived from communications, electronic, and foreign instrumentation signals. Also called SIGINT. . . . Id. at 390 (cross-references omitted). "Communications intelligence" is defined as "Technical information and intelligence derived from foreign communications by other than the intended recipients. Also called COMINT." Id. at 84. "Electronic intelligence" is defined as "Technical and geolocation intelligence derived from foreign non-communications electromagnetic radiations emanating from other than nuclear detonations or radioactive sources. Also called ELINT. . . ." Id. at 140 (cross-references omitted). "Foreign instrumentation signals intelligence" is defined as:

Technical information and intelligence derived from the intercept of foreign electromagnetic emissions associated with the testing and operational deployment of non-US aerospace, surface, and subsurface systems. Foreign instrumentation signals intelligence is a subcategory of signals intelligence. Foreign instrumentation signals include but are not limited to telemetry, beaconry, electronic interrogators, and video data links. Also called FISINT. . . .

Id. at 167 (cross-references omitted).

order,[4125] raise numerous questions regarding the President's authority to order warrantless electronic surveillance. Little information is currently known about the full extent of the NSA domestic surveillance, which was revealed by the New York Times in December, 2005, but allegedly began after the President issued a secret order in 2002. Attorney General Alberto Gonzales laid out some of its parameters, telling reporters that it involves "intercepts of contents of communications where one . . . party to the communication is outside the United States" and the government has "a reasonable basis to conclude that one party to the communication is a member of al Qaeda, affiliated with al Qaeda, or a member of an organization affiliated with al Qaeda, or working in support of al Qaeda."[4126] The aim of the program, according to Principal Deputy Director for National Intelligence General Michael Hayden, is not "to collect reams of intelligence, but to detect and warn and prevent [terrorist] attacks."[4127]

The President has stated that he believes his order to be fully supported by the Constitution and the laws of the United States,[4128] and the Attorney General clarified that the Administration bases its authority both on inherent presidential powers and the joint resolution authorizing the use of "all necessary and appropriate force" to engage militarily those responsible for the terrorist attacks of September 11, 2001 ("AUMF").[4129] Although the resolution does not expressly

---

[4125] James Risen and Eric Lichtblau, Bush Lets U.S. Spy on Callers Without Courts, N.Y. TIMES, Dec. 16, 2005, at 1, 22 (citing anonymous government officials to report that the executive order, which allows some warrantless eavesdropping on persons inside the United States, "is based on classified legal opinions that assert that the president has broad powers to order such searches, derived in part from the September 2001 Congressional resolution authorizing him to wage war on Al Qaeda and other terrorist groups").

[4126] See Press Release, White House, Press Briefing by Attorney General Alberto Gonzales and General Michael Hayden, Principal Deputy Director for National Intelligence (Dec. 19, 2005) (hereinafter Gonzales Press Conference), available at [http://www.whitehouse.gov/news/releases/2005/12/20051219-1.html]. The Attorney General emphasized that his discussion addressed the legal underpinnings only for those operational aspects that have already been disclosed by the President, explaining that "the program remains highly classified; there are many operational aspects of the program that have still not been disclosed and we want to protect that because those aspects of the program are very, very important to protect the national security of this country." Id.

[4127] Id.(describing the program as more "aggressive" than traditional electronic surveillance under FISA, but also as "less intrusive").

[4128] President Bush's Radio Address of December 17, 2005, excerpted in 'A Vital Tool,' USA TODAY, December 19, 2005, at A12.

[4129] Authorization for Use of Military Force ("the AUMF"), Pub. L. 107-40, 115 Stat. 224 (2001). Attorney General Gonzales explained

Justice O'Connor . . . said, it was clear and unmistakable that the Congress had authorized the detention of an American citizen captured on the battlefield as an enemy combatant for the

specify what it authorizes as "necessary and appropriate force," the Administration discerns the intent of Congress to provide the statutory authority necessary take virtually any action reasonably calculated to prevent a terrorist attack, including by overriding at least some statutory prohibitions that contain exceptions for conduct that is "otherwise authorized by statute." Specifically, the Administration asserts that a part of the Foreign Intelligence Surveillance Act (FISA)[4130] that punishes those who conduct "electronic surveillance under color of law except as authorized by statute"[4131] does not bar the NSA surveillance at issue because the AUMF is just such a statute.[4132] On December 22, 2005, the Department of Justice Office of Legislative Affairs released a letter to certain members of the House and Senate intelligence committees setting forth in somewhat greater detail the Administration's position with regard to the legal authority supporting the NSA activities described by the President.[4133]

The Administration's views have been the subject of debate. Critics challenge the notion that federal statutes regarding government eavesdropping may be bypassed by executive order, or that such laws were implicitly superceded by Congress's authorization to use military force. Others, however, have expressed the view that established wiretap procedures are too cumbersome and slow to be effective in the war against terrorism, and that the threat of terrorism justifies extraordinary measures the President deems appropriate, and some agree that Congress authorized the measures when it authorized the use of military force.

---

remainder — the duration of the hostilities. So even though the authorization to use force did not mention the word, 'detention,' she felt that detention of enemy soldiers captured on the battlefield was a fundamental incident of waging war, and therefore, had been authorized by Congress when they used the words, 'authorize the President to use all necessary and appropriate force.'

For the same reason, we believe signals intelligence is even more a fundamental incident of war, and we believe has been authorized by the Congress. And even though signals intelligence is not mentioned in the authorization to use force, we believe that the Court would apply the same reasoning to recognize the authorization by Congress to engage in this kind of electronic surveillance.

Gonzales Press Conference, supra note 3.

[4130] Pub. L. 95-511, Title I, 92 Stat. 1796 (Oct. 25, 1978), codified as amended at 50 U.S.C. §§ 1801 et seq.

[4131] 50 U.S.C. § 1809 (emphasis added).

[4132] See Gonzales Press Conference, supra note 3.

[4133] Letter from Assistant Attorney General William E. Moschella to Chairman Roberts and Vice Chairman Rockefeller of the Senate Select Committee on Intelligence and Chairman Hoekstra and Ranking Minority Member Harman of the House Permanent Select Committee on Intelligence (Dec. 22, 2005) (hereinafter "OLA Letter").

This memorandum lays out a general framework for analyzing the constitutional and statutory issues raised by the NSA electronic surveillance activity. It then outlines the legal framework regulating electronic surveillance by the government, explores ambiguities in those statutes that could provide exceptions for the NSA intelligence-gathering operation at issue, and addresses the arguments that the President possesses inherent authority to order the operations or that Congress has provided such authority.

Constitutional Separation of Powers

Foreign intelligence collection is not among Congress's powers enumerated in Article I of the Constitution, nor is it expressly mentioned in Article II as a responsibility of the President. Yet it is difficult to imagine that the Framers intended to reserve foreign intelligence collection to the states or to deny the authority to the federal government altogether. It is more likely that the power to collect intelligence resides somewhere within the domain of foreign affairs and war powers, both of which areas are inhabited to some degree by the President together with the Congress.[4134]

The *Steel Seizure Case*[4135] is frequently cited as providing a framework for the courts to decide the extent of the President's authority, particularly in matters involving national security. In that Korean War-era case, the Supreme Court declared unconstitutional a presidential order seizing control of steel mills that had ceased production due to a labor dispute, an action justified by President Truman on the basis of wartime exigencies and his role as Commander-in-Chief,[4136] despite the fact that Congress had considered but rejected earlier

---

[4134] The Constitution specifically gives to Congress the power to "provide for the common Defence," U.S.CONST. Art. I, § 8, cl. 1; to "declare War, grant Letters of Marque and Reprisal, and make Rules concerning Captures on Land and Water," id. § 8, cl. 11; "To raise and support Armies," and "To provide and maintain a Navy," id. § 8, cls. 12-13; "To make Rules for the Government and Regulation of the land and naval Forces," id. § 8, cl. 14, "To declare War," id. § 8, cl. 1; and to "make all Laws which shall be necessary and proper for carrying into Execution the foregoing Powers, and all other Powers vested by this Constitution in the Government of the United States, or in any Department or Officer thereof," id. § 8, cl. 18. The President is responsible for "tak[ing] Care that the Laws [are] faithfully executed," Art. II, § 3, and serves as the Commander-in-Chief of the Army and Navy, id. § 2, cl. 1.

[4135] Youngstown Sheet and Tube Co. v. Sawyer, 343 U.S. 579 (1952).

[4136] Id. at 582 (explaining the government's position that the order to seize the steel mills "was made on findings of the President that his action was necessary to avert a national catastrophe which would inevitably result from a stoppage of steel production, and that in meeting this grave emergency the President was acting within the aggregate of his constitutional powers as the Nation's Chief Executive and the Commander in Chief of the Armed Forces of the United States.").

legislation that would have authorized the measure,[4137] and that other statutory means were available to address the steel shortage.[4138] The Court remarked that

> *It is clear that if the President had authority to issue the order he did, it must be found in some provision of the Constitution. And it is not claimed that express constitutional language grants this power to the President. The contention is that presidential power should be implied from the aggregate of his powers under the Constitution. Particular reliance is placed on provisions in Article II which say that 'The executive Power shall be vested in a President . . .'; that 'he shall take Care that the Laws be faithfully executed'; and that he 'shall be Commander in Chief of the Army and Navy of the United States.'*
>
> *The order cannot properly be sustained as an exercise of the President's military power as Commander in Chief of the Armed Forces. The Government attempts to do so by citing a number of cases upholding broad powers in military commanders engaged in day-to-day fighting in a theater of war. Such cases need not concern us here. Even though 'theater of war' be an expanding concept, we cannot with faithfulness to our constitutional system hold that the Commander in Chief of the Armed Forces has the ultimate power as such to take possession of private property in order to keep labor disputes from stopping production. This is a job for the Nation's lawmakers, not for its military authorities.[4139]*

The Court also rejected the argument that past similar assertions of authority by presidents bolstered the executive claims of constitutional power:

> *It is said that other Presidents without congressional authority have taken possession of private business enterprises in order to settle labor disputes. But even if this be true, Congress has not thereby lost its exclusive constitutional authority to make laws necessary and proper to carry out the powers vested by the*

[4137] Id. at 586 (noting that "[w]hen the Taft-Hartley Act was under consideration in 1947, Congress rejected an amendment which would have authorized such governmental seizures in cases of emergency").

[4138] Id. at 585. The Court took notice of two statutes that would have allowed for the seizure of personal and real property under certain circumstances, but noted that they had not been relied upon and the relevant conditions had not been met. In particular, the Court dismissed the government's reference to the seizure provisions of § 201 (b) of the Defense Production Act, which the government had apparently not invoked because it was "'much too cumbersome, involved, and time-consuming for the crisis which was at hand.'" Id. at 586.

[4139] Id. at 587.

> *Constitution 'in the Government of the United States, or any Department or Officer thereof.'*[4140]

The *Steel Seizure Case* is not remembered as much for the majority opinion as it is for the concurring opinion of Justice Robert Jackson, who took a more nuanced view and laid out what is commonly regarded as the seminal explication of separation-of-powers matters between Congress and the President. Justice Jackson set forth the following oft-cited formula:

> *1. When the President acts pursuant to an express or implied authorization of Congress, his authority is at its maximum, for it includes all that he possesses in his own right plus all that Congress can delegate. . . . A seizure executed by the President pursuant to an Act of Congress would be supported by the strongest of presumptions and the widest latitude of judicial interpretation, and the burden of persuasion would rest heavily upon any who might attack it.*
> *2. When the President acts in absence of either a congressional grant or denial of authority, he can only rely upon his own independent powers, but there is a zone of twilight in which he and Congress may have concurrent authority, or in which its distribution is uncertain. Therefore, congressional inertia, indifference or quiescence may sometimes, at least as a practical matter, enable, if not invite, measures on independent presidential responsibility. In this area, any actual test of power is likely to depend on the imperatives of events and contemporary imponderables rather than on abstract theories of law.*
> *3. When the President takes measures incompatible with the expressed or implied will of Congress, his power is at its lowest ebb, for then he can rely only upon his own constitutional powers minus any constitutional powers of Congress over the matter. Courts can sustain exclusive Presidential control in such a case only by disabling the Congress from acting upon the subject. Presidential claim to a power at once so conclusive and preclusive must be scrutinized with caution, for what is at stake is the equilibrium established by our constitutional system.*[4141]

To ascertain where in this framework the President's claimed authority might fall appears to require a determination of the Congress's will and an assessment of how the Constitution allocates the asserted power between the President and Congress, if at all. If the Constitution forbids the conduct, then the court has a

---

[4140] Id. at 589.

[4141] Id. at 637-38 (Jackson, J., concurring) (footnotes and citations omitted).

duty to find the conduct invalid, even if the President and Congress have acted in concert. In the absence of a constitutional bar, Congress's support matters, except in the rare case where the President alone is entrusted with the specific power in question. In other words, under this view, the President may sometimes have the effective power to take unilateral action in the absence of any action on the part of Congress to indicate its will, but this should not be taken to mean that the President possesses the inherent authority to exercise full authority in a particular field without Congress's ability to encroach.

William Rehnquist, at the time an Associate Justice of the Supreme Court, took the opportunity in *Dames & Moore v. Regan*[4142] to refine Justice Jackson's formula with respect to the cases falling within the second classification, the "zone of twilight in which he and Congress may have concurrent authority, or in which its distribution is uncertain."[4143]

> *In such a case the analysis becomes more complicated, and the validity of the President's action, at least so far as separation-of-powers principles are concerned, hinges on a consideration of all the circumstances which might shed light on the views of the Legislative Branch toward such action, including "congressional inertia, indifference or quiescence."*[4144]
>
> *[I]t is doubtless the case that executive action in any particular instance falls, not neatly in one of three pigeonholes, but rather at some point along a spectrum running from explicit congressional authorization to explicit congressional prohibition. This is particularly true as respects cases such as the one before us, involving responses to international crises the nature of which Congress can hardly have been expected to anticipate in any detail.*[4145]

In *Dames & Moore*, petitioners had challenged President Carter's executive order establishing regulations to further compliance with the terms of an executive agreement he had entered into for the purpose of ending the hostage crisis with Iran. The orders, among other things, directed that legal recourse for breaches of contract with Iran and other causes of action must be pursued before a special tribunal established by the Algiers Accords. President Carter relied largely on the

---

[4142] 453 U.S. 668 (1981) (citing Youngstown at 637).

[4143] Id. at 668-69.

[4144] Id.

[4145] Id. at 669.

International Economic Emergency Powers Act (IEEPA),[4146] which provided explicit support for most of the measures taken, but could not be read to authorize actions affecting the suspension of claims in U.S. courts. The Carter Administration also cited the broad language of the Hostage Act, which states that "the President shall use such means, not amounting to acts of war, as he may think necessary and proper to obtain or effectuate the release" of the hostages.[4147] Justice Rehnquist wrote for the majority

> *Although we have declined to conclude that the IEEPA or the Hostage Act directly authorizes the President's suspension of claims for the reasons noted, we cannot ignore the general tenor of Congress' legislation in this area in trying to determine whether the President is acting alone or at least with the acceptance of Congress. As we have noted, Congress cannot anticipate and legislate with regard to every possible action the President may find it necessary to take or every possible situation in which he might act. Such failure of Congress specifically to delegate authority does not, "especially . . . in the areas of foreign policy and national security," imply "congressional disapproval" of action taken by the Executive. On the contrary, the enactment of legislation closely related to the question of the President's authority in a particular case which evinces legislative intent to accord the President broad discretion may be considered to "invite" "measures on independent presidential responsibility." At least this is so where there is no contrary indication of legislative intent and when, as here, there is a history of congressional acquiescence in conduct of the sort engaged in by the President.*[4148]

The Court remarked that Congress's implicit approval of the longstanding presidential practice of settling international claims by executive agreement was critical to its holding that the challenged actions were not in conflict with acts of Congress.[4149] The Court cited Justice Frankfurter's concurrence in Youngstown stating that "a systematic, unbroken, executive practice, long pursued to the knowledge of the Congress and never before questioned . . . may be treated as a

---

[4146] Pub. L. 95-223, 91 Stat. 1626, codified as amended at 50 U.S.C. §§ 1701 et.seq.

[4147] Id at 676 (citing the Hostage Act, 22 U. S. C. § 1732).

[4148] Id. at 678-79 (internal citations omitted).

[4149] Id. at 680 (citing the International Claims Settlement Act of 1949, 64 Stat. 13, codified as amended at 22 U.S.C. § 1621 et seq. (1976 ed. and Supp. IV)).

gloss on 'Executive Power' vested in the President by § 1 of Art. II."[4150] Finally, the Court stressed that its holding was narrow:

> *We do not decide that the President possesses plenary power to settle claims, even as against foreign governmental entities. . . . But where, as here, the settlement of claims has been determined to be a necessary incident to the resolution of a major foreign policy dispute between our country and another, and where, as here, we can conclude that Congress acquiesced in the President's action, we are not prepared to say that the President lacks the power to settle such claims.*[4151]

A review of the history of intelligence collection and its regulation by Congress suggests that the two political branches have never quite achieved a meeting of the minds regarding their respective powers. Presidents have long contended that the ability to conduct surveillance for intelligence purposes is a purely executive function, and have tended to make broad assertions of authority while resisting efforts on the part of Congress or the courts to impose restrictions. Congress has asserted itself with respect to domestic surveillance, but has largely left matters involving overseas surveillance to executive self-regulation, subject to congressional oversight and willingness to provide funds.[4152]

Background: Government Surveillance

Investigations for the purpose of gathering foreign intelligence give rise to a tension between the Government's legitimate national security interests and the protection of privacy interests and First Amendment rights.

The Fourth Amendment

The Fourth Amendment to the Constitution provides:

> *The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.*

[4150] Id at 686 (citing Youngstown at 610-611(Frankfurter, J., concurring)).

[4151] Id. at 688.

[4152] For background on the evolution of U.S. intelligence operations, see CRS Report RL32500, Proposals for Intelligence Reorganization, 1949-2004, by Richard A. Best, Jr.

While the right against unreasonable searches and seizures was originally applied only to tangible things, Supreme Court jurisprudence eventually expanded the contours of the Fourth Amendment to cover intangible items such as conversations. As communications technology has advanced, the technology for intrusion into private conversations has kept pace, as have government efforts to exploit such technology for law enforcement and intelligence purposes. At the same time, the Court has expanded its interpretation of the scope of the Fourth Amendment with respect to such techniques, and Congress has legislated both to protect privacy and to enable the government to pursue its legitimate interests in enforcing the law and gathering foreign intelligence information. Yet the precise boundaries of what the Constitution allows, as well as what it requires, are not fully demarcated, and the relevant statutes are not entirely free from ambiguity.

The Origin of Wiretap Warrants

In *Katz v. United States*,[4153] the Court held for the first time that the protections of the Fourth Amendment extend to circumstances involving electronic surveillance of oral communications without physical intrusion.[4154] In response, Congress enacted Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("Title III")[4155] to provide for search warrants to authorize electronic surveillance for law enforcement purposes, but prohibiting such surveillance in other instances not authorized by law. The *Katz* Court noted that its holding did not extend to cases involving national security, and Congress did not then attempt to regulate national security surveillance. Title III, as originally enacted, contained an exception. It stated that

> *Nothing contained in this chapter or in section 605 of the Communications Act . . . shall limit the constitutional power of the President to take such measures as he deems necessary to protect the Nation against actual or potential attack or other hostile acts of a foreign power, to obtain foreign intelligence information deemed essential to the security of the United States, or to protect national security information against foreign intelligence activities. . . .*[4156]

[4153] Katz v. United States, 389 U.S. 347, 353 (1967), overruling Olmstead v. United States, 277 U.S. 438 (1928).

[4154] Id. at 359 n.23.

[4155] Pub. L. 90-351, 82 Stat. 211, codified as amended at 18 U.S.C. §§ 2510 et seq. For more background see CRS Report 98-326: Privacy: An Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping, by Charles Doyle and Gina Stevens.

[4156] 82 Stat. 214, formerly codified at 18 U.S.C. § 2511(3). The Supreme Court interpreted this provision not as a conferral or recognition of executive authority, but rather, an indication that Congress had "left presidential powers where it found them." United States v. United States

Intelligence Surveillance

Several years later, the Supreme Court addressed electronic surveillance for domestic intelligence purposes. In *United States v. United States District Court*, 407 U.S. 297 (1972) (the *Keith* case), the United States sought a writ of mandamus to compel a district judge to vacate an order directing the United States to fully disclose electronically monitored conversations. The Sixth Circuit refused to grant the writ,[4157] and the Supreme Court granted certiorari and affirmed the lower court decision. The Supreme Court regarded *Katz* as "implicitly recogniz[ing] that the broad and unsuspected governmental incursions into conversational privacy which electronic surveillance entails necessitate the application of Fourth Amendment safeguards."[4158] Mr. Justice Powell, writing for the *Keith* Court, framed the matter before the Court as follows:

> *The issue before us is an important one for the people of our country and their Government. It involves the delicate question of the President's power, acting through the Attorney General, to authorize electronic surveillance in internal security matters without prior judicial approval. Successive Presidents for more than one-quarter of a century have authorized such surveillance in varying degrees, without guidance from the Congress or a definitive decision of this Court. This case brings the issue here for the first time. Its resolution is a matter of national concern, requiring sensitivity both to the Government's right to protect itself from unlawful subversion and attack and to the citizen's right to be secure in his privacy against unreasonable Government intrusion.*[4159]

The Court held that, in the case of intelligence gathering involving domestic security surveillance, prior judicial approval was required to satisfythe Fourth Amendment.[4160] Justice Powell emphasized that the case before it "require[d] no

---

District Court, 407 U.S. 297, 303 (1972). The Senate Judiciary Committee noted, however, that the "highly controversial disclaimer has often been cited as evidence of a congressional ratification of the president's inherent constitutional power to engage in electronic surveillance in order to obtain foreign intelligence information essential to the national security." S. REP. NO. 95-604(I), at 6-7 (1978).

[4157] 444 F. 2d 651.

[4158] United States v. United States District Court, 407 U.S. 297, 313-14 (1972).

[4159] 407 U.S. at 299.

[4160] Id. at 313-14, 317, 319-20. Thus, the Court stated, "These Fourth Amendment freedoms cannot properly be guaranteed if domestic security surveillances may be conducted solely within

judgment on the scope of the President's surveillance power with respect to the activities of foreign powers, within or without the country."[4161] The Court expressed no opinion as to "the issues which may be involved with respect to activities of foreign powers or their agents,"[4162] but invited Congress to establish statutory guidelines.[4163] Thus, at least insofar as domestic surveillance is

---

the discretion of the Executive Branch. . . . The Government argues the special circumstances applicable to domestic security surveillances necessitate a further exception to the warrant requirement. It is urged that the requirement of prior judicial review would obstruct the President in the discharge of his constitutional duty to protect domestic security. . . ." Id. at 317-18. The Government also argued that such surveillances were for intelligence gathering purposes; that the courts "as a practical matter would have neither the knowledge nor the techniques to determine whether there was probable cause to believe that surveillance was necessary to protect national security;" and that disclosure to a magistrate and court personnel of information involved in the domestic security surveillances "would create serious potential dangers to the national security and to the lives of informants and agents" due to the increased risk of leaks. Id. at 318-19. The Court found that "these contentions on behalf of a complete exemption from the warrant requirement, when urged on behalf of the President and the national security in its domestic implications, merit the most careful consideration," but concluded that a case had not been made for a departure from Fourth Amendment standards. Id. at 319-20. Justice Powell also observed that,

National security cases . . . often reflect a convergence of First and Fourth Amendment values not present in cases of "ordinary" crime. Though the investigative duty of the executive may be stronger in such cases, so also is there greater jeopardy to constitutionally protected speech. "Historically the struggle for freedom of speech and press in England was bound up with the issue of the scope of the search and seizure power," Marcus v. Search Warrant, 367 U.S. 717, 724 (1961). . . . Fourth Amendment protections become the more necessary when the targets of official surveillance may be those suspected of unorthodoxy in their political beliefs. The danger to political dissent is acute where the Government attempts to act under so vague a concept as the power to protect "domestic security." . . . Id. at 313-14.

[4161] Id. at 308.

[4162] Id. at 321-22. The Keith Court also stated, "Further, the instant case requires no judgment on the scope of the President's surveillance power with respect to the activities of foreign powers within or without this country." Id. at 308.

[4163] We recognize that domestic surveillance may involve different policy and practical considerations from the surveillance of "ordinary crime." The gathering of security intelligence is often long range and involves the interrelation of various sources and types of information. The exact targets of such surveillance may be more difficult to identify than in surveillance operations against many types of crime specified in Title III [of the Omnibus Crime Control and Safe Streets Act, 18 U.S.C. § 2510 et seq.]. Often, too, the emphasis of domestic intelligence gathering is on the prevention of unlawful activity or the enhancement of the Government's preparedness for some possible future crisis or emergency. Thus, the focus of domestic surveillance may be less precise than that directed against more conventional types of crimes. Given these potential distinctions between Title III criminal surveillances and those involving domestic security, Congress may wish to consider protective standards for the latter which differ from those already prescribed for specified crimes in Title III. Different standards may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens. For the warrant application may vary according to the governmental interest to be enforced and the nature of citizen rights deserving

concerned, the Court has recognized that Congress has a role in establishing rules in matters that touch on national security.

Court of appeals decisions following *Keith* met more squarely the issue of warrantless electronic surveillance in the context of foreign intelligence gathering. In *United States v. Brown*,[4164] while affirming Brown's conviction for a firearm violation, the Fifth Circuit upheld the legality of a warrantless wiretap authorized by the Attorney General for foreign intelligence purposes where the conversation of *Brown*, an American citizen, was incidentally overheard.[4165] The Third Circuit, in *United States v. Butenko*,[4166] in affirming the district court's denial of an espionage defendant's application for disclosure of wiretap records, concluded that warrantless electronic surveillance was lawful, violating neither Section 605 of the Communications Act[4167] nor the Fourth Amendment, if its primary purpose was to gather foreign intelligence information.[4168]

The Ninth Circuit, in *United States v. Buck*,[4169] affirmed the conviction of a defendant found guilty of furnishing false information in connection with the

---

protection. . . . It may be that Congress, for example, would judge that the application and affidavit showing probable cause need not follow the exact requirements of § 2518 but should allege other circumstances more appropriate to domestic security cases; that the request for prior court authorization could, in sensitive cases, be made to any member of a specially designated court . . .; and that the time and reporting requirements need not be so strict as those in § 2518. The above paragraph does not, of course, attempt to guide the congressional judgment but rather to delineate the present scope of our own opinion. We do not attempt to detail the precise standards for domestic security warrants any more than our decision in Katz sought to set the refined requirements for the specified criminal surveillances which now constitute Title III. We do hold, however, that prior judicial approval is required for the type of domestic surveillance involved in this case and that such approval may be made in accordance with such reasonable standards as the Congress may prescribe.

407 U.S. at 323-24 (emphasis added). Some of the structural elements mentioned here appear to foreshadow the structure Congress chose to establish for electronic surveillance to gather foreign intelligence information in FISA.

[4164] 484 F.2d 418 (5th Cir. 1973), cert. denied, 415 U.S. 960 (1974).

[4165] Id. at 426.

[4166] 494 F.2d 593 (3rd Cir. 1974), cert. denied sub nom. Ivanov v. United States, 419 U.S. 881 (1974).

[4167] Pub. L. 73-416, Title VII, § 705, formerly Title VI, § 605, 48 Stat. 1103, codified as amended at 47 U.S.C. § 605 (providing that except as authorized in Title III, "no person not being authorized by the sender shall intercept any communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communication to any person").

[4168] 494 F.2d at 602, 604, and 608. However, it would be unlawful if the interception were conducted on a domestic group for law enforcement purposes. Id. at 606.

[4169] 548 F.2d 871 (9 Cir. 1977), cert. denied, 439 U.S. 890 (1977).

acquisition of ammunition and making a false statement with respect to information required to be kept by a licensed firearm dealer. In responding to Buck's contention on appeal that it was reversible error for the district court to fail to articulate the test it applied in ruling, after an in camera inspection, that the contents of one wiretap did not have to be disclosed to the appellant because it was expressly authorized by the Attorney General and lawful for purposes of gathering foreign intelligence, the Ninth Circuit stated that "[f]oreign security wiretaps" were "a recognized exception to the general warrant requirement and disclosure of wiretaps not involving illegal surveillance was within the trial court's discretion." The court found a determination that the surveillance was reasonable was implicit in the lower court's conclusion.[4170]

In its plurality decision in *Zweibon v. Mitchell*,[4171] a case involving a suit for damages brought by 16 members of the Jewish Defense League against Attorney General John Mitchell and nine FBI special agents and employees for electronic surveillance of their telephone calls without a warrant, the District of Columbia Circuit took a somewhat different view. The surveillance was authorized by the President, acting through the Attorney General, as an exercise of his authority relating to the nation's foreign affairs and was asserted to be essential to protect the nation and its citizens against hostile acts of a foreign power and to obtain foreign intelligence information deemed essential to the security of the United States. The D.C. Circuit, in a plurality decision, held that a warrant was constitutionally required in such a case involving a wiretap of a domestic organization that was not an agent of a foreign power or working in collaboration with a foreign power posing a national security threat.[4172] The court further held that the appellants were entitled to the liquidated damages recovery provided in Title III unless appellees on remand establish an affirmative defense of good faith.[4173] While its holding was limited to the facts before it, the plurality also noted that "an analysis of the policies implicated by foreign security surveillance indicates that, absent exigent circumstances, all warrantless electronic surveillance is unreasonable and therefore unconstitutional."[4174]

[4170] Id. at 875-76.

[4171] 516 F.2d 594 (D.C. Cir. 1975), cert. denied, 425 U.S. 944 (1976).

[4172] 516 F.2d at 650-55.

[4173] Id. at 659-73.

[4174] Id. at 613-14. In the context of the its broad dictum, the court did not clarify what "exigent circumstances" might entail. The court explained its understanding of the distinction between "domestic" and "foreign" as follows:

Throughout this opinion, "internal security" and "domestic security" will refer to threats to the structure or existence of the Government which originate directly from domestic organizations which are neither agents of nor acting in collaboration with foreign powers, and "internal

Surveillance for Foreign Intelligence Purposes

The Foreign Intelligence Surveillance Act of 1978 (FISA)[4175] sought to strike a balance between national security interests and civil liberties. The legislation was a response both to the Senate Select Committee to Study Government Operations with Respect to Intelligence Activities (hereinafter the Church Committee) revelations of past abuses of electronic surveillance for national security purposes and to the somewhat uncertain state of the law on the issue. The Church Committee found that every President since Franklin D. Roosevelt had both asserted the authority to authorize warrantless electronic surveillance and had utilized that authority.[4176] Concerns over abuses of such authority provided impetus to the passage of the legislation. As the Senate Judiciary Committee noted in its statement of the need for legislation:

The need for such statutory safeguards has become apparent in recent years. This legislation is in large measure a response to the revelations that warrantless electronic surveillance in the name of national security has been seriously abused. . . . While the number of illegal or improper national security taps and bugs conducted during the Nixon administration may have exceeded those in previous administrations, the surveillances were regrettably by no means atypical. In summarizing its conclusion that surveillance was "often conducted by illegal or improper means," the Church committee wrote:

---

security" or "domestic security" surveillance will refer to surveillance which is predicated on such threats. "Foreign security" will refer to threats to the structure or existence of the Government which emanate either directly or indirectly from a foreign power, and a "foreign security" surveillance will refer to surveillance which is predicated on such threats. A surveillance is a foreign security surveillance regardless of the stimulus that provoked the foreign power; thus the surveillance in this case will be treated as a foreign security surveillance even though the Soviet threats were provoked by actions of a hostile domestic organization. We believe such treatment is required by the limited holding of the Supreme Court in Keith. "National security" will generally be used interchangeably with "foreign security," except where the context makes it clear that it refers to both "foreign security" and "internal security."

Id. at 614 n.42 (internal citations omitted).

[4175] Pub. L. 95-511, Title I, 92 Stat. 1796 (Oct. 25, 1978), codified as amended at 50 U.S.C. §§ 1801 et seq.

[4176] See S.REP.NO. 95-604(I), at 7, 1978U.S.C.C.A.N. 3904, 3908. The Senate Judiciary Committee report's "Background" section traces in some detail the history of Executive Branch wiretap practice from the 1930's (after the Supreme Court in Olmstead held that the Fourth Amendment did not apply to "intangible" conversations and therefore no warrant was necessary) to the time of the consideration of FISA. See id. at 9-15, 1978 U.S.C.C.A.N. at 3911-16. Olmstead was overruled by Katz, see supra note 30 and accompanying text. The report of the House Permanent Select Committee on Intelligence, in its "Background" section, also provides a detailed recitation on the subject in H. REP. NO. 95-1283 at 15-21.

> *Since the 1930's, intelligence agencies have frequently wiretapped and bugged American citizens without the benefit of judicial warrant . . . . . past subjects of these surveillances have included a United States Congressman, Congressional staff member, journalists and newsmen, and numerous individuals and groups who engaged in no criminal activity and who posed no genuine threat to the national security, such as two White House domestic affairs advisers and an anti-Vietnam War protest group. (Vol. 2, p.12)*
>
> * * * *
>
> *The application of vague and elastic standards for wiretapping and bugging has resulted in electronic surveillances which, by any objective measure, were improper and seriously infringed the Fourth Amendment rights of both the targets and those with whom the targets communicated. The inherently intrusive nature of electronic surveillance, moreover, has enabled the Government to generate vast amounts of information — unrelated to any legitimate government interest — about the personal and political lives of American citizens. The collection of this type of information has, in turn, raised the danger of its use for partisan political and other improper ends by senior administration officials. (Vol. 3, p. 32.)*[4177]

The Senate Judiciary Committee also focused on the potentially chilling effect of warrantless electronic surveillance upon the exercise of First Amendment rights:

> *Also formidable — although incalculable — is the "chilling effect" which warrantless electronic surveillance may have on the constitutional rights of those who were not targets of the surveillance, but who perceived themselves, whether reasonably or unreasonably, as potential targets. Our Bill of Rights is concerned not only with direct infringements on constitutional rights, but also with government activities which effectively inhibit the exercise of these rights. The exercise of political freedom depends in large measure on citizens' understanding that they will be able to be publicly active and dissent from official policy, within lawful limits, without having to sacrifice the expectation of privacy that they rightfully hold. Arbitrary or uncontrolled use of warrantless electronic surveillance can violate that understanding and impair*

[4177] Id. at 7-8, 1978 U.S.C.C.A.N. at 3909.

> *that public confidence so necessary to an uninhibited political life.*[4178]

The Senate Judiciary Committee stated that the bill was "designed . . . to curb the practice by which the Executive Branch may conduct warrantless electronic surveillance on its own unilateral determination that national security justifies it," while permitting the legitimate use of electronic surveillance to obtain foreign intelligence information. Echoing the Church Committee, the Senate Judiciary Committee recognized that electronic surveillance has enabled intelligence agencies to obtain valuable and vital information relevant to their legitimate intelligence missions which would have been difficult to acquire by other means.[4179]

Electronic Surveillance: The Current Statutory Framework

The interception of wire, oral, or electronic communications[4180] is regulated by Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("Title III"), as amended.[4181] Government surveillance for criminal law enforcement is permitted under certain circumstances and in accordance with the procedures set forth in Title III. Government surveillance for the gathering of foreign intelligence information is covered by FISA. These statutes are relevant to the analysis of the legality of the reported NSA surveillance to the extent that their provisions are meant to cover such surveillance, prohibit it, or explicitly exempt it from requirements therein. If Congress meant for FISA to occupy the entire field of electronic surveillance of the type that is being conducted pursuant to the President's executive order, then the operation may fall under the third tier of Justice Jackson's formula, in which the President's "power is at its lowest ebb" and a court could sustain it only by "disabling the Congress from acting upon the subject."[4182] In other words, if FISA, together with Title III, were found to occupy the field, then for a court to sustain the President's authorization of electronic surveillance to acquire foreign intelligence information outside the FISA framework, FISA would have to be considered an unconstitutional encroachment

---

[4178] Id. at 8, 1978 U.S.C.C.A.N. at 3909-10.

[4179] Id. at 8-9, 1978 U.S.C.C.A.N. at 3910.

[4180] For definitions of "wire communications," "oral communications," and "electronic communications," see 18 U.S.C. § 2510(1), (2), and (12). The latter includes, with certain exceptions, the transfer of any signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by wire, radio, electromagnetic, photoelectronic or photooptical system affecting interstate or foreign commerce.

[4181] Pub. L. 90-351, 82 Stat. 211, codified as amended at 18 U.S.C. §§ 2510 et seq.

[4182] Youngstown Sheet and Tube Co. v. Sawyer, 343 U.S. 579, 637-38 (1952) (Jackson, J., concurring). See supra notes 10 et seq., and accompanying text.

on inherent presidential authority. If, on the other hand, FISA leaves room for the NSA surveillance outside its strictures, then the claimed power might fall into the first or second categories, as either condoned by Congress (expressly or implicitly), or simply left untouched.

Title III

Title III provides the means for the Attorney General and designated assistants to seek a court order authorizing a wiretap or similar electronic surveillance to investigate certain crimes (18 U.S.C. § 2516). Most other interceptions of electronic communications are prohibited unless the activity falls under an explicit exception. Under 18 U.S.C. § 2511, any person who "intentionally intercepts . . . any wire, oral, or electronic communication" or "intentionally uses . . . any electronic, mechanical, or other device [that transmits a signal over wire or radio frequencies, or is connected with interstate or foreign commerce] to intercept any oral communication," without the consent of at least one party to the conversation, is subject to punishment or liability for civil damages. The statute also prohibits the intentional disclosure of the contents of an intercepted communication. It prohibits attempts to engage in the prohibited conduct as well as solicitation of other persons to carry out such activity.

Certain exceptions in Title III apply to federal employees and other persons "acting under color of law,"[4183] including exceptions for foreign intelligence acquisition. Section 2511 excepts officers, employees, and agents of the United States who, in the normal course of their official duty, conduct electronic surveillance pursuant to FISA (18 U.S.C. § 2511(2)(e)). Furthermore, Congress emphasized in § 1511(2)(f) that

> *Nothing contained in [chapters 119 (Title III), 121 (stored wire or electronic surveillance or access to transactional records) or 206 (pen registers and trap and trace devices) of title 18, U.S. Code], or section 705 of the Communications Act of 1934,[4184] shall be deemed to affect the acquisition by the United States Government of foreign intelligence information from international or foreign communications, or foreign intelligence activities conducted in*

[4183] Title III also contains some exceptions for private parties, including communications service providers with respect to activity incident to the provision of such service (§ 2511(2)(a)), and for activity related to equipment maintenance and repair, prevention of fraud or unauthorized access, and protection from unlawful interference (§ 2511(2)(g)-(h)). Listening to broadcasts and electronic communications that are available to the general public and not encrypted, such as police band radio, is not prohibited (§ 2511(2)(g)).

[4184] 47 U.S.C. § 605 ("[N]o person receiving, assisting in receiving, transmitting, or assisting in transmitting, any interstate or foreign communication by wire or radio shall divulge or publish the existence, contents, substance, purport, effect, or meaning thereof, except through authorized channels of transmission or reception. . . .").

> *accordance with otherwise applicable Federal law involving a foreign electronic communications system, utilizing a means other than electronic surveillance as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, and procedures in this chapter [119] or chapter 121 and the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which electronic surveillance, as defined in section 101 of such Act, and the interception of domestic wire, oral, and electronic communications may be conducted.*[4185]

Title III does not define "international or foreign communications" or "domestic." It is unclear under the language of this section whether communications that originate outside the United States but are received within U.S. territory, or vice versa, were intended to be treated as foreign, international or domestic. Recourse to the plain meaning of the words provides some illumination. Webster's New Collegiate Dictionary (1977), in pertinent part, defines "international" to mean "affecting or involving two or more nations" or "of or relating to one whose activities extend across national boundaries." Therefore, "international communications" might be viewed as referring to communications which extend across national boundaries or which involve two or more nations. "Foreign" is defined therein, in pertinent part, as "situated outside a place or country; esp situated outside one's own country." Thus, "foreign communications" might be interpreted as referring to communications taking place wholly outside the United States. "Domestic" is defined, in pertinent part, in Webster's to mean "of, relating to, or carried on within one and esp. one's own country." Therefore, "domestic communications" may be defined as communications carried on within the United States.

[4185] 18 U.S.C. § 2511(2)(f), added by the Foreign Intelligence Surveillance Act of 1978 (FISA), § 201(b), Pub. L. 95-511, 92 Stat. 1783. Prior to this amendment, the section read:

> Nothing contained in this chapter, or section 605 [now 705] of the Communications Act of 1934, shall be deemed to affect the acquisition by the United States Government of foreign intelligence information from international or foreign communications by means other than electronic surveillance as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, and procedures in this chapter and the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which electronic surveillance, as defined in section 101 of such Act, and the interception of wire and oral communications may be conducted.

The Electronic Communications Privacy Act, Pub. L. 99-508, § 101(c)(1)(A), substituted "wire, oral, or electronic communication" for "wire or oral communications." Pub. L. 99-508, § 101(b)(3), added the references to "chapter 121," which deals with stored wire and electronic communications and access to transactional records. That subsection also substituted "foreign communications, or foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic communications system, utilizing a means" for "foreign communications by a means."

The phrase "utilizing a means other than electronic surveillance [under FISA]" could be interpreted as modifying only the clause immediately before it or as modifying the previous clause as well. If it is read not to pertain to the clause regarding acquisition of intelligence from foreign or international communications, then Title III and the other named statutes would not affect the interception of foreign and international communications, whether they are acquired through electronic surveillance within the meaning of FISA or through other means. The legislative history does not support such a reading, however, for two reasons. First, the second clause, relating to intelligence activities involving foreign electronic communications systems,[4186] was inserted into the law in 1986 between the first clause and the modifying phrase.[4187] It is thus clear that the modifier initially applied to the first clause, and nothing in the legislative history suggests that Congress intended to effect such a radical change as exempting any electronic surveillance involving communications covered by FISA from the procedures required therein. Second, this conclusion is bolstered by the last sentence of the subsection, which specifies that the methods authorized in FISA and the other statutes are to be the exclusive methods by which the federal government is authorized to intercept electronic communications. Whether given communications are covered by the exclusivity language would require an examination of the definitions of covered communications in Title III and in FISA.[4188]

As originally enacted, § 2511 contained what appeared to be a much broader exception for national security intercepts. It excluded from the coverage of Title III surveillance carried out pursuant to the "constitutional power of the President to take such measures as he deems necessary to protect the Nation against actual

---

[4186] The statute does not explain whether "involving a foreign electronic communications system" encompasses only communications that are transmitted and received without ever traversing U.S. wires, cables, or broadcasting equipment, or whether a communication carried primarily by a U.S. carrier that is at any point routed through a non-U.S. communication system "involves" the foreign system. Either way, the interception would have to be carried out pursuant to "otherwise applicable Federal law."

According to the Senate Judiciary Committee, the language was meant

to clarify that nothing in chapter 119 as amended or in proposed chapter 121 affects existing legal authority for U.S. Government foreign intelligence activities involving foreign electronic communications systems. The provision neither enhances nor diminishes existing authority for such activities; it simply preserves the status quo. It does not provide authority for the conduct of any intelligence activity.

S. REP. NO. 99-541, at 18 (1986). "Proposed chapter 121" refers to FISA.

[4187] Electronic Communications Privacy Act of 1986 § 101(b)(3), Pub. L. 99-508, 100 Stat. 1848 (1986).

[4188] See infra section defining "electronic surveillance."

or potential attack . . ., [and] to obtain foreign intelligence information deemed essential to the security of the United States. . . .[4189] Congress repealed this language when it enacted FISA, and inserted § 2511(2)(f), supra, to make the requirements of Title III or FISA the exclusive means to authorize electronic surveillance within the United States, and to "put[] to rest the notion that Congress recognizes an inherent Presidential power to conduct such surveillances in the United States outside of the procedures contained in chapters 119 and 120 [of title 18, U.S. Code]."[4190] Subsection (2)(f) was intended to clarify that the prohibition does not cover NSA operations (as they were then being conducted) and other surveillance overseas, including that which targets U.S. persons.[4191]

FISA

The Foreign Intelligence Surveillance Act (FISA) provides a framework for the use of "electronic surveillance," as defined in the Act,[4192] and other investigative

---

[4189] 82 Stat. 214, formerly codified at 18 U.S.C. § 2511(3). The Supreme Court interpreted this provision not as a conferral or recognition of executive authority, but rather, as an indication that Congress had "left presidential powers where it found them." United States v. United States District Court, 407 U.S. 297, 303 (1972). The Senate Judiciary Committee noted, however, that the "highly controversial disclaimer has often been cited as evidence of a congressional ratification of the president's inherent constitutional power to engage in electronic surveillance in order to obtain foreign intelligence information essential to the national security." S. REP. NO. 95-604(I), at 6-7 (1978).

[4190] S.REP.NO. 95-604(I), at 64 (1978). Further, the Committee stated, "[a]s to methods of acquisition which come within the definition of 'electronic surveillance' in this bill, the Congress has declared that this statute, not any claimed presidential power, controls." Id. (emphasis added). The reference to chapter 120 of Title 18, U.S.C., in the report language quoted in the text above is to the foreign intelligence provisions in S. 1566, which became FISA. The Senate version of the measure would have included the foreign intelligence surveillance provisions as a new chapter 120 of Title 18, U.S. Code.

[4191] The Senate Judiciary Committee explained that the provision was designed "to make clear the legislation does not deal with international signals intelligence activities as currently engaged in by the National Security Agency and electronic surveillance conducted outside the United States." S. REP. NO. 95-604(I), at 64 (1978). The Senate Select Committee on Intelligence echoed this understanding. S. REP. NO. 95-701, at 71 (1978). While legislation then pending that would have regulated these types of operations was not enacted (S. 2525, 95th Cong.), Congress established oversight over such intelligence activities through a review of relevant executive branch procedures and regulations by the House and Senate Intelligence Committees. See S. REP. NO. 99-541, at 18 (1986) ("As in the past, the Senate expects that any relevant changes in these procedures and regulations will be provided to the Senate and House Intelligence Committees prior to their taking effect."). The President is also required to report "illegal intelligence activity" to the intelligence committees, 50 U.S.C. § 413(b). "Illegal intelligence activity" is undefined, but legislative history suggests it includes activities that violate the Constitution, statutes, or Executive orders. See S. REP. NO. 102-85, at 31 (1991) (explaining that the definition of "illegal intelligence activity" was not changed from the previous version of § 413).

[4192] See discussion of the scope of "electronic surveillance" under FISA in the next section of this memorandum, infra.

methods[4193] to acquire foreign intelligence information.[4194] In pertinent part, FISA provides a means by which the government can obtain approval to conduct electronic surveillance of a foreign power or its agents without first meeting the more stringent standard in Title III that applies to criminal investigations. While Title III requires a showing of probable cause that a proposed target has committed, is committing, or is about to commit a crime, FISA requires a showing of probable cause to believe that the target is a foreign power or an agent of a foreign power.

In the aftermath of the September 11, 2001, terrorist attacks on the United States, Congress amended FISA so that it no longer requires a certification that the (primary) purpose of a search or surveillance is to gather foreign intelligence information.[4195] As amended by the USA PATRIOT Act,[4196] FISA requires that a

---

[4193] FISA also authorizes the use for foreign intelligence purposes of physical searches, 50 U.S.C. § 1821 et seq.; pen registers and trap and trace devices, 50 U.S.C. § 1842 et seq.; and orders for production of business records or any tangible thing "for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution."

[4194] "Foreign intelligence information" is defined in FISA, 50 U.S.C. § 1801(e), to mean:

(1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against —

(A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

(B) sabotage or international terrorism by a foreign power or an agent of a foreign power; or

(C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or

(2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to —

(A) the national defense or the security of the United States; or

(B) the conduct of the foreign affairs of the United States.

[4195] See CRS Report RL30465, The Foreign Intelligence Surveillance Act: An Overview of the Statutory Framework for Electronic Surveillance. "Foreign intelligence information" is defined in 50 U.S.C. § 1801(e) to mean:

(1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against —

"significant purpose" of the investigation be the collection of foreign intelligence information, which has been interpreted to expand the types of investigations that may be permitted to include those in which the primary purpose may be to investigate criminal activity, as long as there is at least a measurable purpose related to foreign intelligence gathering.[4197] Congress later enacted a measure that removed, for a time,[4198] the requirement for the government to show that the intended target, if a non-U.S. person, is associated with a foreign power.[4199]

Electronic Surveillance Under FISA

Whether FISA applies to the electronic surveillances at issue turns in large part on the definition of "electronic surveillance" under FISA. To constitute "electronic surveillance" under FISA, the surveillance must fall within one of four categories set forth in 50 U.S.C. § 1801(f), FISA. These include:

> *(1) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular,*

(A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

(B) sabotage or international terrorism by a foreign power or an agent of a foreign power; or

(C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or

(2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to —

(A) the national defense or the security of the United States; or

(B) the conduct of the foreign affairs of the United States.

[4196] P.L. 107-56 § 218.

[4197] See In re Sealed Case, 310 F.3d 717, 735 (U.S. Foreign Intell. Surveillance Ct. Rev. 2002) ("The addition of the word 'significant' to section 1804(a)(7)(B) imposed a requirement that the government have a measurable foreign intelligence purpose, other than just criminal prosecution of even foreign intelligence crimes.").

[4198] This amendment, added by section 6001 of the Intelligence Reform and Terrorism Prevention Act, Pub. L. 108-458, 118 Stat. 3742 (2004), is subject to the sunset provision of the USA PATRIOT Act. See CRS Report RL32186, USA PATRIOT Act Sunset: Provisions That Expire on December 31, 2005, by Charles Doyle.

[4199] See CRS Report RS22011, Intelligence Reform and Terrorism Prevention Act of 2004: 'Lone Wolf' Amendment to the Foreign Intelligence Surveillance Act, by Elizabeth B. Bazan.

known United States person[4200] who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes;

(2) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States, but does not include the acquisition of those communications of computer trespassers that would be permissible under section 2511(2)(i) of Title 18;

(3) the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States; or

(4) the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.[4201]

[4200] "United States person" is defined in 50 U.S.C. § 1801(i) to mean:

(i) "United States person" means a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 1101(a)(20) of Title 8), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in subsection (a)(1), (2), or (3) of this section.

Under the definition of "foreign power" in 50 U.S.C. § 1801(a), the foreign powers defined in subsections 1801(a)(1), (2), or (3) are either foreign governments or components thereof, factions of a foreign nation or foreign nations which are not substantially composed of U.S. persons, or entities openly acknowledged by a foreign government or governments to be directed and controlled by that government or those governments. These three subsections of the "foreign power" definition do not include international terrorist organizations. See infra note 87 for the full definition of "foreign power" under 50 U.S.C. § 1801(a).

[4201] With respect to the ability of FISA to keep pace with the rapidly changing level of communications technology, it is possible that 50 U.S.C. § 1801(f)(3) and (4) may provide some or all of the needed statutory flexibility. See, e.g., S. REP. NO. 95-604(I) at 34-35, 1978 U.S.C.C.A.N. at 3936, discussing the congressional intent that subsection 1801(f)(4) was intended to be "broadly inclusive, because the effect of including a particular means of surveillance is not to prohibit it but to subject it to judicial oversight." Thus, it was intended to include "the installation of beepers and 'transponders,' if a warrant would be required in the ordinary criminal context. . . .

The legislative history of the Act suggests that some electronic surveillance by the National Security Agency involving communications taking place entirely overseas, even involving U.S. persons, was not intended to be covered.[4202] At the same time, FISA was clearly meant to cover some communications even if one party to the communication is overseas. The interception of wire or radio communications sent by or intended to be received by a targeted United States person[4203] in the United States is covered under 50 U.S.C. § 1801(f)(1). The

---

It could also include miniaturized television cameras and other sophisticated devices not aimed merely at communications." Id. See United States v. Andonian, 735 F. Supp. 1469, 1473 (C.D. Cal. 1990), aff'd and remanded on other grounds, 29 F.3d 634 (9th Cir. 1994), cert. denied, 513 U.S. 1128 (1995).

[4202] For example, in discussing the definition of "electronic surveillance," in H.R. 7308, the House Permanent Select Committee on Intelligence stated,

Therefore, this bill does not afford protections to U.S. persons who are abroad, nor does it regulate the acquisition of the contents of international communications of U.S. persons who are in the United States, where the contents are acquired unintentionally. The committee does not believe that this bill is the appropriate vehicle for addressing this area. The standards and procedures for overseas surveillance may have to be different than those provided in this bill for electronic surveillance within the United States or targeted against U.S. persons who are in the United States.

The fact that this bill does not bring the overseas surveillance and activities of the U.S. intelligence community within its purview, however, should not be viewed as congressional authorization of such activities as they affect the privacy interests of Americans. The committee merely recognizes at this point that such overseas surveillance activities are not covered by this bill. In any case, the requirements of the fourth amendment would, of course, continue to apply to this type of communications intelligence activity.

H. REP.NO.95-1283(I), at 50-51 (June 5, 1978). The House passedH.R.7308, amended (Roll No. 737), 124 Cong. Rec. 28427 (Sept. 7, 1978). Then the House passed S. 1566, having stricken all but the enacting clause of S. 1566 and having inserted in lieu thereof the text of S. 7308. H.R. 7308 was laid on the table, 124 Cong. Rec. 28427-28432 (Sept. 7, 1978).

[4203] The House Permanent Select Committee on Intelligence described the import of "intentionally

targeting" in the context of subsection (1) of the definition of "electronic surveillance" as follows:

Paragraph (1) protects U.S. persons who are located in the United States from being targeted in their domestic or international communications without a court order no matter where the surveillance is being carried out. The paragraph covers the acquisition of the contents of a wire or radio communication of a U.S. person by intentionally targeting that particular, known U.S. person, provided that the person is located within the United States. Thus, for example, any watchlisting activities of the National Security Agency conducted in the future, directed against the international communications of particular U.S. persons who are in the United States, would require a court order under this provision.

Only acquisition of the contents of those wire or radio communications made with a reasonable expectation of privacy where a warrant would be required for law enforcement purposes is

---

interception of international wire[4204] communications to or from any person (whether or not a U.S. person) within the United States without the consent of at least one party is covered under § 1801(f)(2), where the communications are acquired within the United States. The interception of a radio communication is covered under § 1801(f)(3) if all parties to it are located within the United States, unless there is no reasonable expectation of privacy and a warrant would not be required under Title III, even if the interception is acquired by using a device located outside of the United States. The interception of wire, oral, or electronic communications that is not included within the definition of "electronic surveillance" for the purposes of FISA may nevertheless be prohibited by or subject to a warrant requirement pursuant to 18 U.S.C. § 2511 (Title III).

In discussing the repeal in the conforming amendments to FISA of the "national security disclaimer" in former 18 U.S.C. § 2511(3), and the addition of 18 U.S.C. § 2511(f) in the conforming amendments in S. 1566, the Senate Judiciary Committee observed:

> *Specifically, this provision is designed to make clear that the legislation does not deal with international signals intelligence activities as currently engaged in by the National Security Agency[4205] and electronic surveillance conducted outside the*

---

covered by paragraph (1). It is the committee's intent that acquisition of the contents of a wire communication, without the consent of any party thereto, would clearly be included.

The term "intentionally targeting" a particular, known U.S. person who is in the United States includes the deliberate use of a surveillance device to monitor a specific channel of communication which would not be surveilled but for the purpose of acquiring information about a party who is a particular, named U.S. person located within the United States. It also includes the deliberate use of surveillance techniques which can monitor numerous channels of communication among numerous parties, where the techniques are designed to select out from among those communications the communications to which a particular U.S. person located in the United States is a party, and where the communications are selected either by name or by other information which would identify the particular person and would select out his communications.

This paragraph does not apply to the acquisition of the contents of international or foreign communications, where the contents are not acquired by intentionally targeting a particular known U.S. person who is in the United States. . . .

H. REP. NO. 95-1283(I), at 50-51 (June 8, 1978) (emphasis in original).

[4204] "Wire communication" means "any communication while it is being carried by a wire, cable, or other like connection furnished or operated by any person engaged as a common carrier in providing or operating such facilities for the transmission of interstate or foreign communications." 50 U.S.C. § 1801(l).

[4205] The legislative history of FISA reflects serious concerns about the past NSA abuses reflected in the Church Committee reports. See, e.g., SUPPLEMENTARY DETAILED STAFF REPORTS ON INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS,BOOK III,FINAL REPORT

> *United States. As to methods of acquisition which come within the definition of 'electronic surveillance' in this bill, the Congress has declared that this statute, not any claimed presidential power, controls.*[4206]

At the same time, the Committee signaled its intent to reserve its option to regulate U.S. electronic surveillance operations that did not fall within the ambit of FISA:

OF THE SELECT COMMITTEE TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, UNITED STATES SENATE, S. REP.NO. 94-755, 94 Cong., 2d Sess., at 733-86 (1976), cited in S. REP. NO. 95-604(I) at 34 n. 39, 1978 U.S.C.C.A.N. at 3936. Some actions had been taken to address some of these concerns by the President and the Attorney General near the time that FISA was being considered. The decision not to cover NSA activities "as they were then being conducted" in FISA may, in part, have been an acknowledgment of constraints that had been imposed upon some of these practices in E.O. 11905 (Feb. 18, 1976), cited in S. REP. NO. 95-604(I) at 34 n. 40, 1978 U.S.C.C.A.N. at 3936; and in the "substantial safeguards [then] currently embodied in classified Attorney General procedures, " H. REP. NO. 95-1283 at 21. In addition, S. 2525 (95th Cong.) was then pending, which, had it passed, would have addressed those areas excluded from FISA in separate legislation. The House Permanent Select Committee also noted the value of congressional oversight in adding an additional safeguard. Nevertheless, the Committee deemed these protections insufficient without the statutory structure in FISA:

In the past several years, abuses of domestic national security surveillances have been disclosed. This evidence alone should demonstrate the inappropriateness of relying solely on executive branch discretion to safeguard civil liberties. This committee is well aware of the substantial safeguards respecting foreign intelligence electronic surveillance currently embodied in classified Attorney General procedures, but this committee is also aware that over the past thirty years there have been significant changes in internal executive branch procedures, ant there is ample precedent for later administrations or even the same administration loosening previous standards. Even the creation of intelligence oversight committee should not be considered a sufficient safeguard, for in overseeing classified procedures the committees respect their classification, and the result is that the standards for and limitations on foreign intelligence surveillances may be hidden from public view. In such a situation, the rest of the Congress and the American people need to be assured that the oversight is having its intended consequences– the safeguarding of civil liberties consistent with the needs of national security. While oversight can be, and the committee intends it to be, an important adjunct to control of intelligence activities, it cannot substitute for public laws, publicly debated and adopted, which specify under what circumstances and under what restrictions electronic surveillance for foreign intelligence purposes can be conducted.

Finally, the decision as to the standards governing when and how foreign intelligence electronic surveillance should be conducted is and should be a political decision, in the best sense of the term, because it involves the weighing of important public policy concerns–civil liberties and national security. Such a political decision is one properly made by the political branches of Government together, not adopted by one branch on its own and with no regard for the other. Under our Constitution legislation is the embodiment of just such political decisions.

H. REP. NO. 95-1283, at 21-22.

[4206] S. REP. NO. 95-604(I) at 62-65, 1978 U.S.C.C.A.N. at 3964-66. See also S. REP. NO. 95-701 at 71-72, 1978 U.S.C.C.A.N. at 4040-41.

> *The activities of the National Security Agency pose particularly difficult conceptual and technical problems which are not dealt with in this legislation. Although many on the committee are of the opinion that it is desirable to enact legislative safeguards for such activity, the committee adopts the view expressed by the attorney general during the hearings that enacting statutory controls to regulate the National Security Agency and the surveillance of Americans abroad raises problems best left to separate legislation. This language insures that certain electronic surveillance activities targeted against international communications for foreign intelligence purposes will not be prohibited absolutely during the interim period when these activities are not regulated by chapter 120 and charters for intelligence agencies and legislation regulating international electronic surveillance have not yet been developed.*[4207]

FISA Exceptions to Requirement for Court Order

Three current provisions of FISA provide for some measure of electronic surveillance without a court order to gather foreign intelligence information in specified circumstances, 50 U.S.C. §§ 1802 (electronic surveillance of certain foreign powers without a court order upon Attorney General certification);[4208]

[4207] Id.

[4208] 50 U.S.C. § 1802 provides:

(a)

(1) Notwithstanding any other law, the President, through the Attorney General, may authorize electronic surveillance without a court order under this subchapter to acquire foreign intelligence information for periods of up to one year if the Attorney General certifies in writing under oath that —

(A) the electronic surveillance is solely directed at —

(i) the acquisition of the contents of communications transmitted by means of communications used exclusively between or among foreign powers, as defined in section 1801(a)(1), (2), or (3) of this title; or

(ii) the acquisition of technical intelligence, other than the spoken communications of individuals, from property or premises under the open and exclusive control of a foreign power, as defined in section 1801(a)(1), (2), or (3) of this title;

(B) there is no substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person is a party; and

1805(f) (emergency authorization of electronic surveillance for up to 72 hours, while an order approving such surveillance is sought from a judge of the Foreign

---

(C) the proposed minimization procedures with respect to such surveillance meet the definition of minimization procedures under section 1801(h) of this title; and if the Attorney General reports such minimization procedures and any changes thereto to the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence at least thirty days prior to their effective date, unless the Attorney General determines immediate action is required and notifies the committees immediately of such minimization procedures and the reason for their becoming effective immediately.

(2) An electronic surveillance authorized by this subsection may be conducted only in accordance with the Attorney General's certification and the minimization procedures adopted by him. The Attorney General shall assess compliance with such procedures and shall report such assessments to the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence under the provisions of section 1808(a) of this title.

(3) The Attorney General shall immediately transmit under seal to the court established under section 1803(a) of this title a copy of his certification. Such certification shall be maintained under security measures established by the Chief Justice with the concurrence of the Attorney General, in consultation with the Director of National Intelligence, and shall remain sealed unless —

(A) an application for a court order with respect to the surveillance is made under sections 1801(h)(4) and 1804 of this title; or

(B) the certification is necessary to determine the legality of the surveillance under section 1806(f) of this title.

(4) With respect to electronic surveillance authorized by this subsection, the Attorney General may direct a specified communication common carrier to —

(A) furnish all information, facilities, or technical assistance necessary to accomplish the electronic surveillance in such a manner as will protect its secrecy and produce a minimum of interference with the services that such carrier is providing its customers; and

(B) maintain under security procedures approved by the Attorney General and the Director of National Intelligence any records concerning the surveillance or the aid furnished which such carrier wishes to retain.

The Government shall compensate, at the prevailing rate, such carrier for furnishing

such aid.

(b) Applications for a court order under this subchapter are authorized if the President has, by written authorization, empowered the Attorney General to approve applications to the court having jurisdiction under section 1803 of this title, and a judge to whom an application is made may, notwithstanding any other law, grant an order, in conformity with section 1805 of this title, approving electronic surveillance of a foreign power or an agent of a foreign power for the purpose of obtaining foreign intelligence information, except that the court shall not have jurisdiction to grant any order approving electronic surveillance directed solely as described in paragraph (1)(A) of subsection (a) of this section unless such surveillance may involve the acquisition of communications of any United States person.

Intelligence Surveillance Court (FISC));[4209] and 1811 (electronic surveillance without a court order for 15 days following a declaration of war by the Congress).

In particular, 50 U.S.C. § 1802 permits the Attorney General to order electronic surveillance without a court order for up to one year to acquire foreign intelligence information for periods of up to one year if the Attorney General certifies in writing under oath that the electronic surveillance is solely directed at means of communications used exclusively between or among foreign powers or on property or premises under the open and exclusive control of a foreign power (the definition here does not include international terrorist organizations)[4210]

[4209] The emergency authorization provision in 50 U.S.C. § 1805(f) states:

(f) Emergency orders

Notwithstanding any other provision of this subchapter, when the Attorney General reasonably determines that —

(1) an emergency situation exists with respect to the employment of electronic surveillance to obtain foreign intelligence information before an order authorizing such surveillance can with due diligence be obtained; and

(2) the factual basis for issuance of an order under this subchapter to approve such surveillance exists;

he may authorize the emergency employment of electronic surveillance if a judge having jurisdiction under section 1803 of this title is informed by the Attorney General or his designee at the time of such authorization that the decision has been made to employ emergency electronic surveillance and if an application in accordance with this subchapter is made to that judge as soon as practicable, but not more than 72 hours after the Attorney General authorizes such surveillance. If the Attorney General authorizes such emergency employment of electronic surveillance, he shall require that the minimization procedures required by this subchapter for the issuance of a judicial order be followed. In the absence of a judicial order approving such electronic surveillance, the surveillance shall terminate when the information sought is obtained, when the application for the order is denied, or after the expiration of 72 hours from the time of authorization by the Attorney General, whichever is earliest. In the event that such application for approval is denied, or in any other case where the electronic surveillance is terminated and no order is issued approving the surveillance, no information obtained or evidence derived from such surveillance shall be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof, and no information concerning any United States person acquired from such surveillance shall subsequently be used or disclosed in any other manner by Federal officers or employees without the consent of such person, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person. A denial of the application made under this subsection may be reviewed as provided in section 1803 of this title.

[4210] "Foreign power" for purposes of electronic surveillance under FISA is defined in 50 U.S.C. § 1801(a)(1) through (6) as:

where "there is no substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person is a party;" and minimization procedures are put in place.[4211] The Attorney General is also required to report minimization procedures to the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence 30 days in advance. The 30-day requirement can be waived if the Attorney General determines immediate action is required, in which case he is to notify the committees immediately of the minimization procedures and the reason for the urgency. The FISA court is to receive a copy of the certifications under seal.

The emergency authorization provision in 50 U.S.C. § 1805(f) authorizes the Attorney General to issue emergency orders to permit electronic surveillance prior to obtaining a court order if the Attorney General determines that emergency conditions make it impossible to obtain an order with due diligence before the surveillance is begun. The Attorney General or his designee must immediately inform a FISA judge and submit a proper application to that judge as soon as practicable, but not more than 72 hours[4212] after the Attorney General authorizes such surveillance. Minimization procedures must be followed. In the absence of a judicial order, the surveillance must terminate when the information sought is obtained, when the application for the order is denied, or after the expiration of 72 hours from the time the surveillance was authorized. No information obtained or evidence derived from such surveillance may be used as evidence or otherwise disclosed in any trial, hearing, or other government

---

(1) a foreign government or any component thereof, whether or not recognized by the United States;

(2) a faction of a foreign nation or nations, not substantially composed of United States persons;

(3) an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments;

(4) a group engaged in international terrorism or activities in preparation therefor;

(5) a foreign-based political organization, not substantially composed of United States persons; or

(6) an entity that is directed and controlled by a foreign government or governments.

However, for the purpose of § 1802, only subsections 1801(a)(1) through (3) are included.

[4211] "Minimization procedures" are specific procedures implemented with respect to a particular surveillance in order to minimize the acquisition and retention, and prohibit the dissemination, of information concerning unconsenting U.S. persons required to be protected. See 50 U.S.C. § 1801(h).

[4212] Section 314(a)(2)(B) of P.L. 107-108, the Intelligence Authorization Act for Fiscal Year 2002, 115 Stat. 1402 (Dec. 28, 2001), H.Rept. 107-328, replaced 24 hours with 72 hours in each place that it appears in 50 U.S.C. § 1805(f).

proceeding, and no information concerning any U.S. person may be disclosed at all without that person's consent except with the Attorney General's approval where the information indicates a threat of disaster or serious bodily harm to any person.

Where Congress has passed a declaration of war, 50 U.S.C. § 1811 authorizes the Attorney General to conduct electronic surveillance without a court order for fifteen calendar days following a declaration of war by Congress. This provision does not appear to apply to the AUMF, as that does not constitute a congressional declaration of war.[4213] Indeed, even if the authorization were regarded as a declaration of war, the authority to conduct warrantless electronic surveillance under 50 U.S.C. § 1811 would only extend to a maximum of 15 days following its passage.[4214]

The Administration's Position

The Administration's position, as set forth in the Office of Legislative Affairs letter to the leaders of the House and Senate intelligence Committees, is that the President has the constitutional authority to direct the NSA to conduct the activities he described, and that this inherent authority is supplemented by statutory authority under the AUMF.[4215] The Administration interprets the AUMF, based on its reading of the Supreme Court opinion in Hamdi,[4216] as authorizing the President to conduct anywhere in the world, including within the United States, any activity that can be characterized as a fundamental incident of waging war. It includes communications intelligence among the fundamental incidents of waging war. The following sections analyze the extent to which the President's authority to conduct warrantless electronic surveillance is inherent,

---

[4213] For a discussion of declarations of war and authorizations for the use of military force, see CRS Report for Congress RL31133, Declarations of War and Authorizations for the Use of Military Force: Historical Background and Legal Implications, by David M. Ackerman and Richard F. Grimmett.

[4214] This provision originated in the House version of the bill, which would have allowed the President to authorize electronic surveillance for periods up to a year during time of war declared by Congress. The conference substituted a compromise provision authorizing electronic surveillance without a court order to acquire foreign intelligence information for 15 days following a declaration of war. H.R. CONF. REP. NO. 95-1720, at 34 (1978). The 15-day period was intended to "allow time for consideration of any amendment to [FISA] that may be appropriate during a wartime emergency." Id. The conferees also expressed their intent that "all other provisions of this act not pertaining to the court order requirement shall remain in effect during this period." Id.

[4215] OLA Letter, supra note 10, at 2.

[4216] Hamdi v. Rumsfeld, 542 U.S. 507 (2004).

whether the AUMF authorizes the operations,[4217] and whether the NSA operations are consistent with FISA and Title III.[4218]

The President's Inherent Authority to Conduct Intelligence Surveillance

The statutory language in FISA and the legislative history of the bill that became FISA, S. 1566 (95th Cong.), reflect the Congress's stated intention to circumscribe any claim of inherent presidential authority to conduct electronic surveillance, as defined by the Act, to collect foreign intelligence information, so that FISA would be the exclusive mechanism for the conduct of such electronic surveillance. Thus, in the conforming amendments section of the legislation, the previous language explicitly recognizing the President's inherent authority was deleted from 18 U.S.C. § 2511(3), and the language of 18 U.S.C. § 2511(f) was added to Title III of the Omnibus Crime Control and Safe Streets Act of 1968, as amended, which states, in part, that "procedures in this chapter or chapter 121 and the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which electronic surveillance, as defined in section 101 of that Act, and the interception of domestic wire, oral, and electronic communications may be conducted."[4219] The House amendments to the bill provided that the procedures in the bill and in 18 U.S.C., Chapter 119 (Title III), were to be the exclusive "statutory" means by which electronic surveillance as defined in the bill and the interception of domestic wire and oral communications may be conducted, while the Senate bill did not include the word "statutory." The House Conference Report, in accepting the Senate approach, stated, in part, that

The conferees agree that the establishment by this act of exclusive means by which the President may conduct electronic surveillance does not foreclose a different decision by the Supreme Court. The intent of the conferees is to apply the standard set forth in Justice Jackson's concurring opinion in the Steel Seizure case: "When a President takes measures incompatible with the express or implied will of Congress, his power is at the lowest ebb, for then he can rely only upon his

---

[4217] See OLA Letter, supra note 10, at 3 ("Because communications intelligence activities constitute, to use the language of Hamdi, a fundamental incident of waging war, the AUMF clearly and unmistakably authorizes such activities directed against the communications of our enemy.").

[4218] We do not address the Administration's argument that the NSA electronic surveillance at issue is compatible with the Fourth Amendment. For analysis pertinent to that issue, see supra section on the Background of Government Surveillance.

[4219] For further discussion of the pertinent provisions of Title III, see the discussion at notes 54 et seq. and accompanying text.

own constitutional power minus any constitutional power of Congress over the matter." Youngstown Sheet and Tube Co. v. Sawyer, 343 U.S. 579, 637 (1952).[4220]

In this language, the conferees acknowledge that the U.S. Supreme Court, as the final arbiter of constitutional power, might reach a different conclusion. The Court has yet to rule on the matter.[4221]

[4220] H. CONF. REP. NO. 95-1720, at 35, 1978 U.S.C.C.A.N. at 4064 (Oct. 5, 1978); see also S. REP. NO. 95-604(I) at 62-65, 1978 U.S.C.C.A.N. at 3964-66; S. REP. NO. 95-701 at 71-72, 1978 U.S.C.C.A.N. at 4040-41.

[4221] However, some lower court decisions provide significant support for the argument that the exclusivity provision circumscribes the President's use of inherent authority to engage in electronic surveillance to collect foreign intelligence information outside the FISA structure. See, e.g., United States v. Andonian, 735 F. Supp. 1469 (C.D. Cal. 1990), aff'd and remanded on other grounds, 29 F.3d 634 (9th Cir. 1994), cert. denied, 513 U.S. 1128 (1995). The Andonian court found that the exclusivity language in FISA reveals that Congress intended to sew up the perceived loopholes through which the President had been able to avoid the warrant requirement. The exclusivity clause makes it impossible for the President to 'opt-out' of the legislative scheme by retreating to his 'inherent' Executive sovereignty over foreign affairs. At the time of the drafting of FISA, such a retreat would have meant completely unfettered use of electronic surveillance in the foreign affairs arena, as the Supreme Court had twice declined to hold such Executive action captive to the warrant requirement [citing Keith, 407 U.S. 297, Katz, 389 U.S. at 358, n. 23, and S. REP.NO. 95-604[(I)] at 12-14, 1978 U.S.C.C.A.N. at 3913-16]. . . . The exclusivity clause in 18 U.S.C. section 2511(2)(f) assures that the President cannot avoid Congress' limitations by resort to 'inherent' powers as had President Truman at the time of the 'Steel Seizure Case.' Youngstown Sheet and Tube v. Sawyer, 343 U.S. 579 (1952). . . . The difficulty in the case was due to Congressional silence. . . . When the President acts in absence of either a congressional grant or denial of authority, he can only rely upon his own independent powers, but there is a zone of twilight in which he and Congress may have concurrent authority, or in which its distribution is uncertain. Therefore, congressional inertia, indifference or acquiescence may sometimes, at least as a practical matter, enable, if not invite, measures on independent presidential responsibility. In this area, any actual test of power is likely to depend on the imperatives and events and contemporary imponderables rather than on abstract theories of law. . . . To foreclose the arguments which piqued the Court in Youngstown, Congress denied the President his inherent powers outright. Tethering executive reign, Congress deemed that the provisions for gathering intelligence in FISA and Title III were 'exclusive.'

Id. at 1474-76. Cf., United States v. Falvey, 540 F. Supp. 1306 (E.D.N.Y. 1982). The court stated that

FISA is the fifth legislative attempt since the Watergate era to bridle the Executive's 'inherent' power. Congress believes that FISA has provided a 'secure framework by which the Executive Branch may conduct legitimate electronic surveillance for foreign intelligence purposes within the context of this Nation's commitment to privacy and individual rights.' . . . The Act received broad support in Congress and from the then Attorney General Griffin Bell and President Carter. . . . When, therefore, the President has, as his primary purpose, the accumulation of foreign intelligence information, his exercise of Article II power to conduct foreign affairs is not constitutionally hamstrung by the need to obtain prior judicial approval before engaging in wiretapping. While the executive power to conduct foreign affairs exempts the President from the warrant requirement when foreign surveillance is conducted, the President is not entirely free of the constraints of the Fourth Amendment. The search and seizure resulting from the surveillance

The passage of FISA and the inclusion of such exclusivity language reflects Congress's view of its authority to cabin the President's use of any inherent constitutional authority with respect to warrantless electronic surveillance to gather foreign intelligence. The Senate Judiciary Committee articulated its view with respect to congressional power to tailor the President's use of an inherent constitutional power:

The basis for this legislation is the understanding — concurred in by the Attorney General — that even if the President has an "inherent" constitutional power to authorize warrantless surveillance for foreign intelligence purposes, Congress has the power to regulate the exercise of this authority by legislating a reasonable warrant procedure governing foreign intelligence surveillance.[4222]

On the other hand, the Administration asserts constitutional authority under Article II of the Constitution, including his Commander-in-Chief authority, to order warrantless foreign intelligence surveillance within the United States:

> *This constitutional authority to order warrantless foreign intelligence surveillance within the United States, as all federal appellate courts, including at least four circuits, to have addressed*

---

must still be reasonable. With the enactment of FISA, . . . Congress has fashioned a statute for foreign surveillance that fully comports with the Fourth Amendment.

Id. at 1311-12. See United States v. Bin Laden, 126 F. Supp. 2d 264 (S.D.N.Y. 2000). The court noted that

All of the circuit cases finding a foreign intelligence exception [to the warrant requirement] arose before the enactment of FISA (which sets forth procedures for foreign intelligence collection, see 50 U.S.C. § 1801 et seq.) and are probably now governed by that legislation. FISA only governs foreign intelligence searches conducted within the United States. See 50 U.S.C. §§ 1801(f)(1-4), 1803(a), 1821(5), 1822(c).

Id. at 272 n. 8.

[4222] S. REP. NO. 95-604(I), at 16, 1978 U.S.C.C.A.N. at 3917. See also Attorney General Bell's testimony with respect to the Administration's position, id. at 4, 1978 U.S.C.C.A.N. at 3905-06; S. REP. NO. 95-701, at 6-7, 1978 U.S.C.C.A.N. at 3975. The need to comply with FISA for the collection of foreign intelligence information through electronic surveillance is reiterated in E.O. 12333 ("United States Intelligence Activities" (December 4, 1981), as amended), Section 2.5, dealing with Attorney General approval required for certain collection techniques: 2.5 Attorney General Approval. The Attorney General hereby is delegated the power to approve the use for intelligence purposes, within the United States or against a United States person abroad, of any technique for which a warrant would be required if undertaken for law enforcement purposes, provided that such techniques shall not be undertaken unless the Attorney General has determined in each case that there is probable cause to believe that the technique is directed against a foreign power or an agent of a foreign power. Electronic surveillance, as defined in the Foreign Intelligence Surveillance Act of 1978, shall be conducted in accordance with that Act, as well as this Order.

> *the issue have concluded. See, e.g., In re Sealed Case, 310 F.3d 717, 742 (FISA Ct. of Review 2002) ("[A]ll the other courts to have decided the issue [have] held that the President did have inherent authority to conduct warrantless searches to obtain foreign intelligence information . . . . We take for granted that the President does have that authority . . . .").*[4223]

The U.S. Foreign Intelligence Surveillance Court of Review (Court of Review) was created by FISA, 50 U.S.C. § 1803, and has appellate review over denials of FISA applications by the Foreign Intelligence Surveillance Court which was also established under that section. Denials of such applications by the Court of Review may be appealed to the U.S. Supreme Court. The Court of Review has decided only one published case, which is cited by the Administration above. The case was not appealed to the U.S. Supreme Court. As the Court of Review is a court of appeals and is the highest court with express authority over FISA to address the issue, its reference to inherent constitutional authority for the President to conduct warrantless foreign intelligence surveillance might be interpreted to carry considerable weight.

The Court of Review, in its opinion, make two references which appear pertinent to the Administration's position. The first statement, which is cited by the Administration, was made by the Court of Review, in In re Sealed Case,[4224] in its discussion of the constitutionality of FISA and its exploration of the underlying rationale of the "primary purpose" test as articulated in United States v. Truong Dinh Hung,[4225] (which dealt with a pre-FISA surveillance). The Court of Review, in this portion of its constitutional analysis, was considering whether the primary purpose of a FISA electronic surveillance must be to gather foreign intelligence information in order for it to pass constitutional muster. Truong saw such a standard as a constitutional minimum. In assessing and rejecting the Truong approach, the Court of Review stated:

> *It will be recalled that the case that set forth the primary purpose test as constitutionally required was Truong. The Fourth Circuit thought that Keith's balancing standard implied the adoption of the primary purpose test. We reiterate that Truong dealt with a pre-FISA surveillance based on the President's constitutional responsibility to conduct the foreign affairs of the United States. 629 F.2d at 914. Although Truong suggested the line it drew was a constitutional minimum that would apply to a FISA surveillance, see id. at 914 n. 4, it had no occasion to consider the application of*

[4223] OLA Letter, supra note 10, at 2.

[4224] 310 F.3d 717 (U.S. Foreign Intell. Surveillance Ct. Rev. 2002).

[4225] 629 F.2d 908 (4th Cir. 1980).

> *the statute carefully. The Truong court, as did all the other courts to have decided the issue, held that the President did have inherent authority to conduct warrantless searches to obtain foreign intelligence information. It was incumbent upon the court, therefore, to determine the boundaries of that constitutional authority in the case before it. We take for granted that the President does have that authority, and, assuming that is so, FISA could not encroach on the President's constitutional power. The question before us is the reverse, does FISA amplify the President's power by providing a mechanism that at least approaches a classic warrant and which therefore supports the government's contention that FISA searches are constitutionally reasonable.*[4226]

While the Court of Review does not cite to the cases to which it is referring, its allusion to the holdings of "all the other courts to have considered the issue," appears to have been to cases which pre-date FISA's passage or which address pre-FISA surveillances.[4227] Such cases dealt with a presidential assertion of

---

[4226] 310 F.3d at 742 (emphasis added).

[4227] Id. at 742, n. 26; cf., United States v. Duggan, 743 F.2d 59, 71 (2d Cir. 1984) ("Prior to the enactment of FISA, virtually every court that had addressed the issue had concluded that the President had the inherent power to conduct warrantless electronic surveillance to collect foreign intelligence information, and that such surveillances constituted an exception to the warrant requirement of the Fourth Amendment. See United States v. Truong Dinh Hung, 629 F.2d 908, 912-14 (4th Cir.1980), cert. denied,454 U.S. 1144 (1982); United States v. Buck, 548 F.2d 871, 875 (9th Cir.), cert. denied, 434 U.S. 890 (1977); United States v. Butenko, 494 F.2d 593, 605 (3d Cir.) (en banc), cert. denied,419 U.S. 88 (1974); United States v. Brown, 484 F.2d 418, 426 (5th Cir. 1973), cert. denied, 415 U.S. 960 (1974). But see Zweibon v. Mitchell, 516 F.2d 594, 633-51 (D.C. Cir. 1975) (dictum), cert. denied, 425 U.S. 944 (1976). The Supreme Court specifically declined to address this issue in United States v. United States District Court, 407 U.S. 297, 308, 321-22 (1972) (hereinafter referred to as "Keith"), but it had made clear that the requirements of the Fourth Amendment may change when differing governmental interests are at stake, see Camara v. Municipal Court, 387 U.S. 523 (1967), and it observed in Keith that the governmental interests presented in national security investigations differ substantially from those presented in traditional criminal investigations. 407 U.S. at 321-24, 92 S.Ct. at 2138-40."); Truong Dinh Hung, 629 F.2d at 914 ("Perhaps most crucially, the executive branch not only has superior expertise in the area of foreign intelligence, it is also constitutionally designated as the pre-eminent authority in foreign affairs. See First National Bank v. Banco Nacional de Cuba, 406 U.S. 759, 765-68, 92 S.Ct. 1808, 1812-1814, 32 L.Ed.2d 466 (1972); Oetjen v. Central Leather Co., 246 U.S. 297, 302, 38 S.Ct. 309, 310, 62 L.Ed. 726 (1918). The President and his deputies are charged by the constitution with the conduct of the foreign policy of the United States in times of war and peace. See United States v. Curtiss-Wright Corp., 299 U.S. 304, 57 S.Ct. 216, 81 L.Ed. 255 (1936). Just as the separation of powers in Keith forced the executive to recognize a judicial role when the President conducts domestic security surveillance, 407 U.S. at 316-18, 92 S.Ct. at 2136-2137, so the separation of powers requires us to acknowledge the principal responsibility of the President for foreign affairs and concomitantly for foreign intelligence surveillance. In sum, because of the need of the executive branch for flexibility, its practical experience, and its constitutional competence, the courts should not require the executive to secure a warrant each time it conducts foreign intelligence surveillance. Accord, United States v. Butenko, 494 F.2d 593 (3 Cir.), cert.

inherent authority in the absence of congressional action to circumscribe that authority. Where the Congress has exercised its constitutional authority in the areas of foreign affairs and thereby has withdrawn electronic surveillance, as defined by FISA, from the "zone of twilight," between Executive and Legislative constitutional authorities, it might be argued that the President's asserted inherent authority to engage in warrantless electronic surveillance was thereby limited. In the wake of FISA's passage, the Court of Review's reliance on these pre-FISA cases or cases dealing with pre-FISA surveillances as a basis for its assumption of the continued vitality of the President's inherent constitutional authority to authorize warrantless electronic surveillance for the purpose of gathering foreign intelligence information might be viewed as somewhat undercutting the persuasive force of the Court of Review's statement.

The second reference to the "President's inherent constitutional authority" in *In re Sealed Case* is in the conclusion to the opinion. Here the Court of Review makes an oblique reference to the President's inherent authority:

> *Even without taking into account the President's inherent constitutional authority to conduct warrantless foreign intelligence surveillance, we think the procedures and government showings required under FISA, if they do not meet the minimum Fourth Amendment warrant standards, certainly come close. We, therefore, believe firmly, applying the balancing test drawn from Keith, that FISA as amended is constitutional because the surveillances it authorizes are reasonable.*[4228]

The latter statement was made in support of the Court of Review's conclusion that the procedures for electronic surveillance to gather foreign intelligence information under FISA, as amended by the USA PATRIOT Act, Pub. L. 107-56, were constitutionally sufficient under Fourth Amendment standards, whether the court orders under FISA were viewed as warrants for Fourth Amendment purposes or not. While not an explicit recognition of presidential inherent constitutional authority, it might be argued that, when viewed in light of the earlier statement, some level of recognition of that authority might also be inferred from this reference.

---

denied sub nom. Ivanov v. United States, 419 U.S. 881, 95 S.Ct. 147, 42 L.Ed.2d 121 (1974); United States v. Brown, 484 F.2d 418 (5 Cir. 1973), cert. denied, 415 U.S. 960, 94 S.Ct. 1490, 39 L.Ed.2d 575 (1974); United States v. Clay, 430 F.2d 165 (5 Cir. 1970), rev'd on other grounds, 403 U.S. 698, 91 S.Ct. 2068, 29 L.Ed.2d 810 (1971). Contra, Zweibon v. Mitchell, 516 F.2d 594 (D.C.Cir.1975) (dictum in plurality opinion in case involving surveillance of domestic organization having an effect on foreign relations but acting neither as the agent of nor in collaboration with a foreign power).").

[4228] 310 F.3d at 746.

Both statements were made in a case in which the Court of Review upheld the constitutionality of FISA, an act which, in express legislative language in its conforming amendments to Title III and in its legislative history, was clearly intended to cabin any inherent presidential authority over electronic surveillance within its sweep, and to provide an exclusive structure for the conduct of such electronic surveillance. It might be argued that the adoption of one of two possible interpretations of the statement would avoid internal inconsistency within the court's decision. One approach would be to interpret these statements by the Court of Review as referring to the President's inherent authority to conduct such surveillances outside the scope of "electronic surveillance" under FISA. In essence, the court's statements would then be seen as a reference to presidential authority over those areas of NSA activities which were intentionally excluded from FISA when it was enacted. Alternatively, it might be argued that the court's statements may refer to continuing exercise of inherent presidential authority within the FISA structure, which the Court of Review found to be constitutional.

In light of the exclusivity language in Title III, 18 U.S.C. § 2511(2)(f) and the legislative history of FISA, it might be argued that electronic surveillance pursuant to FISA is subject to the statutory framework, and does not rely upon an assertion of Presidential inherent authority to support it. Alternatively, it might be contended that, in enacting FISA, the Congress circumscribed the manner in which the President might exercise his inherent constitutional authority with respect to foreign intelligence electronic surveillance, rather than eliminating the President's authority.

As this discussion suggests, while the congressional intent to cabin the President's exercise of any inherent constitutional authority to engage in foreign intelligence electronic surveillance may be clear from the exclusivity provision in FISA and from the legislative history of the measure, some support may be drawn from the Court of Review's decision in *In re Sealed Case* for the position that the President continues to have the power to authorize warrantless electronic surveillance to gather foreign intelligence outside the FISA framework. Whether such authority may exist only as to those areas which were not addressed by FISA in its definition of "electronic surveillance" or is of broader sweep appears to be a matter with respect to which there are differing views.

The Authorization to Use Military Force

In the aftermath of the September 11, 2001, attacks, Congress passed a joint resolution authorizing the President to

> *use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks that occurred on September 11, 2001, or harbored such organizations or persons, in*

order to prevent any future acts of international terrorism against the United States by such nations, organizations or persons.[4229]

Pursuant to that authority, the President ordered U.S. armed forces to invade Afghanistan for the purpose of rooting out Al Qaeda terrorists and toppling the Taliban government that had provided them safe harbor.

The Administration regards the AUMF as providing the authority to conduct electronic surveillance of the type reported in the press.[4230] This conclusion, it argues, is supported by the 2004 Supreme Court decision in Hamdi v. Rumsfeld,[4231] in which the Supreme Court issued its most thorough interpretation of the AUMF to date.[4232] In Hamdi, a plurality of the Court affirmed the President's power to detain a U.S. citizen as an "enemy combatant" as part of the necessary force authorized by Congress in the AUMF, despite an earlier statute which provides that no U.S. citizen may be detained except pursuant to an act of Congress.[4233] However, the Court appears to have relied on a more limited interpretation of the scope of the AUMF than that which the Administration had asserted in its briefs, and, declaring that a "state of war is not a blank check for the President when it comes to the rights of the Nation's citizens,"[4234] the Court clarified that notwithstanding the authorization, such detainees have some due process rights under the U.S. Constitution.[4235]

The Administration's position would seem to rely on at least two assumptions. First, it appears to require that the power to conduct electronic surveillance for intelligence purposes is an essential aspect of the use of military force in the same way that the capture of enemy combatants on the battlefield is a necessary incident to the conduct of military operations. Second, it appears to consider the "battlefield" in the war on terrorism to extend beyond the area of traditional

---

[4229] Authorization for Use of Military Force ("the AUMF"), Pub. L. 107-40, 115 Stat. 224 (2001). For a discussion of the scant legislative history accompanying the AUMF, see CRS Report RS22357, Authorization for Use of Military Force in Response to the 9/11 Attacks (Pub. L. 107-40): Legislative History, by Richard F. Grimmet.

[4230] See OLA Letter, supra note 10.

[4231] 542 U.S. 507 (2004).

[4232] See CRS Report RS21884, The Supreme Court and Detainees in the War on Terrorism: Summary and Analysis, by Jennifer K. Elsea.

[4233] 18 U.S.C. § 4001(a). For more background and analysis of that statute, see CRS Report RL31724 Detention of American Citizens as Enemy Combatants, by Jennifer K. Elsea; CRS Report RS22130, Detention of U.S. Citizens, by Louis Fisher.

[4234] Hamdi v. Rumsfeld, 542 U.S. 507, 536 (2004).

[4235] Id. at 517 (2004).

military operations to include U.S. territory. Both assumptions have been the subject of debate.

The Use of Force

The government finds support in the Hamdi decision for its assertion that the AUMF implies authority to conduct electronic surveillance operations as a necessary incident to the use of force. This implied authority, it is urged, provides the statutory authority required to dispense with FISA requirements in the same way the Hamdi court found the requirement in the Non-Detention Act (18 U.S.C. § 4001(a)), which prohibits the detention of U.S. citizens except pursuant to an act of Congress, to be satisfied by the AUMF.

There is reason, however, to limit Hamdi to actual military operations on the battlefield as that concept is traditionally understood. Justice O'Connor wrote for the plurality that

> *we understand Congress' grant of authority for the use of 'necessary and appropriate force' to include the authority to detain for the duration of the relevant conflict, and our understanding is based on longstanding law-of-war principles. If the practical circumstances of a given conflict are entirely unlike those of the conflicts that informed the development of the law of war, that understanding may unravel.*[4236]

Hamdi may be limited to a confirmation that the authorization to employ military force against an enemy army necessarily encompasses the authority to capture battlefield enemies, because such captures are an essential aspect of fighting a battle.[4237] International law does not permit the intentional killing of civilians or soldiers who are hors de combat, preferring capture as the method of neutralizing enemies on the battlefield.[4238] The capture of an enemy combatant is arguably as much a use of force as killing or wounding one. Justice O'Connor wrote for the plurality

---

[4236] Hamdi at 520.

[4237] Padilla v. Hanft, another case involving an American citizen detained by the military as an "enemy combatant," could be read as an expansion of the detention authority to encompass persons arrested in the United States, far from any battlefield. 423 F.3d 386 (4th Cir. 2005), petition for cert. filed, 74 USLW 3275 (Oct 25, 2005)(NO. 05-533). The Fourth Circuit reversed a lower court's finding that the detention was unlawful, but the appellate finding was based on an understanding that the petitioner had taken up arms against American forces in Afghanistan prior to traveling to the United States with the intent of carrying out acts of terrorism. Whether Hamdi would also extend to a person detained as an enemy combatant based wholly on activity carried out within the United States has not been addressed by any court.

[4238] See generally Department of the Army, FM 27-10, The Law of Land Warfare (1956).

> *There can be no doubt that individuals who fought against the United States in Afghanistan as part of the Taliban, an organization known to have supported the al Qaeda terrorist network responsible for those attacks, are individuals Congress sought to target in passing the AUMF. We conclude that detention of individuals falling into the limited category we are considering, for the duration of the particular conflict in which they were captured, is so fundamental and accepted an incident to war as to be an exercise of the "necessary and appropriate force" Congress has authorized the President to use.*[4239]

While the collection of intelligence is also an important facet of fighting a battle, it is not clear that the collection of intelligence constitutes a use of force. The Hamdi plurality cited the Geneva Conventions and multiple authorities on the law of war to reach its conclusion that the capture of combatants is an essential part of warfare.[4240] The Administration has not pointed to any authority similar to those cited by the Hamdi plurality to support its proposition that signals intelligence is a fundamental aspect of combat. To be sure, there can be little doubt that Congress, in enacting the AUMF, contemplated that the armed forces would deploy their military intelligence assets in Afghanistan or wherever else the conventional aspect of the conflict might spread, but a presumption that the authorization extends to less conventional aspects of the conflict could unravel the fabric of Hamdi, especially where measures are taken within the United States. While five Justices were willing to accept the government's argument that the detention of enemy combatants captured on the battlefield[4241] is a vital aspect of war-fighting, Justice Thomas alone indicated his agreement with the government's argument that wartime detention is also necessary for intelligence purposes.[4242] Justice O'Connor agreed that the law of war supports detention of

---

[4239] Hamdi at 518. Justice Thomas agreed with this proposition, supplying the fifth vote. Id. at 587 ("Although the President very well may have inherent authority to detain those arrayed against our troops, I agree with the plurality that we need not decide that question because Congress has authorized the President to do so.").

[4240] Hamdi at 518-19.

[4241] The Hamdi plurality limited its decision to "enemy combatants" as defined to mean "an individual who, it alleges, was 'part of or supporting forces hostile to the United States or coalition partners' in Afghanistan and who 'engaged in an armed conflict against the United States' there." Hamdi at 516.

[4242] Id. at 595 (Thomas, J., dissenting) ("The Government seeks to further [its security] interest by detaining an enemy soldier not only to prevent him from rejoining the ongoing fight. Rather, as the Government explains, detention can serve to gather critical intelligence regarding the intentions and capabilities of our adversaries, a function that the Government avers has become

enemy combatants to prevent their return to the battlefield, but agreed with the petitioner that "indefinite detention for the purpose of interrogation is not authorized."[4243]

The boundaries of the authority available under this argument are difficult to discern. May any statutory prohibition arguably touching on national security that applies "unless otherwise authorized by statute" be set aside based on the AUMF? Presidential assertions of wartime power have faltered for lack of express congressional approval, especially where civil liberties are implicated.[4244] A less expansive interpretation of the AUMF might dictate that "necessary and appropriate force" must be read, if possible, to conform to the Constitution and Congress's understanding of what activity constitutes a use of force as opposed to an exercise of authority within the domestic sphere.

---

all the more important in the war on terrorism."). Justice Scalia, with Justice Stevens, recognized that the government's security needs include the "need to obtain intelligence through interrogation," but declined to evaluate whether the need could be met within the criminal justice system, noting that such determinations are "beyond . . . the Court's competence . . . but . . . not beyond Congress's." Id. at 577-78 (Scalia, J., dissenting).

[4243] Hamdi at 521. Justices Souter and Ginsberg, while accepting the government's position that the AUMF could be read to authorize actions consonant with the usages of war, rejected the assertion that such usages could be invoked to justify the detention of a captive where the military's actions are incompatible with the law of war. Id. at 549-50 (Souter, J., concurring in part and dissenting in part). Justices Scalia and Stevens would have found that a U.S. citizen enjoys the full range of due process rights, the AUMF notwithstanding. Id. at 556 (Scalia, J., dissenting).

[4244] Compare Youngstown Sheet and Tube Co. v. Sawyer, 343 U.S. 579 (1952), Ex parte Endo, 323 U.S. 214 (1944) (authority to detain U.S. citizen during war not authorized by implication), Ex parte Milligan, 71 U.S. (4 Wall.) 2 (1866) (civilian accused of violating the law of war in non-hostile territory could not be tried by military commission), and Little v. Barreme, 6 U.S. (2 Cr.) 170 (1804) (where Congress had authorized as part of a limited war the seizure of vessels bound to French ports, the President could not authorize the seizure of vessels coming from French ports) with Ex parte Quirin, 317 U.S. 1, 26-27 (1942) (President's order establishing military commissions to try enemy combatants for violating the law of war was valid where Congress had recognized military commissions in statute), Hirabayashi v. United States, 320 U.S. 81, 89-90 (1943) (discriminatory wartime curfew implemented by the executive branch could be enforced against U.S. citizen where Congress had expressly provided for such enforcement) and Korematsu v. United States, 323 U.S. 214 (1944) (same). The Administration cites the Prize Cases, 67 U.S. (2 Black) 635, 668 (1863), for the proposition that "the President has the responsibility to protect the Nation from further attacks, and the Constitution gives him all necessary authority to fulfill that duty." OLA Letter, supra note 10, at 2. The Prize Cases have generally been interpreted as supporting an assertion of inherent presidential power to thwart an attack. See CONSTITUTION ANNOTATED, S.REP.NO. 108-17, at 328-29. It may, however, be significant that the naval blockade there at issue was instituted prior to Congress's having had the opportunity to take action rather than in the face of a statutory prohibition against such action, and was quickly ratified by Congress. See id. at 461-62. Given the Court's tendency to treat the latter question as one calling for judicial avoidance based on the "political question" doctrine, id. at 329, it is possible that the question may never reach a fuller exegesis. However, the area has been characterized by concessions between the President and Congress with respect to the scope of authority of each. See id., id. at 473-75.

The Domestic Sphere versus Military Operations

Although the lack of a formal declaration of war is not relevant to the existence of an armed conflict and is arguably unnecessary for the President to invoke some war powers, it may be argued that a formal declaration makes a difference in determining what law applies within the United States, whether to aliens or citizens.[4245] For example, the Alien Enemy Act and the Trading with the Enemy Act (TWEA),[4246] both of which regulate the domestic conduct of persons during a war, expressly require a declared war and are not triggered simply by an authorization to use force.[4247] The Supreme Court long ago held that the President has no implied authority to promulgate regulations permitting the capture of enemy property located in the United States during hostilities short of a declared war, even where Congress had authorized a "limited" war.[4248] More pertinently, FISA contains an exception to its requirements for 15 days after a congressional declaration of war.[4249] The inclusion of this exception strongly suggests that Congress intended for FISA to apply even during wartime, unless Congress were to pass new legislation. The fact that Congress amended FISA subsequent to September 11, 2001, in order to maximize its effectiveness against the terrorist threat further bolsters the notion that FISA is intended to remain fully applicable. To conclude otherwise would appear to require an assumption that Congress intended the AUMF to authorize the President to conduct electronic surveillance, even against American citizens not involved in combat, under fewer restrictions than would apply during a declared war, notwithstanding FISA provisions strengthened to take such circumstances into account. Even assuming, for argument's sake, that the NSA operations are necessary to prevent another terrorist attack, a presumption that Congress intended to authorize them does not necessarily follow.

[4245] See Youngstown, 343 U.S. at 645 (Jackson, J., concurring) (noting that separation-of-powers concerns are "heightened when the Commander-in-Chief's powers are exercised in the domestic sphere").

[4246] 50 U.S. App. § 1 et seq.

[4247] See generally CRS Report RL31133, Declarations of War and Authorizations for the Use of Military Force: Background and Legal Implications, by David M. Ackerman and Richard F. Grimmett (identifying statutes effective only during declared wars or during hostilities).

[4248] See Brown v. United States, 12 U.S. (8 Cranch) 110 (1814); Little v. Barreme, 6 U.S. (2 Cr.) 170 (1804).

[4249] 50 U.S.C. § 1811. The legislative history indicates that the 15-day period was intended to "allow time for consideration of any amendment to this act that may be appropriate during a wartime emergency." H.R. CONF. REP. NO. 95-1720, at 34 (1978).

It might be argued that the United States is part of the battlefield in the war against terrorism in more than just a metaphorical sense. Proponents of this point of view would argue that the AUMF to authorizes the use of force anywhere in the world,[4250] including the territory of the United States, against any persons determined by the President to have "planned, authorized, committed, or aided the terrorist attacks" or "harbored such organizations or persons." Under this view, the United States is under actual and continuing enemy attack, and the President has the authority to conduct electronic surveillance in the same way the armed forces gather intelligence about the military operations of enemy forces, even if no actual combat is taking place. After all, intelligence efforts are aimed at identifying an attack before it occurs. If electronic surveillance is considered to be a use of force, the AUMF would seem to limit it to those who "planned, authorized, committed, aided" the Sept. 11 attacks or who "harbored such . . . persons." To the extent that the President's executive order authorizes surveillance of persons who are suspected of merely supporting Al Qaeda or affiliated terrorist organizations, it may be seen as being overly broad.

Are the NSA electronic surveillances consistent with FISA and Title III?

Having concluded that the AUMF authorizes the NSA activity, the Administration finds that the activity meets FISA requirements as well. Although the Administration appears to accept the premise that the surveillance is "electronic surveillance" within the meaning of FISA, it argues that it is excused from following the required procedures because section 109 of FISA[4251] exempts from criminal liability those who conduct electronic surveillance without following the FISA procedures where such surveillance is "authorized by statute."

Subsection (a) of section 109 of FISA provides criminal sanctions[4252] for a person who intentionally "engages in electronic surveillance under color of law except as authorized by statute;" or who "discloses or uses information obtained under color of law by electronic surveillance, knowing or having reason to know that the information was obtained through electronic surveillance not authorized by statute." Under subsection (b), it is a defense to a prosecution under subsection (a) that the defendant was a law enforcement or investigative officer engaged in the course of his official duties and the electronic surveillance was authorized by and conducted pursuant to a search warrant or court order of a court of

---

[4250] See Khalid v. Bush, 355 F.Supp.2d 311, 320 (D. D.C. 2005) (noting that "the AUMF does not place geographic parameters on the President's authority to wage this war against terrorists").

[4251] 50 U.S.C. § 1809(a)(1).

[4252] Subsection (c) provides, "An offense described in this section is punishable by a fine of not more than $10,000 or imprisonment for not more than five years, or both." In light of the general fines provision in 18 U.S.C. § 3571, the maximum fine would appear to be $250,000 for an individual defendant, and $500,000 for an institutional defendant."

competent jurisdiction. Under subsection (d), there is federal jurisdiction over an offense under this section if the person committing the offense was an officer or employee of the United States at the time the offense was committed.[4253]

The language of this section was drawn by the conferees from the House version of the measure, with modifications taken from the Senate version.[4254] The House Conference Report, H. CONF. REP. 95-1720, at 33, 1978 U.S.C.C.A.N. at 4062, adopted the House version of these provisions, with amendments to include the Senate provision regarding disclosure or use of information obtained under color of law by electronic surveillance, knowing or having reason to know that the information was obtained through electronic surveillance not authorized by statute. The House Conference Committee described its actions as follows:

[4253] Under 50 U.S.C. § 1810, an aggrieved person, other than a foreign power or an agent of a foreign power, as defined in 50 U.S.C. § 1801(a) or (b)(1)(A), who has been subjected to electronic surveillance or about whom information obtained by electronic surveillance of that person has been disclosed or used in violation of 50 U.S.C. § 1809 may bring an action against any person who committed that violation for actual and punitive damages, plus reasonable attorney's fees and other reasonably incurred investigation and litigation costs. Actual damages may not be less than liquidated damages of $1,000 or $100 per day for each day of the violation, whichever is greater.

[4254] The Senate Judiciary Committee, in S. REP. NO. 95-604(I), at 61, 1978 U.S.C.C.A.N. at 39623963; see also, pertinent portion of the Senate Select Committee on Intelligence's S. REP. NO. 95701, at 68-69, 1978 U.S.C.C.A.N. at 4037-4038, described the Senate version of this provision, which would have provided conforming amendments to Title 18 of the U.S. Code:

[Section 4(a)(1) and (2) are]. . . designed to establish the same criminal penalties for violations of [FISA, conceived in the Senate bill as a new chapter 120 of Title 18, U.S. Code] as apply to violations of chapter 119 [of Title 18, U.S.C.]. As amended, these sections will make it a criminal offense to engage in electronic surveillance except as otherwise specifically provided in chapters 119 and 120. This amendment also provides, however, that "with respect to techniques used by law enforcement officers" which do not involve the actual interception of wire or oral communications, yet do fall within the literal definition of electronic surveillance in Chapter 120 [FISA] — such as the use of a pen register — the procedures of chapter 120 do not apply. In such cases criminal penalties will not attach simply because the government fails to follow the procedures in chapter 120 (such penalties may, of course, attach if the surveillance is commenced without a search warrant or in violation of a court order.) In all cases involving electronic surveillance for the purpose of obtaining foreign intelligence information, however, the prohibitions of 18 U.S.C. 2511 would apply.

(a)(3), (4), (5), and (6). These amendments make clear that the prohibitions in chapter 119 concerning disclosure and use of information, obtained through the interception of wire or oral communications in sections 2511(1)(c) and (d), also apply to disclosure and use of information obtained through electronic surveillance as defined in chapter 120.

The statute calls for a fine of not more than $10,000 or imprisonment for not more than five years, or both, for each violation.

The Senate bill provided, by conforming amendment to title 18, United States Code, for criminal penalties for any person who, under color of law, willfully engages in electronic surveillance except as provided in this bill; for any person who willfully discloses, or endeavors to disclose to any other person information obtained under color of law by electronic surveillance, knowing or having reason to know that the information was obtained through unlawful electronic surveillance; and for any person who willfully uses, or endeavors to use, information obtained through unlawful electronic surveillance.

The House amendments provided for separate criminal penalties in this act, rather than by conforming amendment to title 18, for any person who intentionally engages in electronic surveillance under color of law except as authorized by statute. A defense was provided for a defendant who was a law enforcement or investigative officer engaged in the course of his official duties and the electronic surveillance was authorized by and conducted pursuant to a search warrant or court order of a court of competent jurisdiction.

The conference substitute adopts the House provision modified to add the Senate criminal penalty for any person who discloses or uses information obtained under color of law by electronic surveillance, knowing or having reason to know that the information was obtained through electronic surveillance not authorized by statute. The conferees agree that the criminal penalties for intelligence agents under this Act should be essentially the same as for law enforcement officers under title 18.[4255]

The Administration appears to rely upon the Authorization to Use Military Force (AUMF), Pub. L. 107-40, 115 Stat. 224 (2001), in arguing that the NSA electronic surveillances at issue are "authorized by statute," as that phrase is used in 50 U.S.C. § 1809(a). The FISA bill as passed included the House version of Section 109(a)(1) of the measure, while Section 109(a)(2) was drawn from the Senate

---

[4255] The House Intelligence Committee discussed the meaning of "intentionally" in the context of Section 109(a)(2) of the House bill, which was replaced by the Senate language. However, as the legislative language was written, the word "intentionally" applied to both Section 109(a)(1) and Section 109(a)(2). The House Report, H. REP. NO. 95-1283, at 97, emphasized that "intentionally" as used in this section was "intended to reflect the most strict standard for criminal culpability. What is proscribed is an intentional violation of an order or one of the specified provisions, not just intentional conduct. The Government would have to provide beyond a reasonable doubt both that the conduct engaged in was in fact a violation, and that it was engaged in with a conscious objective or desire to commit a violation. . . ."

passed bill. The House Permanent Select Committee's Report, H. Rep. No. 95-1283(I), at 96 (June 8, 1978), sheds some light on the intended meaning of Section 109(a)(1) of H.R. 7308 (95th Cong.) which became 50 U.S.C. § 1809(a)(1):

> *Section 109(a)(1) carries forward the criminal provisions of chapter 119 [of Title 18, U.S.C.] and makes it a criminal offense for officers or employees of the United States to intentionally engage in electronic surveillance under color of law except as specifically authorized in chapter 119 of title III [of the Omnibus Crime Control and Safe Streets Act of 1968] and this title. Since certain technical activities — such as the use of a pen register — fall within the definition of electronic surveillance under this title, but not within the definition of wire or oral communications under chapter 119 [of Title 18, U.S.C.], the bill provides an affirmative defense to a law enforcement or investigative officer who engages in such an activity for law enforcement purposes in the course of his official duties, pursuant to a search warrant or court order.*

The House Permanent Select Committee on Intelligence also noted that, "[o]ne of the important purposes of the bill is to afford security to intelligence personnel so that if they act in accordance with the statute and the court order, they will be insulated from liability; it is not to afford them immunity when they intentionally violate the law."

Thus, the legislative history appears to reflect an intention that the phrase "authorized by statute" was a reference to chapter 119 of Title 18 of the U.S. Code (Title III) and to FISA itself, rather than having a broader meaning, in which case a clear indication of Congress's intent to amend or repeal it might be necessary before a court would interpret a later statute as superceding it. Nevertheless, without taking into account the legislative history, the phrase might be seen as having a more expansive application. This broader view appears to have been taken by the Administration in its position regarding the authority provided by the AUMF.

Next, the Administration turns to the wiretap prohibition contained in Title III, which contains an exception for surveillance carried out pursuant to FISA. Pointing out that the exception in section 109 is broad in comparison to the exception in 18 U.S.C. § 2511, whose prohibition applies "except as otherwise specifically provided in this chapter," the Administration appears to conclude that the broader FISA exception subsumes the narrower exception in Title III, at least with respect to national security wiretaps. It cites two of the specific exceptions in Title III. First, 18 U.S.C. 2511(2)(e) provides a defense to criminal liability to government agents who "conduct electronic surveillance, as defined in section 101 of [FISA], as authorized by that Act." The Administration appears to interpret "as authorized by [FISA]" to include activity exempt from the FISA prohibition by virtue of its being authorized by other statute. Under this

interpretation, subsection 2511(2)(e) should be read to exempt electronic surveillance "as authorized by FISA or any other statute."

Similar analysis leads the Administration to conclude that the Title III exclusivity provision in 18 U.S.C. § 2511(2)(f) poses no impediment. Section 2511(2)(f), which exempts

U.S. foreign intelligence activities not covered by FISA, also provides that the procedures in Title III and FISA "shall be the exclusive means by which electronic surveillance, as defined in section 101 of [FISA], and the interception of domestic wire, oral, and electronic communications may be conducted." The Administration argues that

> *By expressly and broadly excepting from its prohibition electronic surveillance undertaken "as authorized by statute," section 109 of FISA permits an exception to the "procedures" of FISA referred to in 18 U.S.C. § 2511(2)(f) where authorized by another statute, even if the other authorizing statute does not specifically amend section 2511(2)(f).*[4256]

In other words, it appears, the FISA "procedures" described in Title III (in 18 U.S.C. § 2511(2)(f)) can include any other procedures authorized, expressly or implicitly, by any other statute, because these would not be prohibited by FISA section 109. This reading would seem to make the exclusivity provision meaningless, a construction not ordinarily favored by courts. It may be questioned whether Congress actually intended for the exception to the criminal prohibition in FISA to negate the more specific requirements in Title III and its exclusivity provision.

The Administration continues

> *Some might suggest that FISA could be read to require that a subsequent statutory authorization must come in the form of an amendment to FISA itself. But under established principles of statutory construction, the AUMF and FISA must be construed in harmony to avoid any potential conflict between FISA and the President's Article II authority as Commander in Chief. Accordingly, any ambiguity as to whether the AUMF is a statute that satisfies the requirements of FISA and allows electronic surveillance in the conflict with al Qaeda without complying with FISA procedures must be resolved in favor of an interpretation*

[4256] OLA Letter, supra note 10, at 3.

> *that is consistent with the President's long-recognized authority.*[4257]

It is unclear how FISA and the AUMF are seen to collide. Principles of statutory construction generally provide guidance for interpreting Congress's intent with respect to a statute where the text is ambiguous or a plain reading leads to anomalous results; and where possible, a statute that might be read in such a way as to violate the Constitution is to be construed to avoid the violation. However, such principles are only to be applied where there is a genuine ambiguity or conflict between two statutes,[4258] and where there is some possible reading that might avoid a conflict. While the Court has been known to read into a statute language that does not appear, it would be unusual for the Court to read express statutory language out of a statute, except by declaring at least that portion of the statute to be unconstitutional. It would not ordinarily be presumed that Congress meant the opposite of what it said, merely because its words are constitutionally problematic.

It appears that the Administration's views regarding the statutory authorization supporting the NSA activity also rely on an assumption that FISA, at least to the extent that its provisions apply to activity conducted in the war against terrorism, may be an unconstitutional encroachment into presidential powers. Its argument, partly based on the exigencies of the post-9/11 period, seems to imply such a view of FISA:

> *As explained above. the President determined that it was necessary following September 11 to create an early warning detection system. FISA could not have provided the speed and agility required for the early warning detection system. In addition, any legislative change, other than the AUMF, that the President might have sought specifically to create such an early warning system would have been public and would have tipped off our enemies concerning our intelligence limitations and capabilities.*

[4257] *Id.* at 4 (citing INS v. Cyr, 533 U.S. 289, 300 v. (2001) (holding that "if an otherwise acceptable construction of a statute would raise serious constitutional problems, and where an alternative interpretation of the statute is 'fairly possible,' we are obligated to construe the statute to avoid such problems") (internal citation omitted); *Zadvydas v. Davis*, 533 U.S. 678, 689 (2001) (noting that a "'cardinal principle' of statutory interpretation [is] that when an Act of Congress raises 'a serious doubt' as to its constitutionality, 'this Court will first ascertain whether a construction of the statute is fairly possible by which the question may be avoided'") (citations omitted)). Both cited cases involved due process implications rather than whether a statute violated the principle of separation of powers by encroaching on presidential powers.

[4258] *See, e.g*, Ruckelshaus v. Monsanto Co., 467 U.S. 986, 1018 (1984) ("Where two statutes are capable of co-existence, it is the duty of the courts, absent a clearly expressed congressional intention to the contrary, to regard each as effective" (internal quotation marks omitted)).

Insofar as the Administration's position is founded upon a concern that FISA was not adequate to the needs of the moment, it might be considered whether 50 U.S.C. §§ 1802 (Attorney General certification that certain conditions are met) and 1805(f) (72-hour emergency order), where applicable, may have provided some of the flexibility that the President considered warranted under the circumstances. To the extent that a lack of speed and agility is a function of internal Department of Justice procedures and practices under FISA, it may be argued that the President and the Attorney General could review those procedures and practices in order to introduce more streamlined procedures to address such needs. Where FISA's current statutory framework proved inadequate to the task, legislative changes might be pursued.

The Administration argues that, "any legislative change, other than the AUMF, that the President might have sought specifically to create such an early warning system would have been public and would have tipped off our enemies concerning our intelligence limitations and capabilities."[4259] However, some of these concerns may be minimized or addressed by virtue of the fact that, where appropriate, oversight may be conducted in executive session; and access to classified information, including information relating to sensitive intelligence sources and methods, may be limited by statute, by House and Senate procedures, or both. Nevertheless, to some degree, the federal legislative process is, by its very nature, public. Depending upon how such legislation was structured, an argument may be made that it might give rise to some inferences as to present or future intelligence practices or capabilities. On the other hand, the legislative vehicle chosen and the legislative language used might minimize some of those concerns. In addition, no legal precedent appears to have been presented that would support the President's authority to bypass the statutory route when legislation is required, based an asserted need for secrecy.[4260]

Conclusion

Whether an NSA activity is permissible under the Fourth Amendment and the statutory scheme outlined above is impossible to determine without an understanding of the specific facts involved and the nature of the President's authorization, which are for the most part classified. If the NSA operations at

---

[4259] See OLA Letter, supra note 10, at 5.

[4260] *C.f.* Youngstown Sheet and Tube Co. v. Sawyer, 343 U.S. 579, 603-04 (Frankfurter, J., concurring):

The utmost that the Korean conflict may imply is that it may have been desirable to have given the President further authority, a freer hand in these matters. Absence of authority in the President to deal with a crisis does not imply want of power in the Government. Conversely the fact that power exists in the Government does not vest it in the President. The need for new legislation does not enact it. Nor does it repeal or amend existing law.

issue are encompassed in the definition of "electronic surveillance" set forth under FISA, it would seem consistent with Congress's intent that such surveillance must be carried out in accordance with FISA procedures. Although section 109(a) of FISA does not explicitly limit the language "as authorized by statute" to refer only to Title III and to FISA, the legislative history suggests that such a result was intended. The exceptions to the criminal prohibition under Title III, however, are specifically limited to those mentioned within Title III. Even if the AUMF is read to provide the statutory authorization necessary to avoid criminal culpability under FISA, it does not necessarily follow that the AUMF provides a substitute authority under FISA to satisfy the more specific language in Title III. To the extent that any of the electronic surveillance at issue may be outside the sweep of FISA or Title III, Congress does not appear to have legislated specifically on the subject, nor, by the absence of legislation, to have authorized or acquiesced in such surveillance.

Whether such electronic surveillances are contemplated by the term "all necessary and appropriate force" as authorized by the AUMF turns on whether they are, under the Hamdi analysis, an essential element of waging war. Even assuming that the President's role as Commander in Chief of the Armed Forces is implicated in the field of electronic surveillance for the collection of foreign intelligence information within the United States, it should not be accepted as a foregone conclusion that Congress has no role to play.[4261] By including the emergency authorization for electronic surveillance without a court order for fifteen days following a declaration of war, Congress seems clearly to have contemplated that FISA would continue to operate during war, although such conditions might necessitate amendments. Amendments to FISA in the USA PATRIOT Act and subsequent legislation further demonstrate Congress's willingness to make adjustments. The history of Congress's active involvement in regulating electronic surveillance within the United States leaves little room for arguing that Congress has accepted by acquiescence the NSA operations here at issue.

To the extent that the Administration seems to base its interpretation of the AUMF and FISA on the assumption that a reading contrary to the one they rely upon would be an unconstitutional violation of separation-of-powers principles, it appears to regard the matter as deserving the highest level of deference under

---

[4261] Id. at 643-44 (Jackson, J., concurring).

There are indications that the Constitution did not contemplate that the title Commander in Chief of the Army and Navy will constitute him also Commander in Chief of the country, its industries and its inhabitants. He has no monopoly of 'war powers,' whatever they are. While Congress cannot deprive the President of the command of the army and navy, only Congress can provide him an army or navy to command. It is also empowered to make rules for the 'Government and Regulation of land and naval Forces,' by which it may to some unknown extent impinge upon even command functions.

Youngstown's first category[4262] simply by virtue of the assumption that it would survive scrutiny under the third category. To conclude that Congress's enactments are unconstitutional and therefore could not reflect Congress's intent seems to beg the question.

Court cases evaluating the legality of warrantless wiretaps for foreign intelligence purposes provide some support for the assertion that the President possesses inherent authority to conduct such surveillance. The Court of Review, the only appellate court to have addressed the issue since the passage of FISA, "took for granted" that the President has inherent authority to conduct foreign intelligence electronic surveillance under his Article II powers, stating that, "assuming that was so, FISA could not encroach on that authority."[4263] However, much of the other lower courts' discussions of inherent presidential authority occurred prior to the enactment of FISA, and no court has ruled on the question of Congress's authority to regulate the collection of foreign intelligence information.

From the foregoing analysis, it appears unlikely that a court would hold that Congress has expressly or impliedly authorized the NSA electronic surveillance operations here under discussion, and it would likewise appear that, to the extent that those surveillances fall within the definition of "electronic surveillance" within the meaning of FISA or any activity regulated under Title III, Congress intended to cover the entire field with these statutes. To the extent that the NSA activity is not permitted by some reading of Title III or FISA, it may represent an exercise of presidential power at its lowest ebb, in which case exclusive presidential control is sustainable only by "disabling Congress from acting upon the subject."[4264] While courts have generally accepted that the President has the power to conduct domestic electronic surveillance within the United States inside the constraints of the Fourth Amendment, no court has held squarely that the Constitution disables the Congress from endeavoring to set limits on that power. To the contrary, the Supreme Court has stated that Congress does indeed have power to regulate domestic surveillance,[4265] and has not ruled on the extent to which Congress can act with respect to electronic surveillance to collect foreign intelligence information. Given such uncertainty, the Administration's legal

---

[4262] See OLA Letter, supra note 10, at 3 (asserting that "the President's 'authority is at its maximum,'" under Justice Jackson's concurrence in Youngstown and suggestingthat the NSA operations contrast with the seizure invalidated in that case, which resulted from "the absence of a statute 'from which [the asserted authority] [could] be fairly implied'" (citing Youngstown at 585)).

[4263] 310 F.3d at 742; see also id. at 746.

[4264] Id. at 638.

[4265] United States v. United States District Court, 407 U.S. 297, 323-24 (1972).

justification, as presented in the summary analysis from the Office of Legislative Affairs, does not seem to be as well-grounded as the tenor of that letter suggests.

Subchapter III: Pen Registers and Trap and Trace Devices for Foreign Intelligence Purposes (50 U.S.C. §§ 1841-1846)

And

Subchapter IV: Access to Certain Business Records for Foreign Intelligence Purposes (50 U.S.C. §§ 1861-1863)

Government Access to Phone Calling Activity and Related Records: Legal Authorities, RL33424 (February 2, 2010).

ELIZABETH B. BAZAN, EDWARD C. LIU, & GINA STEVENS, CONGRESSIONAL RESEARCH SERV., GOVERNMENT ACCESS TO PHONE CALLING ACTIVITY AND RELATED RECORDS: LEGAL AUTHORITIES (2010), , *available at* http://www.intelligencelaw.com/library/secondary/crs/pdf/RL33424_2-2-2010.pdf.

Elizabeth B. Bazan
Legislative Attorney
ebazan@crs.loc.gov, 7-7202

Edward C. Liu
Legislative Attorney
eliu@crs.loc.gov, 7-9166

Gina Stevens
Legislative Attorney
gstevens@crs.loc.gov, 7-2581

February 2, 2010

Congressional Research Service

7-5700
www.crs.gov
RL33424

Summary

Public interest in the means by which the government may collect telephone call records has been raised by ongoing revelations regarding alleged intelligence activity by the National Security Agency (NSA) and the Federal Bureau of Investigation (FBI). According to a USA Today article from May 11, 2006, the NSA allegedly sought and obtained records of telephone numbers called and received from millions of telephones within the United States from three telephone service providers; a fourth reportedly refused to provide such records. Additionally, a series of reports issued by the Department of Justice's Office of the Inspector General (DOJ OIG), most recently in January of 2010, indicate that, between 2002 and 2006, consumer records held by telephone companies had been provided to the FBI through the use of "exigent letters" and other informal methods that fell outside of the national security letter (NSL) process embodied in statute and internal FBI policies.

The Supreme Court has held that there is no Fourth Amendment protection of telephone calling records held in the hands of third party providers, where the content of any call is not intercepted. However, this report summarizes existing statutory authorities regarding access by the government, for either foreign intelligence or law enforcement purposes, to information related to telephone calling patterns or practices. Where pertinent, it also discusses statutory prohibitions against accessing or disclosing such information, along with relevant exceptions to those prohibitions.

Statutory provisions authorizing, pursuant to court order, the use of pen registers and trap and trace devices exist in both the Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. § 1841 et seq., and, for law enforcement purposes, in 18 U.S.C. § 3121 et *seq*.

FISA's "business records" provision, 50 U.S.C. § 1861, provides authority, pursuant to court order, for requests for production of "any tangible thing" relevant to collection of foreign intelligence information not concerning a U.S. person, or relevant to an investigation into international terrorism or clandestine intelligence activities. Under 50 U.S.C. § 1861, an investigation concerning a U.S. person may not be based solely on activities protected by the First Amendment.

Access to stored electronic communications is addressed in 18 U.S.C. § 2701 et seq. 18 U.S.C. § 2702 prohibits voluntary disclosure of customer communications records by a service provider unless it falls within one of several exceptions. Required disclosure of customer records to the government under certain circumstances is addressed under 18 U.S.C. § 2703, including, among others, disclosure pursuant to a warrant or grand jury or trial subpoena. 18 U.S.C. § 2709 is a national security letter provision, under which a wire or electronic service provider may be compelled to provide subscriber information and toll billing records information, or electronic communication transactional records in its custody or possession.

Finally, § 222 of the Communications Act of 1934, as amended, protects customer proprietary network information, and violations of pertinent provisions of law or regulation may expose service providers to criminal sanctions, civil penalties, and forfeiture provisions.

Introduction

Public interest in the means by which the government may collect telephone call records has been raised by ongoing revelations regarding alleged intelligence activity by the National Security Agency (NSA) and the Federal Bureau of Investigation (FBI). According to a *USA Today* article from May 11, 2006, the NSA allegedly sought and obtained records of telephone numbers called and received from millions of telephones within the United States from three telephone service providers; a fourth reportedly refused to provide such records.[4266] Additionally, a series of reports issued by the Department of Justice's Office of the Inspector General (DOJ OIG), most recently in January of 2010, indicate that, between 2002 and 2006, consumer records held by telephone companies had been provided to the FBI through the use of "exigent letters" and other informal methods that fell outside of the national security letter (NSL) process embodied in statute and internal FBI policies.[4267] These reports also indicate that records may have been sought without demonstrating a relationship to an active investigation.[4268]

This report summarizes legal authorities regarding access by the government, for either foreign intelligence or law enforcement purposes, to information related to telephone calling patterns or practices. Where pertinent, it also discusses statutory prohibitions against accessing or disclosing such information, along with relevant exceptions to those prohibitions.

[4266] Leslie Cauley, NSA Has Massive Database of Americans' Phone Calls; 3 Telecoms Help Government Collect Billions of Domestic Records, USA TODAY, May 11, 2006, at 1A. The story alleged that Verizon, BellSouth, and AT&T provided calling records in response to the NSA's inquiry or production demand, while Qwest did not. In December of 2008, more revelations regarding an alleged NSA program, given the codename "Stellar Wind," were reported in the December 22, 2008, issue of Newsweek. See Michael Isikoff, The Fed Who Blew the Whistle, NEWSWEEK, Dec. 22, 2008, at 40, 44.

[4267] U.S. DEPARTMENT OF JUSTICE, OFFICE OF THE INSPECTOR GENERAL, A Review of the Federal Bureau of Investigation's Use of Exigent Letters and Other Informal Requests for Telephone Records (Jan. 2010), available at http://www.justice.gov/oig/special/s1001r.pdf; U.S. DEPARTMENT OF JUSTICE, OFFICE OF THE INSPECTOR GENERAL, A Review of the Federal Bureau of Investigation's Use of National Security Letters, at 96 (March 2007), available at http://www.usdoj.gov/oig/special/s0703b/final.pdf.

[4268] Id. at 92-93.

Telephone Records and the Fourth Amendment

The Supreme Court, in *Smith v. Maryland*, 442 U.S. 735 (1979), in a pen register case,[4269] has held that there is no Fourth Amendment protected reasonable expectation of privacy in records of telephone calls held in the hands of third party providers, where the content of any call is not intercepted. The Fourth Amendment to the United States Constitution guarantees:

> *The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.*[4270]

Whether the use of a pen register is a "search and seizure" within the meaning of the Fourth Amendment determines if the government, in compliance with the Constitution, must secure a warrant or court order prior to its installation. In 1979, the United States Supreme Court decided this question in Smith v. Maryland,[4271] holding that the Fourth Amendment does not prohibit the use of pen registers without a warrant. Writing the majority opinion joined by four other justices, Justice Harry Blackmun drew a distinction between the acquisition of contents of telephone communications using electronic listening devices, which the Court in Katz v. United States[4272] had deemed to be a "search" under the Fourth Amendment, and the capture of electronic impulses that identify the numbers dialed on a telephone using a pen register device. According to the majority in Smith, it is a constitutionally significant difference that pen registers do not record the contents of communications, in contrast to the listening devices employed in Katz.[4273] The Court explained that the Fourth Amendment does not apply to the use of pen registers because individuals do not have a legitimate expectation of privacy against invasion by government action, that protects the numbers dialed into a telephone system:

All telephone users realize that they must "convey" phone numbers to the telephone company, since it is through telephone company switching equipment

---

[4269] A pen register is a device or process which records the dialing, routing, addressing, or signaling information transmitted in conjunction with an electronic communication, but does not record the contents of that communication. See 18 U.S.C. § 3127(3).

[4270] U.S. CONST. amend. IV.

[4271] 442 U.S. 735 (1979).

[4272] 389 U.S. 347 (1967).

[4273] Smith, 442 U.S. at 741 (emphasis in original).

that their calls are completed. All subscribers realize, moreover, that the phone company has facilities for making permanent records of the numbers they dial, for they see a list of their long-distance (toll) calls on their monthly bills. In fact, pen registers and similar devices are routinely used by telephone companies "for the purposes of checking billing operations, detecting fraud, and preventing violations of law."[4274]

The Court stated that telephone customers, by voluntarily conveying phone numbers to the telephone company and "expos[ing] that information to its equipment in the ordinary course of business," assume the risk that the company may disclose such information to law enforcement.[4275] Because there is no actual or legitimate expectation of privacy in the numbers dialed from a telephone, the installation and use of a pen register is not a "search" requiring a warrant under the Fourth Amendment, the Court ruled.[4276]

In contrast, the dissenting opinions in Smith concluded that telephone numbers dialed from a phone are entitled to the same constitutional protection that telephone conversations receive under Katz because such numbers are not without "content" - they "reveal the identities of the persons and the places called, and thus reveal the most intimate details of a person's life."[4277] Furthermore, the dissenters objected to the majority's characterization that the use of a telephone involves an assumption of risk on the part of the customer that telephone dialing information might be disclosed to the government; assumption of risk generally requires there to have been a choice to engage in the activity, and "as a practical matter, individuals have no realistic alternative" to the use of a telephone.[4278]

Although the protections of the Fourth Amendment may not reach records of telephone calls held by third parties, Congress has enacted a number of statutes since the Smith decision that both permit access by the government for foreign intelligence or law enforcement purposes to information relating to telephone numbers dialed from or received by a particular telephone number, as well as duration and usage, while simultaneously imposing limitations as to how such information may be accessed and under what circumstances it may be used.

[4274] Id. at 742 (quoting United States v. New York Tel. Co., 434 U.S. 159, 174-75 (1977)).

[4275] Id. at 744.

[4276] Id. at 745-46.

[4277] Id. at 747-48 (Stewart, J., dissenting).

[4278] Id. at 749 (Marshall, J., dissenting).

Statutory Provisions

Information regarding telephone calling patterns, duration, usage, and length of service may be sought by the government directly through the use of pen registers[4279] or trap and trace devices.[4280] Statutory provisions authorizing, pursuant to court order, the use of pen registers and trap and trace devices exist in both the Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. § 1841 et seq., and, for law enforcement purposes, in 18 U.S.C. § 3121 et seq.

Telephone calling activity may also be collected indirectly by seeking telephone toll or transactional records from third party providers. For example, FISA's "business records" provision, 50 U.S.C. § 1861, authorizes court orders to compel the production of "any tangible thing" relevant to collection of foreign intelligence information not concerning a U.S. person, or relevant to an investigation into international terrorism or clandestine intelligence activities.[4281]

Access to stored electronic communications is also addressed in 18 U.S.C. § 2701 *et seq*. 18 U.S.C. § 2702 prohibits voluntary disclosure of customer communications records by a service provider unless it falls within one of several exceptions. Required disclosure of customer records to the government under certain circumstances is addressed under 18 U.S.C. § 2703, including, among others, disclosure pursuant to a warrant or grand jury or trial subpoena. 18 U.S.C. § 2709 is a national security letter provision,[4282] under which a wire or electronic service provider[4283] may be compelled to provide subscriber information and toll

---

[4279] Under 50 U.S.C. § 1841(2), which cross references the definition in 18 U.S.C. § 3127(3), the term "pen register" "means a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication, but such term does not include any device or process used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device or process used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business."

[4280] Under 50 U.S.C. § 1841(2), which cross references the definition in 18 U.S.C. § 3127(4), the term "trap and trace device" "means a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication."

[4281] Under 50 U.S.C. § 1861, an investigation concerning a U.S. person may not be based solely on First Amendment protected activities.

[4282] See CRS Report RL33320, National Security Letters in Foreign Intelligence Investigations: Legal Background and Recent Amendments, by Charles Doyle.

[4283] Under 18 U.S.C. § 2709(f), "A library (as that term is defined in section 213(1) of the Library Services and Technology Act (20 U.S.C. 9122(1)), the services of which include access to the

billing records information, or electronic communication transactional records in its custody or possession in response to a request by the Director of the Federal Bureau of Investigation (FBI) if the Director of the FBI, or his designee in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge designated by the FBI Director in a field office, certifies that the records or information sought is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a U.S. person is not conducted solely on the basis of First Amendment protected activities.

Finally, § 222 of the Communications Act of 1934, as amended, 47 U.S.C. § 222, restricts the voluntary disclosure of customer proprietary network information by telecommunications service providers. Violations of the pertinent provisions of law or regulation may expose service providers to criminal sanctions, civil penalties and forfeiture provisions, 47 U.S.C. §§ 501-503.[4284]

Each of these statutory schemes is described in more detail below.

Pen Registers and Trap and Trace Devices for Foreign Intelligence and International Terrorism Investigations Under FISA

Under 50 U.S.C. § 1842,[4285] the Attorney General or a designated attorney for the government may apply for an ex parte court order authorizing the use of a pen register or trap and trace device to a Foreign Intelligence Surveillance Court (FISC) judge or to a U.S. magistrate judge designated by the Chief Justice of the United States to have the power to hear applications or grant orders approving installation and use of a pen register or trap and trace device on behalf of an FISC judge. The application must be approved by the Attorney General or a designated government attorney; must identify the federal officer seeking to use the pen register or trap and trace device; and must include a certification that the information likely to be obtained is foreign intelligence information[4286] not

---

Internet, books, journals, magazines, newspapers, or other similar forms of communication in print or digitally by patrons for their use, review, examination, or circulation, is not a wire or electronic communication service provider for purposes of this section, unless the library is providing the services defined in section 2510(15) ("electronic communication service") of this title." Subsection (f) was added by P.L. 109-178, § 5.

[4284] See CRS Report RL34409, Selected Laws Governing the Disclosure of Customer Phone Records by Telecommunications Carriers, by Kathleen Ann Ruane.

[4285] Other provisions of this chapter deal with authorization for pen registers or trap and trace devices during emergencies, 50 U.S.C. § 1843, authorization during time of war, 50 U.S.C. 1844, use of information gathered under a FISA pen register or trap and trace device, 50 U.S.C. § 1845, and congressional oversight, 50 U.S.C. § 1846.

[4286] Under 18 U.S.C. § 1801(e), "foreign intelligence information" is defined to mean information that relates to, and if concerning a United States person is necessary to, the ability of the United

concerning a U.S. person[4287] or that the information is relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities. An investigation of a U.S. person may not be conducted solely on the basis of First Amendment protected activities.

The order must specify the identity of the person who is the subject of the investigation, if known. If known, the order must identify the person to whom the telephone line or other facility to which the pen register or trap and trace device is to be attached is leased or in whose name it is listed. In addition, the order must list the attributes of the communications to which it applies, such as the number or other identifier and, if known, the location of the telephone line or other facility involved. In the case of a trap and trace device, the order must also identify the geographic limits of the trap and trace order.

Such an order, at the request of the applicant, also directs the provider of the wire or electronic service, landlord, custodian, or other person, to furnish any information, facilities, or technical assistance needed to accomplish the installation and operation of the pen register or trap and trace device in a manner that will protect its secrecy and minimize interference with the services provided. In addition, the order directs the provider, landlord, custodian, or other person not to disclose the existence of the investigation or the pen register or trap and trace device to anyone unless or until ordered to do so by the court. Records concerning the pen register or trap and trace device or the aid furnished are to be kept under security procedures approved by the Attorney General and the Director of National Security under 50 U.S.C. § 1805(b)(2)(C). The order also directs the applicant for the order to provide compensation for reasonable expenses incurred by the provider, landlord, custodian, or other person in providing information, facilities, or technical assistance.

States to protect against actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power, sabotage or international terrorism by a foreign power or an agent of a foreign power, or clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to the national defense or the security of the United States or the conduct of the foreign affairs of the United States. The phrase "agents of a foreign power" currently includes, among others, non-U.S. persons that are engaged in international terrorism, but are not linked to an identifiable terrorist organization or foreign government. For a more detailed discussion of treatment of so-called "lone wolf" terrorists under FISA, see CRS Report R40138, Amendments to the Foreign Intelligence Surveillance Act (FISA) Set to Expire February 28, 2010, by Anna C. Henning and Edward C. Liu, at 2-4.

[4287] Under 50 U.S.C. § 1801(i), "United States person" means a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 1101(a)(20) of Title 8), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in subsection (a)(1), (2), or (3) of this section.

Under 50 U.S.C. § 1842(d)(2)(C)(i), upon the request of the applicant for the court order, the court shall direct the wire or electronic service provider to provide the federal officer using the pen register or trap and trace device with the name; address; and the telephone number, instrument number or subscriber number or identifier of the customer or subscriber using the service covered by the order for the period specified by the order, including temporarily assigned network address or associated routing or transmission information. The service provider must also provide, if so ordered by the court upon the applicant's request, information on length of service of the customer or subscriber, as well as local or long distance telephone records of the subscriber or customer, and, if applicable, any records on periods of usage by the customer or subscriber. Further, the court, at the applicant's request, may order disclosure by the service provider of any mechanisms and sources of payment for the service (i.e., credit card, bank account).

Similarly, under 50 U.S.C. § 1842(d)(2)(C)(ii), if the information is available with respect to any customer or subscriber of incoming or outgoing communications to or from the service covered by the order, the court, upon the request of the applicant for the order, is to direct the wire or electronic service provider to provide the name; address; telephone number, instrument number or other subscriber number or identifier, of such customer or subscriber, as well as length of service provided to and types of serviced utilized by the subscriber or customer.

In general, the duration of an order issued under this section is not to exceed 90 days, with the possibility of extension for periods of not more than 90 days. However, if the applicant for the order certifies that the information likely to be obtained is foreign intelligence information not concerning a United States person, then an extension may be for up to a year. No cause of action may be brought against any wire or electronic service provider, landlord, custodian, or other person that furnishes information, facilities, or technical assistance pursuant to an order issued under this provision. Unless otherwise ordered by the judge, the results of the pen register or trap and trace device are to be provided to the authorized government official or officials at reasonable intervals.

Under 50 U.S.C. § 1805(i), as added by the FISA Amendments Act of 2008,[4288] if an FISC judge grants an application by the government to conduct electronic surveillance under FISA, then, upon the request of the applicant, the FISC judge shall also authorize the installation and use of pen registers and trap and trace devices. In such circumstances, the provisions of 50 U.S.C. § 1842(d)(2) regarding disclosure of customer or subscriber information to the government would apply.

[4288] P.L. 110-261, § 105.

Pen Registers or Trap and Trace Devices Generally, and for Use in an Ongoing Criminal Investigation

18 U.S.C. § 3121 prohibits the installation and use of a pen register or trap and trace device without first obtaining a court order under FISA or under 18 U.S.C. § 3123. This prohibition does not apply to use by an electronic or wire service provider relating to:

- the operation, maintenance and testing of a service or protection of the rights or property of the service provider;
- the protection of users of the service from abuse or unlawful use of the service;
- to recording of the fact that a wire or electronic communication was initiated or completed to protect the service provider, another provider furnishing service toward completion of the wire communication, or a user of the service from fraudulent, unlawful or abusive use of the service; or
- to use where the consent of the user of the service has been obtained.

A government agency authorized to install and use a pen register or trap and trace device under the provisions of this chapter of Title 18, U.S.C., or under state law must use technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to the dialing, routing, addressing, and signaling information utilized in the processing and transmitting of wire or electronic communications in a manner that does not include the contents of that communication.

An application for a court order authorizing a pen register or trap and trace device under this chapter must be made pursuant to 18 U.S.C. § 3122 in writing under oath or affirmation to a court of competent jurisdiction. Such an application must include the identity of the attorney for the government or the state law enforcement or investigative officer making the application and the identity of the law enforcement agency conducting the investigation, as well as a certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency.

Under 18 U.S.C. § 3123, the court shall enter an ex parte order authorization installation and use of a pen register or trap and trace device anywhere in the United States if the court finds that the applicant for the order has made such a certification. An order may authorize installation and use of a pen register or trap and trace device for a period of up to 60 days, which can be extended by court order for additional periods of no more than 60 days. The order must also direct that the order be sealed until otherwise ordered by the court, and must prohibit the person owning or leasing the line or other facility to which the pen register or trap and trace device is attached or applied, or who is obligated by the order to assist the applicant, from disclosing the existence of the pen register or trap and

trace device or of the investigation to the listed subscriber or to any other person unless or until the court orders otherwise.[4289]

Access to Business Records for Foreign Intelligence and International Terrorism Investigations

Under 50 U.S.C. § 1861, the Director of the Federal Bureau of Investigation (FBI) or a designee of the Director, whose rank shall not be lower than Assistant Special Agent in Charge, may apply to the FISA court for an order granting the government access to any tangible item (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information not concerning a United States person, or to protect against international terrorism or clandestine intelligence activities. Such an investigation of a United States person may not be conducted solely upon the basis of activities protected by the first amendment to the Constitution.

The application for such an order must include a statement of facts demonstrating that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized or preliminary investigation to protect against international terrorism or espionage, or to obtain foreign intelligence information not concerning a U.S. person.[4290] However, certain tangible items are deemed presumptively relevant to an investigation if the application's statement of facts shows that the items sought pertain to a foreign power or an agent of a foreign power, the activities of a suspected agent of a foreign power who is the subject of such authorized investigation, or an individual in contact with, or known to, a suspected agent of a foreign power who is the subject of such authorized investigation.[4291]

The FISA court judge shall approve an application for an order under 50 U.S.C. § 1861, as requested or as modified, upon a finding that the application complies with statutory requirements. The order must contain a particularized description

---

[4289] 18 U.S.C. § 3124 addresses assistance in installation and use of the pen register or trap and trace device; while 18 U.S.C. § 3125 deals with emergency installation of a pen register and trap or trap and trace device. 18 U.S.C. § 2136 provides for annual reports to Congress by the Attorney General on the number of applications by law enforcement agencies of the Department of Justice for pen registers or trap and trace devices orders, as well as certain details with respect to court orders issued in response to such applications.

[4290] 50 U.S.C. § 1861(b)(2)(A).

[4291] The phrase "agents of a foreign power" currently includes, among others, non-U.S. persons that are engaged in international terrorism, but are not linked to an identifiable terrorist organization or foreign government. For a more detailed discussion of treatment of so-called "lone wolf" terrorists under FISA, see CRS Report R40138, Amendments to the Foreign Intelligence Surveillance Act (FISA) Set to Expire February 28, 2010, by Anna C. Henning and Edward C. Liu, at 2-4.

of the items sought, provide for a reasonable time to assemble them, and be limited to things which may be obtained under a grand jury subpoena or an order of a U.S. court for production of records or tangible things.[4292] The order to produce the tangible things (production order) is also accompanied by a nondisclosure requirement (nondisclosure order) that prohibits the recipient from disclosing to any other person that the FBI has sought the tangible things described in the order, with limited exceptions.[4293]

The recipient may immediately challenge the legality of the production order by filing a petition with the FISA court; however, the recipient must wait one year before challenging the nondisclosure order.[4294] A FISA court judge considering the recipient's petition to modify or set aside the production order may do so only if the judge finds that the order does not meet statutory requirements or is otherwise unlawful.[4295] A nondisclosure order may be modified or set aside if the judge finds that there is no reason to believe that disclosure may endanger the national security of the United States; interfere with a criminal, counterterrorism, or counterintelligence investigation; interfere with diplomatic relations; or endanger the life or physical safety of any person.[4296] If, at the time the individual files the petition for judicial review of a nondisclosure order, the Attorney General, Deputy Attorney General, an Assistant Attorney General, or the Director of the FBI certifies that disclosure may endanger the national security of the United States or interfere with diplomatic relations, then the FISA judge must treat such government certification as conclusive unless the judge finds that the certification was made in bad faith.[4297]

Authority to collect communications records under FISA is currently set to expire on December 31, 2009. After this date, and absent congressional extension, only records from common carriers, public accommodation facilities, storage facilities, and vehicle rental facilities may be sought under FISA.[4298]

[4292] 50 U.S.C. § 1861(c).

[4293] A recipient of a FISA order under this section may disclose its existence to persons to whom disclosure is necessary to comply with the order, to an attorney to obtain legal advice with respect to the production of things in response to the order, as well as to other persons approved by the FBI. 50 U.S.C. § 1861(d)(1).

[4294] 50 U.S.C. § 1861(f)(2)(A).

[4295] 50 U.S.C. § 1861(f)(2)(B).

[4296] 50 U.S.C. § 1861(f)(2)(C)(i).

[4297] 50 U.S.C. § 1861(f)(2)(C)(ii).

[4298] See CRS Report R40138, Amendments to the Foreign Intelligence Surveillance Act (FISA) Set to Expire February 28, 2010, by Anna C. Henning and Edward C. Liu, at 7-11.

Access to Stored Electronic Communications and Transactional Records

Access to stored electronic communications and transactional records is addressed in 18 U.S.C. § 2701 et seq. Under 18 U.S.C. § 2702, voluntary disclosure of customer communications records by a service provider is prohibited unless it falls within one of several exceptions, including

- disclosure as authorized in 18 U.S.C. § 2703;
- disclosure with the lawful consent of the customer or subscriber; or
- disclosure to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency.[4299]

In various reports regarding the use of "exigent letters," the DOJ OIG noted that one of the justifications for the use of exigent letters and other informal governmental requests for telephone records had been based upon this voluntary emergency disclosure provision.[4300] However, these reports also concluded that many of the situations in which these tools were used did not appear to meet the emergency standard provided by this exception.[4301]

Under 18 U.S.C. § 2703, a provider of electronic communication service or remote computing service shall disclose to a government entity the name, address, local and long distance telephone connection records, or records of session times and durations, length of service and types of service utilized, telephone instrument number or other subscriber number or identity, including temporarily assigned network address, and means and source of payment for such service pursuant to

- a warrant;

[4299] This language was added by P.L. 109-177, Title I, § 107(b)(1)(B). It replaced an exception which covered "disclosure to a governmental entity if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person justifies disclosure of the information."

[4300] U.S. DEPARTMENT OF JUSTICE OFFICE OF THE INSPECTOR GENERAL, A Review of the Federal Bureau of Investigation's Use of Exigent Letters and Other Informal Requests for Telephone Records, at 260-263, 269 (Jan. 2010), available at http://www.justice.gov/oig/special/s1001r.pdf; U.S. DEPARTMENT OF JUSTICE, OFFICE OF THE INSPECTOR GENERAL, A Review of the Federal Bureau of Investigation's Use of National Security Letters, at 96 (March 2007), available at http://www.usdoj.gov/oig/special/s0703b/final.pdf.

[4301] Id.

- a court order based upon specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication or the records or other information sought are relevant and material to an ongoing criminal investigation;
- customer or subscriber consent;
- a written request from the governmental entity relevant to a law enforcement investigation regarding telemarketing fraud;
- an administrative subpoena authorized by federal or state statute, or
- a federal or state grand jury subpoena or trial subpoena.

A governmental entity receiving such records or information is not required to provide notice to a subscriber or customer. Nor does any cause of action lie against any service provider of wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order, warrant, subpoena, statutory authorization or certification under this chapter.

18 U.S.C. § 2706 requires a government entity obtaining records or other information under §§ 2702 or 2703 to reimburse the costs reasonably necessary and directly incurred in searching for, assembling, reproducing or otherwise providing such information. The amount of payment is to be mutually agreed upon by the government entity and the person or entity providing the information, or, in the absence of an agreement, determined by the court issuing the production order. The reimbursement requirement does not apply to records or other information maintained by a communications common carrier that relate to telephone records and telephone listings obtained under 18 U.S.C. § 2703 unless a court orders payment upon a determination that the information required is unusually voluminous in nature or otherwise caused an undue burden upon the provider.

National Security Letters

Under 18 U.S.C. § 2709, a national security letter provision,[4302] wire or electronic service providers[4303] must provide subscriber information and toll billing records information, or electronic communication transactional records in its custody or possession in response to a request by the Director of the Federal Bureau of

---

[4302] See CRS Report RL33320, National Security Letters in Foreign Intelligence Investigations: Legal Background and Recent Amendments, by Charles Doyle.

[4303] Under 18 U.S.C. § 2709(f), "A library (as that term is defined in section 213(1) of the Library Services and Technology Act (20 U.S.C. 9122(1)), the services of which include access to the Internet, books, journals, magazines, newspapers, or other similar forms of communication in print or digitally by patrons for their use, review, examination, or circulation, is not a wire or electronic communication service provider for purposes of this section, unless the library is providing the services defined in section 2510(15) ("electronic communication service") of this title." Subsection (f) was added by P.L. 109-178, § 5.

Investigation (FBI) if the Director of the FBI, or his designee in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge designated by the FBI Director in a field office, certifies that the records or information sought is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a U.S. person is not conducted solely on the basis of First Amendment protected activities.

Under 18 U.S.C. § 2709(b), if the Director of the Federal Bureau of Investigation, or his designee, certifies that disclosure of the request may result in a danger to the national security of the United States, interference with a criminal, counterterrorism, or counterintelligence investigation, interference with diplomatic relations, or danger to the life or physical safety of any person, no wire or electronic communications service provider, or officer, employee, or agent thereof, shall disclose to any person (other than those to whom such disclosure is necessary to comply with the request or an attorney to obtain legal advice or legal assistance with respect to the request) that the Federal Bureau of Investigation has sought or obtained access to information or records under this section.[4304] The FBI must notify the person or entity to whom a §2709(b) request is made where such a nondisclosure requirement is applicable. A recipient of such a request who notifies those to whom notice is necessary for compliance with the request or who notifies an attorney to obtain legal advice or legal assistance with respect to the request must also advise them of the nondisclosure requirement.

At the request of the Director of the Federal Bureau of Investigation or the designee of the Director, any person making or intending to make a disclosure under this section shall identify to the Director or such designee the person to whom such disclosure will be made or to whom such disclosure was made prior to the request, except that nothing in this section shall require a person to inform the Director or such designee of the identity of an attorney to whom disclosure was made or will be made to obtain legal advice or legal assistance with respect to the request.

The FBI may only disseminate records obtained under this section as provided in guidelines approved by the Attorney General for foreign intelligence collection

---

[4304] P.L. 109-177, § 116(a), rewrote subsection (c) of 18 U.S.C. § 2709, which formerly read, "No wire or electronic communication service provider, or officer, employee, or agent thereof, shall disclose to any person that the Federal Bureau of Investigation has sought or obtained access to information or records under this section." P.L. 109-178, § 4(b), rewrote subsection (c)(4), as amended by P.L. 109-177, § 116(a), which formerly read, "At the request of the Director of the Federal Bureau of Investigation or the designee of the Director, any person making or intending to make a disclosure under this section shall identify to the Director or such designee the person to whom such disclosure will be made or to whom such disclosure was made prior to the request, but in no circumstance shall a person be required to inform the Director or such designee that the person intends to consult an attorney to obtain legal advice or legal assistance."

and foreign counterintelligence investigations conducted by the Federal Bureau of Investigation, and, with respect to dissemination to an agency of the United States, only if such information is clearly relevant to the authorized responsibilities of such agency. On a semiannual basis, the Director of the Federal Bureau of Investigation is required to fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate, and the Committee on the Judiciary of the House of Representatives and the Committee on the Judiciary of the Senate, concerning all requests made under subsection (b) of this section.

Penalties

Except as provided in 18 U.S.C. § 2703(e), 18 U.S.C. § 2707 provides a civil cause of action for any provider of electronic communication service, subscriber, or other person aggrieved by a knowing or intentional violation of this chapter. The aggrieved party may receive equitable relief and damages. The damages which may be assessed by the court are actual damages suffered by the plaintiff plus any profits made by the violator as a result of the violation. At a minimum, a person entitled to recover damages must receive no less than $1,000. If a court or appropriate department or agency determines that the United States has violated this chapter and that the circumstances surrounding the violation raise questions as to whether a federal officer or employee acted willfully or intentionally with respect to the violation, disciplinary action against that officer or employee may also be initiated.

A person aggrieved by a willful violation of this chapter or a willful violation of 50 U.S.C. § 1845(a), which deals with the use of information gathered through a pen register and trap and trace under FISA, may commence a civil action against the United States in a U.S. district court to receive money damages under 18 U.S.C. § 2712. If the claim is successful in establishing such a violation, the court may assess actual damages, but not less than $10,000, whichever is greater, plus reasonably incurred litigation costs. There is a two year statute of limitations applicable to this provision, and this section states that this is the exclusive remedy against the United States for claims within the purview of the section. The agency or department must reimburse any award under this section to the U.S. treasury. Administrative discipline may also be pursued. A proceeding under 18 U.S.C. § 2712 shall be stayed by the court, upon motion by the United States, if the court determines that civil discovery will adversely affect the government's ability to conduct a related investigation or prosecution of a related criminal case. Such a stay also tolls the statute of limitations.

Communications Act of 1934

Telecommunications carriers are also subject to obligations to guard the confidentiality of customer proprietary network information (CPNI) and to ensure that it is not disclosed to third parties without customer approval or as required by law. Section 222 of the Communication Act of 1934, as amended, establishes a duty of every telecommunications carrier to protect the

confidentiality of its customers' customer proprietary network information.[4305] Section 222 attempts to achieve a balance between marketing and customer privacy.

CPNI includes personally identifiable information derived from a customer's relationship with a telephone company, irrespective of whether the customer purchases landline or wireless telephone service. CPNI is defined as

> *(A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier.*[4306]

CPNI includes customers' calling activities and history (e.g., phone numbers called, frequency, duration, and time), and billing records.[4307] It does not include subscriber list information, such as name, address, and phone number.[4308]

In section 222, Congress created a framework to govern telecommunications carriers' use of information obtained through provision of a telecommunications service. Section 222 of the act provides that telecommunications carriers must protect the confidentiality of customer proprietary network information. The act limits carriers' abilities to use customer phone records, including for their own marketing purposes, without customer approval and appropriate safeguards. The act also prohibits carriers from using, disclosing, or permitting access to this information without the approval of the customer, or as otherwise required by law, if the use or disclosure is not in connection with the provided service.

Section 222(a) imposes a general duty on telecommunications carriers to protect the confidentiality of proprietary information of other carriers, equipment manufacturers, and customers.[4309] Section 222(b) states that a carrier that

---

[4305] 47 U.S.C. § 222. Section 222 was added to the Communications Act by the Telecommunications Act of 1996. Telecommunications Act of 1996, P.L. 104-104, 110 Stat. 56 (codified at 47 U.S.C. §§ 151 et seq.).

[4306] 47 U.S.C. § 222(h)(1).

[4307] See FED. COMM. COMM'N, Protecting Your Telephone Calling Records (Oct. 20, 2008) available at http://www.fcc.gov/cgb/consumerfacts/phoneaboutyou.html.

[4308] 47 U.S.C. § 222(h)(3).

[4309] 47 U.S.C.§ 222(a).

receives or obtains proprietary information from other carriers in order to provide a telecommunications service may use such information only for that purpose and may not use that information for its own marketing efforts.[4310]

The confidentiality protections applicable to customer proprietary network information are established in section 222(c). Subsection (c)(1) constitutes the core privacy requirement for telecommunications carriers.

> *Except as required by law or with the approval of the customer, a telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications service shall only use, disclose, or permit access to individually identifiable customer proprietary network information in its provision of (A) the telecommunications service from which such information is derived, or (B) services necessary to, or used in, the provision of such telecommunications service, including the publishing of directories.*[4311]

Section 222(c)(2) provides that a carrier must disclose CPNI "upon affirmative written request by the customer, to any person designated by the customer."[4312] Section 222(c)(3) provides that a carrier may use, disclose, or permit access to aggregate customer information other than for the purposes described in subsection (1).[4313] Thus, the general principle of confidentiality for customer information is that a carrier may only use, disclose, or permit access to customers' individually identifiable CPNI in limited circumstances: (1) as required by law;[4314] (2) with the customer's approval; or (3) in its provision of the telecommunications service from which such information is derived, or services necessary to or used in the provision of such telecommunications service.

Exceptions to the general principle of confidentiality permit carriers to use, disclose, or permit access to customer proprietary network information to (1) initiate, render, bill, and collect for telecommunications services; (2) protect the rights or property of the carrier, the customers, and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services; (3)

[4310] 47 U.S.C. § 222(b).

[4311] 47 U.S.C. § 222(c)(1).

[4312] 47 U.S.C. § 222(c)(2).

[4313] 47 U.S.C. § 222(c)(3). The term "aggregate customer information" means collective data that relates to a group or category of services or customers, from which individual customer identities and characteristics have been removed. 47 U.S.C. § 222(h)(2).

[4314] Whether the statutory provisions discussed in this report would fall within this exception is uncertain.

provide any inbound telemarketing, referral, or administrative services to the customer for the duration of the call; and (4) provide call location information concerning the user of a commercial mobile service for emergency.[4315]

Section 222(e) addresses the disclosure of subscriber list information, and permits carriers to provide subscriber list information to any person upon request for the purpose of publishing directories. The term "subscriber list information" means any information identifying the listed names of subscribers of a carrier and such subscribers' telephone numbers, addresses, or primary advertising classifications, or any combination of such listed names, numbers, addresses, or classifications; that the carrier or an affiliate has published, caused to be published, or accepted for publication in any directory format.[4316]

Customer Proprietary Network Information (CPNI) Regulations

In 1998, the Federal Communications Commission issued its *CPNI Order* to implement section 222.[4317] The CPNI Order and subsequent orders issued by the Commission govern the use and disclosure of customer proprietary network information by telecommunications carriers. When the FCC implemented Section 222, telecommunications carriers were required to obtain express consent from their customers (i.e., "opt-in consent") before a carrier could use customer phone records to market services outside of the customer's relationship with the carrier. The United States Court of Appeals for the Tenth Circuit struck down those rules, finding that they violated the First and Fifth Amendments of the Constitution.[4318]

Subsequently, the FCC amended its CPNI regulations to require telecommunications carriers to receive opt-in (affirmative) consent before disclosing CPNI to third parties or affiliates that do not provide communications-related services.[4319] However, carriers are permitted to disclose CPNI to affiliated parties after obtaining a customer's "opt-out" consent.[4320] "Opt-Out" consent

---

[4315] 47 U.S.C. § 222(d).

[4316] 47 U.S.C. § 222(e).

[4317] CPNI Order, 13 FCC Rcd 8061.

[4318] U.S. West v. FCC, 182 F.3d 1224 (10th Cir. 1999), cert. denied Competition Policy Instit. v. U.S. West, Inc., 530 U.S. 1213 (2000).

[4319] Except as required by law, carriers may not disclose CPNI to third parties or their own affiliates that do not provide communications-related services unless the consumer has given "opt in" consent, which is express written, oral, or electronic consent. 47 C.F.R. §§ 64.2005(b), 64.2007(b)(3); 64.2008(e); see also 47 C.F.R. § 64.2003(h) (defining "optin approval").

[4320] 47 C.F.R. §§ 64.2005(b), 64.2007(b)(1).

means that the telephone company sends the customer a notice saying it will consider the customer to have given approval to use the customer's information for marketing unless the customer tells it not to do so (usually within 30 days.)[4321] Carriers are required, prior to soliciting the customer's approval, to provide notice to the customer of the customer's right to restrict use, disclosure, and access to the customer's CPNI.[4322] Carriers are also required to establish safeguards to protect against the unauthorized disclosure of CPNI, including requirements that carriers maintain records that track access to customer CPNI records.[4323] Each carrier is also required to certify annually its compliance with the CPNI requirements and to make this certification publicly available.[4324] The FCC recently proposed $100,000 fines on telephone companies with inadequate certifications regarding compliance with FCC rules protecting customer information from disclosure.[4325] A suit challenging the opt-in requirement is currently pending before the D.C. Circuit.[4326]

Penalties

Carriers in violation of the CPNI requirements are subject to a variety of penalties under the act. Under the criminal penalty provision in section 501 of the act, 47 U.S.C. § 501, any person who willfully and knowingly does, causes or allows to be done, any act, matter, or thing prohibited by the act or declared unlawful, or who willfully and knowingly omits or fails to do what is required by the act, or who willfully or knowingly causes or allows such omission or failure, shall be punished for any such offense for which no penalty (other than a forfeiture) is provided by the act by a fine up to $10,000, imprisonment up to one year, or both, and in the case of a person previously convicted of violating the act, a fine up to $10,000, imprisonment up to two years, or both.

Section 502 of the act, 47 U.S.C. § 502, punishes willful and knowing violations of Federal Communication Commission regulations. Any person who willfully and knowingly violates any rule, regulation, restriction, or condition made or imposed

---

[4321] FCC Consumer Advisory: Protecting the Privacy of Your Telephone Calling Records, at http://www.fcc.gov/cgb/ consumerfacts/phoneaboutyou.html.

[4322] 47 C.F.R. §§ 64.2008.

[4323] 47 C.F.R. §§ 64.2009.

[4324] 47 C.F.R. §§ 64.2009(e).

[4325] In the Matter of Cbeyond Communications, LLC, 2006 FCC LEXIS 1902 (April 21, 2006), at http://www.fcc.gov/ eb/Orders/2006/DA-06-916A1.html.

[4326] See CRS Report RL34409, Selected Laws Governing the Disclosure of Customer Phone Records by Telecommunications Carriers, by Kathleen Ann Ruane, at 9.

by the Commission is, in addition to other penalties provided by law, subject to a maximum fine of $500 for each day on which a violation occurs.[4327]

Under section 503(b)(1) of the act, 47 U.S.C. § 503(b)(1), any person who is determined by the Commission to have willfully or repeatedly failed to comply with any provision of the act or any rule, regulation, or order issued by the Commission shall be liable to the United States for a civil money "forfeiture" penalty.[4328] Section 312(f)(1) of the act, 47 U.S.C. § 312(f)(1), defines "willful" as "the conscious and deliberate commission or omission of [any] act, irrespective of any intent to violate" the law. "Repeated" means that the act was committed or omitted more than once, or lasts more than one day. If the violator is a common carrier, section 503(b) authorizes the Commission to assess a forfeiture penalty of up to $130,000 for each violation or for each day of a continuing violation, except that the amount assessed for any continuing violation shall not exceed a total of $1,325,000 for any single act or failure to act.[4329] To impose such a forfeiture penalty, the Commission must issue a notice of apparent liability, and the person against whom the notice has been issued must have an opportunity to show, in writing, why no such forfeiture penalty should be imposed. The Commission will then issue a forfeiture if it finds by a preponderance of the evidence that the person has violated the act or a Commission rule.

[4327] 47 U.S.C. § 502.

[4328] 47 U.S.C. § 503(b)(1).

[4329] FCC Forfeiture Proceedings, Limits on the amount of forfeiture assessed, 47 C.F.R. Part 1.80(b).

Subchapter VI: Additional Procedures Regarding Certain Persons Outside the United States (50 U.S.C. §§ 1881-1881g)

P.L. 110-55, the Protect America Act of 2007: Modifications to the Foreign Intelligence Surveillance Act, RL34143 (August 23, 2007)

ELIZABETH B. BAZAN, CONGRESSIONAL RESEARCH SERV., P.L. 110-55, THE PROTECT AMERICA ACT OF 2007: MODIFICATIONS TO THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (2007), *available at* http://www.intelligencelaw.com/library/secondary/crs/pdf/RL34143_8-23-2007.pdf.

Order Code RL34143

August 23, 2007

Elizabeth B. Bazan
Legislative Attorney
American Law Division

Summary

On August 5, 2007, P.L. 110-55, the Protect America Act of 2007, was signed into law by President Bush, after having been passed by the Senate on August 3 and the House of Representatives on August 4. The measure, introduced by Senator McConnell as S. 1927 on August 1, makes a number of additions and modifications to the Foreign Intelligence Surveillance Act of 1978 (FISA), as amended, 50 U.S.C. §§ 1801 *et seq*., adds additional reporting requirements, and sunsets in 180 days. This report describes the provisions of P.L. 110-55, discusses its possible impact on and parallels to existing law, and summarizes the legislative activity with respect to S. 1927, H.R. 3356, and S. 2011.

The Foreign Intelligence Surveillance Act of 1978 was enacted in response both to the Committee to Study Government Operations with Respect to Intelligence Activities (Church Committee) revelations with regard to past abuses of electronic surveillance for national security purposes and to the somewhat uncertain state of the law on the subject. In creating a statutory framework for the use of electronic surveillance to obtain foreign intelligence information, the Congress sought to strike a balance between national security interests and civil liberties. Critical to an understanding of the FISA structure are its definitions of terms such as "electronic surveillance" and "foreign intelligence information." P.L. 110-55 limits the construction of the term "electronic surveillance" so that it does not cover surveillance directed at a person reasonably believed to be located

outside the United States. It also creates a mechanism for acquisition, without a court order under a certification by the Director of National Intelligence (DNI) and the Attorney General, of foreign intelligence information concerning a person reasonably believed to be outside the United States. The Protect America Act provides for review by the Foreign Intelligence Surveillance Court (FISC) of the procedures by which the DNI and the Attorney General determine that such acquisitions do not constitute electronic surveillance. In addition, P.L. 110-55 authorizes the Attorney General and the DNI to direct a person with access to the communications involved to furnish aid to the government to facilitate such acquisitions, and provides a means by which the legality of such a directive may be reviewed by the FISC petition review pool. A decision by a judge of the FISC petition review pool may be appealed to the Foreign Intelligence Surveillance Court of Review, and review by the U.S. Supreme Court may be sought by petition for writ of certiorari.

The report will be updated should subsequent developments require it.

Introduction

In response to concerns raised by the Director of National Intelligence, Admiral Mike McConnell, that the Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. §§ 1801 *et seq*., required modernization to meet the current intelligence needs of the nation, a number of bills were introduced in the Senate and the House of Representatives. Intense legislative activity with respect to proposed amendments to FISA in both bodies resulted in the enactment of the Protect America Act of 2007, P.L. 110-55 on August 5, 2007. The measure was introduced as S. 1927 by Senator McConnell, for himself and Senator Bond, on August 1, 2007. The bill was considered in the Senate on August 3, in conjunction with S. 2011, entitled The Protect America Act of 2007, introduced by Senator Levin, for himself and Senator Rockefeller. The Senate agreed by unanimous consent to an amendment to S. 1927 offered by Senator McConnell, for himself and Senator Bond, providing that sections 2, 3, 4, and 5 of the bill would sunset 180 days after its enactment.[4330] As amended, S. 1927 passed the Senate the same day.[4331] S. 2011 did not receive the requisite 60 votes, and was placed on the Senate calendar under general orders.[4332]

That evening, the House considered H.R. 3356, the Improving Foreign Intelligence Surveillance to Defend the Nation and the Constitution Act of 2007, introduced by Representative Reyes for himself, Representative Conyers, Representative Schiff, and Representative Flake. After a motion to suspend the

---

[4330] S.Amdt. No. 2649 to S. 1927.

[4331] Record Vote Number 309, 60-28 (August 3, 2007).

[4332] Record Vote Number 310, 43-45 (August 3, 2007).

rules and pass H.R. 3356 fell short of the required two-thirds vote of the Members[4333] on Friday night, the House took up S. 1927 the following day. At 10:19 p.m. Saturday night, August 4, the House passed S. 1927.[4334] It was signed by the President on August 5, 2007.

This report discusses the provisions of P.L. 110-55 and their impact on or relationship with the prior provisions of FISA.

Sec. 1. Short Title

Sec. 1 of S. 1927 states that the short title of the law is the Protect America Act of 2007.

Sec. 2. Additional Procedures for Authorizing Certain Acquisitions of Foreign Intelligence Information

Section 2 of the law contains its first substantive provisions. They are summarized in order below.

New Section 105A of FISA, "Clarification of Electronic Surveillance of Persons Outside the United States"

New Section 105A of FISA, as added by Section 2 of P.L. 110-55, states:

> *Nothing in the definition of electronic surveillance under section 101(f) shall be construed to encompass surveillance directed at a person reasonably believed to be located outside of the United States.*

Section 101(f) of FISA, 50 U.S.C. § 1801(f), sets forth the definition of "electronic surveillance" under the statute. It provides:

> *(f) "Electronic surveillance" means —*
> *(1) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person[4335] who is in the United States, if the*

[4333] The August 3, 2007, vote on the motion to suspend the rules and pass H.R. 3356 was 218 - 207 (Roll no. 821).

[4334] The bill was passed by the Yeas and Nays: 227 - 183 (Roll no. 836).

[4335] As defined in section 101(i) of FISA, 50 U.S.C. § 1801(i), "United States person" means a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 1101(a)(20) of Title 8), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a

contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes;
(2) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States, but does not include the acquisition of those communications of computer trespassers that would be permissible under section 2511(2)(i) of Title 18;
(3) the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States; or
(4) the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.

To what extent would the new section 105A affect the scope of "electronic surveillance" as defined in section 101(f) of FISA?

Absent the interpretation required by section 105A, two of the four definitions of "electronic surveillance" under section 101(f) of FISA, by their terms, appear to be broad enough to encompass electronic surveillance directed at a person abroad where the communications involved transcend U.S. borders.[4336] Subsections

---

corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in subsection (a)(1), (2), or (3) of this section.

"Foreign power," as defined in section 101(a)(1), (2), or (3), 50 U.S.C. § 1801(a)(1), (2), or (3), means:

(1) a foreign government or any component thereof, whether or not recognized by the United States;
(2) a faction of a foreign nation or nations, not substantially composed of United States persons;
(3) an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments[.]

[4336] Because new section 105A of FISA explicitly addresses electronic surveillance "directed at a person reasonably believed to be located outside the United States," it would not appear to affect subsection 101(f)(1), which deals with electronic surveillance of the contents of wire or radio communications acquired from an intentionally targeted U.S. person within the United States under specified circumstances. "Electronic surveillance" as defined in subsection 101(f)(3) of FISA

101(f)(2) and (f)(4) of FISA, on their face, appear to have the potential of reaching electronic surveillance of such communications targeted at a person outside the United States. In addition, it might be argued that the language of subsection 101(f)(4) might encompass the possibility of reaching some foreign to foreign communications in limited circumstances. This would suggest that, under FISA prior to the passage of section 105A of P.L. 110-55, some interceptions directed at a person abroad covered by the language of these subsections might have been regarded by the FISC as requiring court authorization.[4337]

In pertinent part, "electronic surveillance," as defined by subsection 101(f)(2), covers acquisition of the contents of wire communications to or from a person in the United States where the acquisition occurs within the United States and no party to the communication has consented to the interception. Unlike subsection 101(f)(1), there is no express requirement that the person in the United States be known, that he or she be United States person, or that he or she be intentionally targeted by the electronic surveillance.

To the extent that an electronic surveillance under subsection 101(f)(2) intercepts communications between persons in the United States, it would not be impacted by section 105A of FISA, as added by P.L. 110-55, nor would section 105A affect electronic surveillance targeted at a person within the United States. However, to the extent that the language in subsection 101(f)(2) might encompass interception of communications between a person in the United States and one or more parties outside the United States, where the surveillance is targeted at a person outside the United States, section 105A would seem to restrict the previous reach of the definition of "electronic surveillance" in section 101(f)(2).

Subsection 101(f)(4) defines "electronic surveillance" under FISA to include "the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication,[4338] under circumstances in which a person has a

---

involves the intentional acquisition of the contents of radio communications in specified circumstances where the sender and all the intended recipients to the communication are in the United States, so it would not seem to be impacted by new section 105A.

[4337] *See*, Greg Miller, Spy chief reveals details of operations, L.A. Times, August 23, 2007, *available at* [http://www.latimes.com/news/nationworld/nation/la-na-intel23aug23,0,6229712.story?coll=la-home-center].

[4338] Section 101(l) of FISA, 50 U.S.C. § 1801(l), defines "wire communication" to mean:

(l) "Wire communication" means any communication while it is being carried by a wire, cable, or other like connection furnished or operated by any person engaged as a common carrier in providing or operating such facilities for the transmission of interstate or foreign communications.

It does not have a separate definition of "radio communication." However, subsection 101(f)(4) of FISA appears to contemplate that communications can be transmitted using technologies other

reasonable expectation of privacy and a warrant would be required for law enforcement purposes." This subsection does not explicitly address the location of the parties to the communication or the location of the acquisition of the information involved. Thus, by its terms, it could conceivably be interpreted to cover some communications between parties in the United States, between a party in the United States and a party outside the United States, or between parties abroad, if the other requirements of the subsection were satisfied. The restrictions in this section are two-fold: the information must be acquired other than from a wire or radio communication; and the circumstances of the acquisition must be such that a person would have a reasonable expectation of privacy and a warrant would be required for law enforcement purposes. To the extent that "electronic surveillance" under subsection 101(f)(4) of FISA could have been or has been directed at a person or persons abroad, prior to the enactment of P.L. 110-55, new section 105A may also have the effect of limiting the scope of this subsection of the definition of "electronic surveillance" as it was previously interpreted.

New Section 105B of FISA, "Additional Procedure for Authorizing Certain Acquisitions Concerning Persons Located Outside the United States"

New section 105B(a) of FISA permits the Attorney General and the Director of National Intelligence, for periods of up to one year, to authorize acquisition of foreign intelligence information concerning persons reasonably believed to be outside the United States, if the Attorney General and the DNI determine, based on the information provided to them, that five criteria have been met. Under these criteria, the Attorney General and the DNI must certify that:

> *(1) there are reasonable procedures in place for determining that the acquisition of foreign intelligence information under this section concerns persons reasonably believed to be located outside*

---

wire or radio. For example, in Title III of the Omnibus Crime Control and Safe Streets Act, as amended, 18 U.S.C. § 2510(12), "electronic communication" includes other technologies. Under § 2510(12), this term is defined to mean:

any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include —

(A) any wire or oral communication;
(B) any communication made through a tone-only paging device;
(c) any communication from a tracking device (as defined in [18 U.S.C. § 3117]); or

(D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds[.]

the United States,[4339] and such procedures will be subject to review of the Court pursuant to section 105C of this Act;[4340]
(2) the acquisition does not constitute electronic surveillance;
(3) the acquisition involves obtaining the foreign intelligence information from or with the assistance of a communications service provider, custodian, or other person (including any officer, employee, agent, or other specified person of such service provider, custodian, or other person) who has access to communications, either as they are transmitted or while they are stored, or equipment that is being or may be used to transmit or store such communications;

[4339] The reporting requirements in Sec. 4 of the P.L. 110-55 require, in part, that the Attorney General report to the House Permanent Select Committee on Intelligence, the Senate Select Committee on Intelligence, and the House and Senate Judiciary Committees regarding incidents of non-compliance by an element of the Intelligence Community with guidelines or procedures for determining that the acquisition of foreign intelligence authorized by the DNI and the Attorney General under section 105B "concerns persons reasonably [sic?] to be outside the United States."

[4340] Section 105B(a)(1) states that the "procedures for determining that the acquisition of foreign intelligence information under this section concerns persons reasonably believed to be located outside the United States" are to be submitted to the FISC for review pursuant to section 105C of FISA. There appears to be some ambiguity in the language of section 105B, particularly as compared with section 105C, as to what the procedures cover and what procedures are to be submitted to the FISC. The phrasing of section 105B(a)(1) on its face, seems to require submission to the FISC only of "reasonable procedures . . . for determining that the acquisition of foreign intelligence information under this section concerns persons reasonably believed to be located outside the United States." This is the only mention in section 105B of procedures being submitted to the FISC. Thus, there is no mention in section 105B of creation of, or submission to the FISC of, procedures upon which the government bases its determination that the acquisition does not constitute electronic surveillance.
However, section 105C, by its terms, addresses only the submission by the Attorney General to the FISC of the procedures by which the government determines that acquisitions conducted pursuant to section 105B do not constitute electronic surveillance, making no mention of the procedures referred to in section 105B(a)(1). In light of this apparent inconsistency, it is unclear what review, if any, the FISC is intended to give the procedures for determining that the acquisition of foreign intelligence information under section 105B "concerns persons reasonably believed to be located outside the United States." It is also not made clear in the language of either section by whom the procedures to be reviewed by the FISC under section 105C are to be promulgated.

On the other hand, section 105A provides that the definition of "electronic surveillance" shall not be "construed to encompass surveillance directed at a person reasonably believed to be located outside of the United States." In light of this, it might be argued that the procedures by which the DNI and the Attorney General determine whether an acquisition of foreign intelligence information under section 105B concerns persons reasonably believed to be located outside the United States could be regarded as part of the FISC's analysis as to whether the procedures to determine that the acquisitions under 105B constitute electronic surveillance are clearly erroneous.

---

(4) a significant purpose of the acquisition is to obtain foreign intelligence information; and
(5) the minimization procedures to be used with respect to such acquisition activity meet the definition of minimization procedures under section 101(h).[4341]

Except in circumstances where immediate government action is required and there is not sufficient time to prepare a certification, the determination by the Attorney General and the DNI that these criteria have been satisfied must be in the form of a certification, under oath, supported by affidavit of appropriate officials in the national security field appointed by the President, by and with the advice and consent of the Senate, or the Head of any agency of the Intelligence Community. Where imminent government action is required, the determination must be reduced to a certification as soon as possible within 72 hours after the

---

[4341] Section 101(h) of FISA, 50 U.S.C. § 1801(h), defines "minimization procedures" for purposes of title I of FISA, dealing with electronic surveillance, to mean:

(h) "Minimization procedures", with respect to electronic surveillance, means —
(1) specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information;
(2) procedures that require that nonpublicly available information, which is not foreign intelligence information, as defined in subsection (e)(1) of this section, shall not be disseminated in a manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to understand foreign intelligence information or assess its importance;
(3) notwithstanding paragraphs (1) and (2), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes; and
(4) notwithstanding paragraphs (1), (2), and (3), with respect to any electronic surveillance approved pursuant to section 1802(a) of this title, procedures that require that no contents of any communication to which a United States person is a party shall be disclosed, disseminated, or used for any purpose or retained for longer than 72 hours unless a court order under section 1805 of this title is obtained or unless the Attorney General determines that the information indicates a threat of death or serious bodily harm to any person.

It may be noted that, while section 105B of FISA appears to be located in title I of FISA, which deals with electronic surveillance, the DNI and the Attorney General, under section 105B(a)(2) of FISA, are expressly required to certify that the acquisitions under section 105B do not constitute electronic surveillance. Similarly, the minimization procedures in section 101(h) of FISA, 50 U.S.C. § 1801(h), deal explicitly with minimization in the context of electronic surveillance, while, under subsection 105B(a)(5) of FISA, the DNI and the Attorney General must certify that "the minimization procedures to be used with respect to such acquisition[s] meet the definition of minimization procedures under section 101(h)." This seems likely to be intended to mean that the minimization procedures applicable to such acquisitions must set parallel standards to those applicable to electronic surveillance under the minimization procedures in section 101(h) of FISA, 50 U.S.C. § 1801(h).

determination is made.[4342] The certification need not identify specific facilities, places, premises, or property at which the acquisition will be directed.[4343]

A copy of a certification made under section 105B(a) must be transmitted under seal to the FISC as soon as practicable, there to be maintained under security measures established by the Chief Justice of the United States and the Attorney General, in consultation with the DNI. The copy of the certification must remain sealed unless needed to determine the legality of the acquisition involved.[4344]

Where a certification has been prepared, an acquisition under section 105B of FISA must be conducted in accordance with that certification and minimization procedures adopted by the Attorney General. If a certification has not yet been prepared because of inadequate time, the acquisition must comply with the oral instructions of the DNI and the Attorney General and the applicable minimization procedures.[4345] Section 105B(d) requires the DNI and the Attorney General must report their assessments of compliance with "such procedures"[4346] to the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence under section 108(a) of FISA, 50 U.S.C. § 1808(a).[4347]

[4342] Protect America Act of 2007, P.L. 110-55, Sec. 105B(a), 121 Stat. 552 (August 5, 2007) (hereinafter P.L. 110-55).

[4343] P.L. 110-55, Sec. 105B(b).

[4344] P.L. 110-55, Sec. 105B(c).

[4345] P.L. 110-55, Sec. 105B(d).

[4346] In the context of the subsection 105B(d), the reference to "such procedures" might be seen to be susceptible of two possible interpretations. Perhaps the more likely and more limited interpretation would be that this may be a reference to the applicable minimization procedures referenced earlier in the subsection. Alternatively, a more expansive view might interpret this as a reference to the applicable minimization procedures plus the relevant certification, including the "reasonable procedures in place for determining that the acquisition of foreign intelligence information under this section concerns persons reasonably believed to be located outside the United States," or oral instructions regarding the acquisition at issue.

[4347] Section 108 of FISA, 50 U.S.C. § 1808, provides:

§ 1808. Report of Attorney General to Congressional committees; limitation on authority or responsibility of information gathering activities of Congressional committees; report of Congressional committees to Congress

(a)

(1) On a semiannual basis the Attorney General shall fully inform the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence, and the Committee on the Judiciary of the Senate, concerning all electronic surveillance under this subchapter [title I of FISA, 50 U.S.C. §§ 1801 et seq.]. Nothing in this subchapter [title I of FISA] shall be deemed to limit the authority and responsibility of the appropriate committees of each House of Congress to obtain such information as they may need to carry out their respective functions and duties.

(2)

Each report under the first sentence of paragraph (1) shall include a description of —

In connection with an acquisition authorized under section 105B, the DNI and the Attorney General may issue a directive to a person to immediately provide the government with all information, facilities, and assistance needed to accomplish the acquisition in a manner which will protect the secrecy of the acquisition and minimize interference with the services provided by that person to the target of the acquisition.[4348] The government must compensate the person furnishing such aid at the prevailing rate.[4349] Any records that person wishes to keep relating to the acquisition or the aid provided must be maintained under security procedures approved by the DNI and the Attorney General.[4350] P.L. 110-55 bars any cause of action in any court against any person for providing information, facilities or assistance in accordance with a directive under this section.[4351] If a person receiving such a directive fails to comply therewith, the FISC, at the Attorney General's request, shall issue an order to compel such compliance if the

---

(A) the total number of applications made for orders and extensions of orders approving electronic surveillance under this subchapter where the nature and location of each facility or place at which the electronic surveillance will be directed is unknown;
(B) each criminal case in which information acquired under this chapter has been authorized for use at trial during the period covered by such report; and
(C) the total number of emergency employments of electronic surveillance under section 1805(f) of this title and the total number of subsequent orders approving or denying such electronic surveillance.
(b) On or before one year after October 25, 1978, and on the same day each year for four years thereafter, the Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence shall report respectively to the House of Representatives and the Senate, concerning the implementation of this chapter. Said reports shall include but not be limited to an analysis and recommendations concerning whether this chapter should be (1) amended, (2) repealed, or (3) permitted to continue in effect without amendment.

It may be noted that the reporting requirements under subsection 108(a) of FISA deal explicitly with electronic surveillance under FISA, and impose responsibility only upon the Attorney General. While section 105B has been added to title I of FISA, which deals with electronic surveillance, the DNI and the Attorney General, under subsection 105B(a)(2) are required to certify, with respect to each acquisition under section 105B, that such acquisition "does not constitute electronic surveillance." The reporting requirement in section 105B(d) may be intended to direct the DNI and the Attorney General to include their assessments with respect to the procedures involved in the semiannual report of the Attorney General required by section 108(a), or it may be intended to require that the DNI and the Attorney General fully inform the House and Senate Intelligence Committees of their assessments on a semi-annual basis.

[4348] P.L. 110-55, Sec. 105B(e)(1).

[4349] P.L. 110-55, Sec. 105B(f).

[4350] P.L. 110-55, Sec. 105B(e)(2).

[4351] P.L. 110-55, Sec. 105B(l).

court finds that the directive was issued in accordance with section 105B(e) and is otherwise lawful.[4352]

A person receiving a directive under section 105B(e) may challenge its legality by filing a petition before the petition review pool of the FISC.[4353] Under subsection 105B(h)(1)(B) as written, the presiding judge of the Foreign Intelligence Surveillance Court of Review (Court of Review)[4354] shall assign a petition filed

---

[4352] P.L. 110-55, Sec. 105B(g). Service of process may be made upon such person in any judicial district in which he or she is found.

[4353] Section 103(e)(1) of FISA, 50 U.S.C. § 1803(e)(1), established this pool. As amended by Sec. 5 of P.L. 110-55, section 103(e) provides:

(e)
(1) Three judges designated under subsection (a) of this section who reside within 20 miles of the District of Columbia, or, if all of such judges are unavailable, other judges of the court established under subsection (a) of this section as may be designated by the presiding judge of such court, shall comprise a petition review pool which shall have jurisdiction to review petitions filed pursuant to section 105B(h) or 501(f)(1) of [FISA].

(2) Not later than 60 days after March 9, 2006, the court established under subsection (a) of this section shall adopt and, consistent with the protection of national security, publish procedures for the review of petitions filed pursuant to section 105B(h) or 501(f)(1) of [FISA] by the panel established under paragraph (1). Such procedures shall provide that review of a petition shall be conducted in camera and shall also provide for the designation of an acting presiding judge. [Emphasis added.]

Subsection 103(a) requires the Chief Justice of the United States to publicly designate 11 U.S. district court judges from seven of the United States judicial circuits to become the FISC judges. The reference to section 501(f)(1) of FISA, 50 U.S.C. § 1861(f)(1), may be intended to be a reference to section 501(f), 50 U.S.C. § 1861(f). Section 501(f), as added to FISA by P.L. 109-177, § 106(f), was rewritten by P.L. 109-178, § 3. Current section 501(f)(1) of FISA contains two subsections, defining the terms "production order" and "nondisclosure order," respectively, for purposes of section 501.

[4354] Section 105B(h)(1)(B) states that the "presiding judge designated pursuant to section 103(b) shall assign a petition filed under subparagraph (a) to one of the judge serving in the pool established by section 103(e)(1)." This may be intended to refer to the presiding judge of the FISC designated pursuant to section 103(a), rather than the presiding judge of the Foreign Intelligence Surveillance Court of Review designated pursuant to section 103(b). The petition review pool established by section 103(e)(1) is made up of FISC judges. See footnote 24, supra. Section 501(f)(2)(A)(ii) provides that, when a petition under that section is filed with the petition review pool of the FISC, "the presiding judge" shall immediately assign it to one of the judges in the pool. The rules, effective May 5, 2006, promulgated by the FISC under section 103(e)(2) of FISA are more explicit. Under title III, sections 8 and 9, of the "Procedures for review of Petitions filed pursuant to Section 501(f) of the Foreign Intelligence Surveillance Act of 1978, As Amended," the "Presiding Judge of the Foreign Intelligence Surveillance Court," where available, assigns petitions received under section 501(f) of FISA to one of the FISC judges in the petition review pool. If the Presiding Judge of the FISC is unavailable, the local FISC judge with the most seniority, other than the Presiding Judge, becomes Acting Presiding Judge, and assigns the petition to an FISC judge in the petition review pool. If no local judge is available, the most senior

with the petition review pool to one of the FISC judges in the pool. The assigned judge must conduct an initial review of the directive within 48 hours after the assignment. If he or she determines that the petition is frivolous, the petition is immediately denied and the directive or that portion of the directive that is the subject of the petition is affirmed. If the judge does not find the petition frivolous, he or she has 72 hours in which to consider the petition and provide a written statement for the record of the reasons for any determination made. A petition to modify or set aside a directive may only be granted if the judge finds that the directive does not meet the requirements of section 105B or is otherwise unlawful. Otherwise the judge must immediately affirm the directive and order its recipient to comply with it. A directive not explicitly modified or set aside remains in full effect.[4355] Within seven days of the assigned judge's decision, the government or a recipient of the directive may petition the Foreign Intelligence Surveillance Court of Review for review of that decision. The Court of Review must provide a written statement on the record of the reasons for its decision. The government or any recipient of the directive may seek review of the decision of the Court of Review by petition for a writ of certiorari to the U.S. Supreme Court.[4356] All judicial proceedings under this section are to be concluded as expeditiously as possible.[4357]

All petitions under this section are filed under seal. Upon request of the government in any proceeding under this section, the court shall review ex parte and in camera any government submission or portion of a submission which may contain classified information.[4358] The record of all proceedings, including petitions filed, orders granted, and statements of reasons for decision, must be maintained under security measures established by the Chief Justice of the United States in consultation with the Attorney General and the DNI.[4359] A directive made or an order granted under this section must be retained for at least ten years.[4360]

Effect on or parallels to existing law.

FISC judge who is reasonably available becomes the Acting Presiding Judge, and makes the assignment of the petition.

[4355] P.L. 110-55, Sec. 105B(h).

[4356] P.L. 110-55, Sec. 105B(i).

[4357] P.L. 110-55, Sec. 105B(j).

[4358] P.L. 110-55, Sec. 105B(k).

[4359] P.L. 110-55, Sec. 105B(j).

[4360] P.L. 110-55, Sec. 105B(m).

Section 105B is a new section added to title I of FISA, 50 U.S.C. §§ 1801 *et seq*. It differs from the other provisions of title I of FISA in that it does not deal with electronic surveillance, but rather with acquisitions that do not constitute electronic surveillance. Because section 105B does not specify where such acquisitions may occur or from whom, it appears that such foreign intelligence information concerning persons reasonably believed to be outside the United States may be acquired, at least in part, from persons, including U.S. persons, who are located within the United States.[4361]

Similar to electronic surveillance under section 102 of FISA, 50 U.S.C. § 1802, which may be authorized for up to one year by the President, through the Attorney General, without a court order if the Attorney General certifies in writing under oath that certain requirements are satisfied,[4362] acquisitions under section 105B of FISA, may be authorized by the DNI and the Attorney General without a court order if they certify in writing under oath that certain criteria are met. However, section 105B has no parallel to section 102(a)(1)(B)'s requirement

---

[4361] It may be noted that the description of an acquisition under section 105B of FISA appears broad enough to encompass future collection of phone calling records for pattern analysis, but does not appear intended to address any past use of such investigative techniques. Cf., Hepting v. AT&T Corp., 439 F. Supp. 2d. 974 (N.D. Cal. 2006); In re: National Security Agency Telecommunications Records Litigation, MDL No. 06-1791-VRW (March 13, 2007) (stipulation and order staying all cases except Hepting against AT&T Defendants); Hepting v. United States, Nos. 06-80109, 06-80110 (9th Cir. 2006) (order granting appeal).

[4362] Section 102(a), 50 U.S.C. § 1802(a) provides:

(a)(1) Notwithstanding any other law, the President, through the Attorney General, may authorize electronic surveillance without a court order under this subchapter to acquire foreign intelligence information for periods of up to one year if the Attorney General certifies in writing under oath that —

(A) the electronic surveillance is solely directed at —
(i) the acquisition of the contents of communications transmitted by means of communications used exclusively between or among foreign powers, as defined in section 1801(a)(1), (2), or (3) of this title; or
(ii) the acquisition of technical intelligence, other than the spoken communications of individuals, from property or premises under the open and exclusive control of a foreign power, as defined in section 1801(a)(1), (2), or (3) of this title;

(B) there is no substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person is a party; and

(C) the proposed minimization procedures with respect to such surveillance meet the definition of minimization procedures under section 1801(h) of this title; and if the Attorney General reports such minimization procedures and any changes thereto to the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence at least thirty days prior to their effective date, unless the Attorney General determines immediate action is required and notifies the committees immediately of such minimization procedures and the reason for their becoming effective immediately.

that "there is no substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person is a party."

Similar to section 105B(d)'s reporting requirements, section 102(a)(2) requires electronic surveillance under that section to be carried out in accordance with the Attorney General's certification and applicable minimization requirements, and directs the Attorney General to assess compliance with "such procedures" and report his assessments to the House and Senate intelligence committees under the provisions of section 108(a) of FISA.

Section 102(a)(4), which permits the Attorney General to direct a specified communication common carrier to provide information, facilities, or technical assistance to the government needed to carry out the electronic surveillance involved and to compensate that communication common carrier at the prevailing rate for its aid, is structurally similar to section 105B(e) and (f). However, subsections 105B(e) and (g)-(i) permit the Attorney General and the DNI to direct "a person," rather than a "specified communication common carrier," to "immediately" furnish such aid; provide authority for the Attorney General to seek the aid of the FISC to compel compliance with such a directive; give the recipient of the directive a right to challenge the legality of the directive before the petition review pool of the same court; and permit both the government and the recipient of the directive to appeal that court's decision. The authority to challenge the legality of such a directive and to appeal the decision appears modeled, to some degree, after the process set forth in section 501(f) of FISA, 50 U.S.C. § 1861(f), dealing with challenges to the legality of production and nondisclosure orders.

Unlike electronic surveillance pursuant to a court order sought under section 104 of FISA, 50 U.S.C. § 1804, and authorized under section 105 of FISA, 50 U.S.C. § 1805, where the government provides the FISC with specific categories of substantive information about the electronic surveillance involved upon which the court can base its determinations; the government submits certain procedures[4363] for review to the FISC, but does not provide the court with substantive information about the acquisitions themselves.

Sec. 3. Submission to Court Review and Assessment of Procedures

Section 3 of the act creates a new section 105C of FISA, creating a review process for the procedures under which the government determines that acquisitions of foreign intelligence information from persons reasonably believed to be located outside the United States do not constitute electronic surveillance.

[4363] Compare section 105B(a)(1) with section 105C.

New Section 105C of FISA. "Submission to Court Review of Procedures"

Subsection 105C(a) requires the Attorney General, within 120 days of enactment of the act,[4364] to submit to the FISC the procedures by which the government determines that acquisitions conducted pursuant to section 105B of the act do not constitute electronic surveillance.[4365] The procedures are to be updated and submitted to the FISC annually. Within 180 days after enactment, the FISC must assess whether the government's determination under section 105B(1) of FISA that the procedures are "reasonably designed to ensure that acquisitions conducted pursuant to section 105B do not constitute electronic surveillance"[4366] is clearly erroneous.[4367]

If the FISC deems the government's determination not clearly erroneous, the court must enter an order approving the continued use of the procedures. On the other hand, if the government's determination is found to be clearly erroneous, new procedures must be submitted with 30 days or any acquisitions under section 105B implicated by the FISC order must cease.[4368] Any order issued by the FISC under subsection 105C(c) may be appealed by the government to the Foreign Intelligence Surveillance Court of Review. If the Court of Review finds the FISC order was properly entered, the government may seek U.S. Supreme

---

[4364] Under Sec. 6(a) of the act, except as otherwise provided, the amendments made by the act are to take effect immediately after the date of enactment of the act. Sec. 105C(a) states that it will take effect within 120 days of the effective date of the act. For purposes of Sec. 105C(a), that would be 120 days after enactment.

[4365] Section 105B(1) on its face refers only to "reasonable procedures in place for determining that the acquisition of foreign intelligence information under this section concerns persons reasonably believed to be located outside the United States," and requires "such procedures [to be] subject to review of the [FISC] pursuant to section 105C of this Act." See footnote 11, supra, for further discussion of the seeming ambiguities in the statutory language of sections 105B and 105C with respect to the procedures to be reviewed by the FISC.

[4366] There appears to be some ambiguity regarding the procedures referenced in section 105B(a) and section 105C of FISA. Section 105B permits the DNI and the Attorney General to authorize acquisition of foreign intelligence information concerning persons reasonably believed to be outside the United States if the DNI and the Attorney General determine, based upon information provided to them, "that — (a)(1) there are reasonable procedures in place for determining that the acquisition of foreign intelligence information under this section concerns persons reasonably believed to be located outside the United States, and such procedures will be subject to review of the Court pursuant to section 105C of this Act[.]" However, section 105C requires the Attorney General to submit to the FISC "the procedures by which the Government determines that acquisitions conducted pursuant to section 105B do not constitute electronic surveillance." For further discussion, see 15, supra.

[4367] Section 105C(b) of FISA, as added by P.L. 110-55, Sec. 3.

[4368] Section 105C(c) of FISA, as added by P.L. 110-55, Sec. 3.

Court review through a petition for a writ of certiorari.[4369] Any acquisitions affected by the FISC order at issue may continue throughout the review process.

Comparison of this provision with court review.

The section 105C procedure review process is new and does not appear to have a parallel in the other provisions of FISA.

Other possible effects of new sections 105A, 105B, and 105C.

The Terrorist Surveillance Program has been characterized as involving "intercepts of contents of communications where one . . . party to the communication is outside the United States" and the government has "a reasonable basis to conclude that one party to the communication is a member of al Qaeda, affiliated with al Qaeda, or a member of an organization affiliated with al Qaeda, or working in support of al Qaeda."[4370] In a letter from the Attorney General to Senator Leahy and Senator Specter on January 17, 2007, the Attorney General indicated that, based upon classified orders issued by a judge of the Foreign Intelligence Surveillance Court (FISC), electronic surveillances previously carried out under the Terrorist Surveillance Program would thereafter be under the court's supervision. His letter stated, in part:

> *I am writing to inform you that on January 10, 2007, a Judge of the Foreign Intelligence Surveillance Court issued orders authorizing the Government to target for collection international communications into or out of the United States where there is probable cause to believe that one of the communicants is a member or agent of al Qaeda or an associated terrorist organization. As a result of these orders, any electronic surveillance that was occurring as part of the Terrorist Surveillance Program will now be conducted subject to the approval of the Foreign Intelligence Surveillance Court. . .* [4371]

[4369] Section 105C(d) of FISA, as added by P.L. 110-55, Sec. 3. If the Court of Review affirms the FISC order, the Court of Review must immediately prepare a written statement of each of the reasons for its decision. Should the government file a certiorari petition, that written record would be transmitted under seal to the U.S. Supreme Court.

[4370] See Press Release, White House, Press Briefing by Attorney General Alberto Gonzales and General Michael Hayden, Principal Deputy Director for National Intelligence (December 19, 2005).

[4371] 153 *Cong. Rec.* S646-S647 (January 17, 2007) (Letter of Attorney General Alberto Gonzales to the Chairman and Ranking Member of the Senate Judiciary Committee ordered printed, without objection, in the *Record* during Senator Leahy's remarks on the FISA Program).

A question may arise as to whether new section 105A's interpretation of the definition of "electronic surveillance" under FISA, might impact the FISC's jurisdiction over some or all of the interceptions to which the Attorney General referred. Under section 103(a) of FISA, 50 U.S.C. § 1803(a):

> *The Chief Justice of the United States shall publicly designate 11 district court judges from seven of the United States judicial circuits of whom no fewer than 3 shall reside within 20 miles of the District of Columbia who shall constitute a court which shall have jurisdiction to hear applications for and grant orders approving electronic surveillance anywhere within the United States under the procedures set forth in this chapter, except that no judge designated under this subsection shall hear the same application for electronic surveillance under this chapter which has been denied previously by another judge designated under this subsection. . . .*

Section 102(b) of FISA, 50 U.S.C. § 1802(b), provides that:

> *Applications for a court order under [title I of FISA, 50 U.S.C. §§ 1801 et seq.] are authorized if the President has, by written authorization, empowered the Attorney General to approve applications to the court having jurisdiction under section 1803 of this title, and a judge to whom an application is made may, notwithstanding any other law, grant an order, in conformity with section 1805 of this title, approving electronic surveillance of a foreign power or an agent of foreign power for the purpose of obtaining foreign intelligence information, except that the court shall not have jurisdiction to grant any order approving electronic surveillance directed solely as described in paragraph (1)(A) of subsection (a) of this section unless such surveillance may involve the acquisition of communications of any United States person.*

The answer to the jurisdictional question raised above would seem to depend on whether those interceptions were directed at the communications of a person reasonably believed to be located outside the United States. If so, then, by virtue of section 105A, such interceptions would not be construed to fall within the definition of "electronic surveillance" under FISA, and therefore a review of the underpinnings of such interceptions would not be within the FISC's jurisdiction in connection with an application to authorize electronic surveillance. If treated instead as acquisitions under new section 105B of FISA, then the FISC would seem to be limited to reviewing, under a clearly erroneous standard, the general procedures under which the Director of National Intelligence (DNI) and the Attorney General would make determinations that acquisitions did not constitute

electronic surveillance;[4372] and judges of the FISC petition review pool would have jurisdiction to consider petitions challenging the legality of directives to persons to furnish aid to the government to accomplish those acquisitions.[4373]

Implicit in the previous discussion is the question what impact, if any, any possible narrowing of the interpretation of the definition of "electronic surveillance" under FISA might have upon the scope of "acquisitions" under new section 105B of FISA. In other words, if an interception of communications directed toward a person reasonably believed to be located outside the United States does not constitute "electronic surveillance" for purposes of FISA, regardless of where the other parties to the communication may be located or whether some or all of those other parties may be U.S. persons, could some or all such interceptions be deemed "acquisitions" under the provisions of section 105B?

For this to be the case, it would appear that the interception would have to be authorized by the DNI and the Attorney General under section 105B of FISA to acquire foreign intelligence information concerning persons reasonably believed to be outside the United States, and would have to satisfy the five criteria set forth in section 105B(a), including the use of minimization procedures.[4374] If these requirements are met, then it appears that some communications to which U.S. persons located within the United States might be parties could be intercepted for periods of up to one year without a court order under section 105B.

This contrasts markedly with the detailed information to be provided by the government to the FISC in an application for a court order for electronic surveillance under section 104 of FISA, 50 U.S.C. § 1804,[4375] and the level of FISC

[4372] Section 105C(a) of FISA, as added by P.L. 110-55, Sec. 3.

[4373] Section 105B(h) of FISA, as added by P.L. 110-55, Sec. 2.

[4374] Section 105B(a)(5) of FISA, as added by Sec. 2 of P.L. 110-55. For further discussion of minimization procedures in section 105B(a)(5), see footnote 12, supra, and accompanying text. Under section 105(f) of FISA, 50 U.S.C. § 1805(f), in approving an application for electronic surveillance under FISA, an FISC judge must find, in part, that the proposed minimization procedures applicable to that surveillance meet the definition of minimization procedures under section 101(h) of FISA, 50 U.S.C. § 1801(h). In authorizing an acquisition under section 105B, the DNI and the Attorney General must certify in writing under oath, in part, that "the minimization procedures to be used with respect to such acquisition activity meet the definition of minimization procedures under section 101(h)."

[4375] Section 104 of FISA, 50 U.S.C. § 1804, which deals with application for FISC court orders authorizing electronic surveillance, requires eleven categories of detailed information to be submitted by a federal office in writing under oath or affirmation to an FISC judge. Each application must be approved by the Attorney General based upon his finding that the application satisfies the criteria and requirements set forth in title I of FISA. Section 105 of FISA, 50 U.S.C. § 1805, sets out the findings that a FISC judge must make in approving such an application.

review provided for such applications. To the extent that new section 105A circumscribes the previous interpretation of "electronic surveillance" as defined under section 101(f) of FISA, 50 U.S.C. § 1801(f), it could be argued that this might significantly diminish the degree of judicial review to which such interceptions might have heretofore been entitled. On the other hand, if the interpretation of the definition of "electronic surveillance" contemplated in new section 105A of FISA is consistent with prior practice, then this concern with respect to section 105A's impact would appear to be eliminated.

A somewhat closer parallel might be drawn between the statutory structure for acquisitions contemplated in section 105B and that for electronic surveillance under section 102 of FISA, 50 U.S.C. § 1802. The latter section permits the President, through the Attorney General, to authorize electronic surveillance for up to one year without a court order, if the Attorney General certifies in writing under oath that the electronic surveillance is solely directed at the acquisition of the contents of communications transmitted by means of communications used exclusively between or among foreign powers, as defined in section 1801(a)(1), (2), or (3) of this title;[4376] or the acquisition of technical intelligence, other than the spoken communications of individuals, from property or premises under the open and exclusive control of such a foreign power. In addition, the Attorney General must certify that there is no substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person is a party; and that the proposed minimization procedures with respect to such surveillance meet the definition of minimization procedures under section 1801(h) of this title; and he must comply with reporting requirements regarding those minimization procedures.

Subsection 102(b) of FISA denies the FISC jurisdiction to grant any order approving electronic surveillance directed solely at the acquisition of communications used exclusively between or among such foreign powers or the acquisition of such technical intelligence from property or premises under the exclusive and open control of such foreign powers, *unless such surveillance may involve the acquisition of communications of any United States person*. Section 105B provides the FISC no similar jurisdiction if an acquisition involves the communications of a United States person. Again, if the interpretation of the definition of "electronic surveillance" contemplated in new section 105A of FISA is consistent with prior practice, then this concern regarding section 105A's effect would appear to be eliminated.

To the extent that any intentional interceptions of communications which were previously deemed to be covered by the definition of "electronic surveillance" under FISA are now excluded from that definition, another question which may

---

[4376] *See* footnote 6, supra, for the definition of "foreign power" under section 101(a)(1), (2), or (3) of FISA.

arise is whether any of those interceptions may now be found to fall within the general prohibition against intentional interception of wire, oral, or electronic communications under Title III of the Omnibus Crime Control and Safe Streets Act of 1968, as amended, 18 U.S.C. § 2511. Under 18 U.S.C. § 2511(2)(f), "electronic surveillance," as defined in section 101 of the Foreign Intelligence Surveillance Act, is an exception to this general prohibition.[4377] If such interceptions were deemed to violate 18 U.S.C. § 2511, then the intentional use or disclosure of the contents of such communications, knowing that the information was obtained through the interception of a wire, oral, or electronic communication in violation of 18 U.S.C. § 2511 would also be prohibited under that section.

Sec. 4. Reporting to Congress

Section 4 of P.L. 110-55 requires the Attorney General to inform the Senate Select Committee on Intelligence, the House Permanent Select Committee on Intelligence, the Senate Judiciary Committee and the House Judiciary Committee semi-annually concerning acquisitions "under this section"[4378] during the previous six-month period. Each report is to include descriptions of any incidents of noncompliance with a directive issued by the DNI and the Attorney General under section 105B, including noncompliance by an element of the Intelligence Community with guidelines or procedures for determining that "the acquisition of foreign intelligence authorized by the Attorney General and the [DNI] concerns persons reasonably to be outside the United States,"[4379] and incidents of noncompliance by a specified person to whom a directive is issued under section 105B. The report is also required to include the number of certifications and directives issued during the reporting period.

Sec. 5. Technical Amendment and Conforming Amendments

Section 5(a)(1) and (a)(2) make technical amendments to section 103(e)(1) and (2) of FISA, 50 U.S.C. § 1803(e)(1) and (2), to reflect the jurisdiction of the FISC

[4377] If there are any types of intentional interceptions of communications previously covered by FISA's definition of electronic surveillance, which may now be prohibited under 18

U.S.C. § 2511, this, in turn, might give rise to the question whether, if the President were to carry out such interceptions under an assertion of his constitutional authority under Article II, the application of Title III's prohibition to those interceptions would be found by a court to be unconstitutional, or whether the application of this prohibition to such interceptions would withstand constitutional scrutiny. Cf., In re Sealed Case, 310 F. 3d 717, 742, 746 (U.S. Foreign Intell. Surveillance Ct. Rev. 2002).

[4378] This appears to be a reference to section 105Bof FISA, as added by P.L.110-55, Sec. 2.

[4379] This may be intended to read "the acquisition of foreign intelligence information authorized by the Attorney General and Director of National Intelligence concerns persons reasonably believed to be outside the United States." (Emphasis added.)

petition review pool over petitions under section 105B(h) of FISA, dealing with challenges to the legality of directives issued under section 105B(e) of FISA to a person by the Attorney General and the DNI, and over petitions under section 501(f)[4380] of FISA, 50 U.S.C. § 1861, dealing with challenges to production orders or nondisclosure orders issued by the FISC under section 501(c) of FISA, 50 U.S.C. § 1861(c).

Section 5(b) makes conforming amendments to the table of contents of the first "section"[4381] of FISA, 50 U.S.C. § 1801 et seq., to reflect the additions of new sections 105A, 105B, and 105C of FISA.

Sec. 6. Effective Date; Transition Procedures

Effective Date

Under Section 6(a) of P.L. 110-55, the amendments to FISA made in the act are to take effect immediately after its enactment except as otherwise provided.

Transition Procedures

Section 6(b) of P.L. 110-55 provides that any order issued under FISA in effect on the date of enactment of P.L. 110-55 (August 5, 2007) shall remain in effect until the date of expiration of the order, and, at the request of the applicant for the order, the FISC shall reauthorize the order as long as the facts and circumstances continue to justify its issuance under FISA as in effect the day before the applicable effective date of P.L.110-55. This appears to refer to orders and applications for orders under FISA authorizing electronic surveillance,[4382] physical searches,[4383] pen registers or trap and trace devices,[4384] or production of tangible things and related nondisclosure orders.[4385]

[4380] Sec. 5(a)(1) and (2) of the act refer here to section "501(f)(1)," rather than to section "501(f)," of FISA. The reference to section 501(f)(1) of FISA, 50 U.S.C. § 1861(f)(1), may be intended to be a reference to section 501(f), 50 U.S.C. § 1861(f). Section 501(f), as added to FISA by P.L. 109-177, § 106(f), was rewritten by P.L. 109-178, § 3. Current section 501(f)(1) of FISA contains two subsections, defining the terms "production order" and "nondisclosure order," respectively, for purposes of section 501. For further discussion, see footnote 24, *supra*.

[4381] This appears to be intended to refer to the title I of FISA, dealing with electronic surveillance.

[4382] Applications for electronic surveillance are covered by section 104 of FISA, 50 U.S.C. § 1804, while orders authorizing such surveillance are addressed in section 105 of FISA, 50 U.S.C. § 1805. These sections were not amended by P.L.110-55.

[4383] Applications for physical searches are addressed in sections 302(b) and 303 of FISA, 50 U.S.C. §§ 1822(b) and 1823, while orders authorizing such physical searches are addressed in section 304 of FISA, 50 U.S.C. § 1824. These sections were not amended by P.L.110-55.

[4384] Applications for installation and use of pen registers and trap and trace devices are addressed in subsections 402(a), (b), and (c) of FISA, 50 U.S.C. § 1842(a), (b), and (c); while orders

Section 6(b) provides further that the government may also file new applications and the FISC shall enter orders granting such applications pursuant to FISA, as long as the application meets the requirements set forth in FISA as in effect on the day before the applicable effective date of P.L. 110-55. This seems to indicate that preexisting authorities under FISA remain available in the wake of P.L. 110-55's enactment. At the applicant's request, the FISC shall extinguish any extant authorizations to conduct electronic surveillance or physical searches pursuant to FISA. Any surveillance conducted pursuant to an order entered under subsection 6(b) of P.L. 110-55 is to be subject to the provisions of FISA as in effect before the effective date of P.L. 110-55.

Under Section 6(c) of P.L. 110-55, sections 2, 3, 4, and 5 of that act sunset 180 days after the date of enactment of the act, except as provided in section 6(d). Under section 6(d), any authorizations for acquisition of foreign intelligence information or directives issued pursuant to those authorizations issued under section 105B shall remain in effect until their expiration. Section 6(d) also provides that such acquisitions shall be governed by the applicable amendments made to FISA by P.L. 110-55, and shall not be deemed to constitute electronic surveillance as that term is defined in section 101(f) of FISA.[4386]

---

authorizing installation and use of such pen registers and trap and trace devices are covered by subsection 402(d), 50 U.S.C. § 1842(d). No amendments to these subsections were made in P.L. 110-55.

[4385] Applications for orders "requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution" are addressed in subsections 501(a) and (b) of FISA, 50 U.S.C. § 1861(a) and (b). Production orders are covered in subsection 501(c) of FISA, 50 U.S.C. § 1861(c), while related nondisclosure orders are addressed in subsection 501(d) of FISA, 50 U.S.C. § 1861(d). These subsections were not amended by P.L. 110-55.

[4386] The provisions in section 6(c) and (d) were added by Senate amendment 2649 to S. 1927, proposed by Senator McConnell, for himself and Senator Bond. It was agreed to by unanimous consent on August 3, 2007. As amended, the bill passed the Senate by Yea-Nay vote, 60-28 (Record Vote Number 309), 153 *Cong. Rec.* S10861-S10872 (August 3, 2007).

Subchapter VII: Protection of Persons Assisting the Government (50 U.S.C. §§ 1885-1885c)

Retroactive Immunity Provided by the FISA Amendments Act of 2008, RL34600 (July 25, 2008).

EDWARD C. LIU, CONG. RESEARCH SERV., RETROACTIVE IMMUNITY PROVIDED BY THE FISA AMENDMENTS ACT OF 2008 (2008), *available at* http://www.intelligencelaw.com/library/secondary/crs/pdf/RL34600_7-25-2008.pdf.

Order Code RL34600
July 25, 2008

Edward C. Liu
Legislative Attorney
American Law Division

Summary

On July 10, 2008, P.L. 110-261, entitled the FISA Amendments Act of 2008, was signed into law. Although many of the changes enacted by the FISA Amendments Act were controversial, one particularly contentious issue was whether to grant retroactive immunity to telecommunications providers that may have facilitated warrantless surveillance by the federal government under a Terrorist Surveillance Program between 2001 and 2007. Proponents of retroactive immunity argued that it was necessary to assure private cooperation with critical intelligence investigations. On the other hand, opponents of retroactive immunity argued that its inclusion undermined the statutory penalties that were designed to deter unlawful intrusions into individual liberties. This report discusses the various retroactive immunity mechanisms that were proposed to be included in the FISA Amendments Act, one of which was ultimately adopted, and their likely effect on lawsuits facing telecommunications providers.

Retroactive immunity is more than simply protection from liability; it can also act as protection from the cost of litigation. Without retroactive immunity, many legal issues would need to be addressed, possibly at great expense, in order to resolve these lawsuits. The plaintiffs would need to show that the actions of the defendants were not lawful. The Bush Administration's theory of inherent wiretapping ability might need to be litigated. Additionally, the applicability of the state secrets privilege to these cases might be the subject of litigation.

As enacted, the FISA Amendments Act lays out a procedure for the Attorney General to bring about the dismissal of lawsuits alleging unlawful participation in the Terrorist Surveillance Program (TSP). In order for a suit to be dismissed by a court, the Attorney General must certify that the defendant provided assistance

in connection with the TSP and was given written assurances that the program was authorized by the President and determined to be lawful. The Attorney General could also certify that the alleged assistance was not in fact provided by the defendant. All parties are permitted to submit documents and arguments relevant to dismissal which the court may consider. Dismissal is only proper if the court finds, based upon its review, that the Attorney General's certification is supported by "substantial evidence."

Introduction

In November of 2007, the House of Representatives passed H.R. 3773, the RESTORE Act, which would have amended several provisions of the Foreign Intelligence Surveillance Act (FISA). In February of 2008, the Senate passed an amendment in the nature of a substitute to H.R. 3773. The Senate amendment included, among other things, a provision allowing the Attorney General to seek the dismissal of civil lawsuits brought by private citizens against telecommunications providers that may have assisted the federal government in carrying out warrantless electronic surveillance. In March of 2008, the House responded by passing a third version of H.R. 3773 removing the retroactive immunity provisions, but later passed a compromise bill, H.R. 6304, in June. H.R. 6304 included a variation on the retroactive immunity provisions of the Senate's version of H.R. 3773. In July of 2008, the Senate passed H.R. 6304, also titled the FISA Amendments Act of 2008 (FISA Amendments Act), without modification, and the President subsequently signed it into law.[4387] This report discusses the effect of the retroactive immunity provided by the FISA Amendments Act on lawsuits alleging unlawful electronic surveillance by telecommunications providers under a Terrorist Surveillance Program (TSP) between 2001 and 2007.

The Terrorist Surveillance Program

In late 2005, the New York Times reported that the federal government had "monitored the international telephone calls and international e-mail messages of hundreds, perhaps thousands, of people in the United States without warrants."[4388] Subsequently, President Bush acknowledged that, after the attacks of September 11, 2001, he had authorized the National Security Agency to "intercept international communications into and out of the United States" by "persons linked to al Qaeda or related terrorist organizations" based upon "his constitutional authority to conduct warrantless wartime electronic surveillance of

---

[4387] FISA Amendments Act of 2008, P.L. 110-261 (July 10, 2008).

[4388] James Risen and Eric Lichtblau, Bush Lets U.S. Spy on Callers Without Courts, NEW YORK TIMES, Dec. 16, 2005, at 1.

the enemy."[4389] The revelation of the existence of the TSP aroused controversy because it appeared to run afoul of the general rule[4390] that electronic surveillance by the federal government is unlawful unless conducted pursuant to the Foreign Intelligence Surveillance Act (FISA)[4391] or Title III of the Omnibus Crime Control and Safe Streets Act (Title III).[4392] In contrast, the Bush Administration's position has been that such warrantless surveillance is lawful under the President's constitutionally granted authority and the Authorization for Use of Military Force (AUMF) enacted by Congress in 2001.[4393]

On Jan 17, 2007, a letter from the Attorney General to Congress indicated that "any electronic surveillance that was occurring as part of the Terrorist Surveillance Program [would] be conducted subject to the approval of the Foreign Intelligence Surveillance Court." Now discontinued, the TSP appears to have been active from shortly after September 11, 2001, to sometime in January of 2007.[4394]

Dozens of lawsuits have been filed by private citizens and interest groups alleging various statutory and constitutional violations by the telecommunications companies that participated in the TSP.[4395] The debate over retroactive immunity is of central importance to these cases, as it would likely render any litigation of the underlying legal issues moot.[4396] On August 2, 2007, the Director of National Intelligence (DNI) stated that "those who assist the Government in protecting us from harm must be protected from liability," specifically "those who are alleged

---

[4389] U.S.DEP'T OF JUSTICE, Legal Authorities Supporting the Activities of the National Security Agency Described by the President, at 5, 17, Jan. 19, 2006, available at [http://www.usdoj.gov/opa/whitepaperonnsalegalauthorities.pdf].

[4390] The "procedures in [Title III of the Omnibus Crime Control and Safe Streets Act] and the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which electronic surveillance, as defined in section 101 of FISA, and the interception of domestic wire, oral, and electronic communications may be conducted." 18 U.S.C. § 2511(2)(f) (emphasis added).

[4391] P.L. 95-511, 92 Stat. 1783 (1978) (codified as amended at 50 U.S.C. §§ 1801 et seq.).

[4392] P.L. 90-351, tit. III, 82 Stat. 197, 211 (1968) (codified as amended at 18 U.S.C. §§ 2510 et seq.).

[4393] P.L. 107-40, 115 Stat. 224 (2001). See, also, CRS Congressional Distribution Memo, Presidential Authority to Conduct Warrantless Electronic Surveillance to Gather Foreign Intelligence Information, by Elizabeth B. Bazan and Jennifer K. Elsea (Jan. 5, 2008).

[4394] S.Rept. 110-209, at 4.

[4395] Id. at 7.

[4396] For a more detailed discussion of these lawsuits and retroactive immunity, see, CRS Report RL34279, The Foreign Intelligence Surveillance Act: An Overview of Selected Issues, by Elizabeth B. Bazan, at 14-21.

to have assisted the Government after September 11, 2001 and have helped keep the country safe."[4397] Proponents of retroactive immunity also argued that without "the [telecommunications providers'] voluntary cooperation it [foreign intelligence gathering] is much harder and we get much less [information]."[4398] On the other hand, opponents of retroactive immunity pointed out that retroactive immunity "strips [unlawfully surveilled] individuals of the ability to vindicate their rights in court regarding wiretapping abuses of the past,"[4399] and that "if we want [telecommunications providers] to follow the law in the future, it sends a terrible message, and sets a terrible precedent, to give them a 'get out of jail free' card for allegedly ignoring the law in the past."[4400]

Issues Raised by Civil Actions Against Telecommunications Providers

Retroactive immunity is more than simply protection from liability; it can also act as protection from the cost of litigation. Therefore, before discussing the effects of any retroactive immunity provisions, it may be helpful to examine how a covered lawsuit might proceed in the absence of retroactive immunity. Without retroactive immunity, many legal issues would need to be addressed, possibly at great expense, in order to resolve these cases. The plaintiffs would need to show that the actions of the defendants were not lawful under the laws in effect when the TSP was active. The Bush Administration's theory of inherent wiretapping ability might be litigated. Additionally, the applicability of the state secrets privilege could also be the subject of litigation. Each of these issues is discussed below.

Lawfulness Under the FISA and Title III

As a general principle, if electronic surveillance is likely to result in the acquisition of communications to or from someone in the United States such surveillance may not be conducted unless sanctioned by a court order.[4401] Federal

---

[4397] Admiral Michael McConnell, Director of Nat'l Intelligence, Modernization of the Foreign Intelligence Surveillance Act (FISA), Aug. 2, 2007, available at [http://www.odni.gov/press_releases/20070802_release.pdf].

[4398] 154 CONG. REC. S6454 (daily ed. July 9, 2008) (statement of Sen. Bond).

[4399] ACLU, Letter to the Senate Urging No Votes On Any Bill That Would Authorize Warrantless Wiretapping or Grant Immunity to Telecoms, Feb. 2, 2008, available at [http://www.aclu.org/safefree/general/33909leg20080204.html].

[4400] 154 CONG. REC. S6381 (daily ed. July 8, 2008) (statement of Sen. Feingold).

[4401] But, 50 U.S.C. § 1802 authorizes electronic surveillance without a court order for up to one year, if the targets are means of communications, property, or premises used exclusively by foreign governments, and there is no substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person is a party. Exceptions also apply

law provides two statutory frameworks for obtaining warrants to conduct electronic surveillance: Title III of the Omnibus Crime Control and Safe Streets Act and FISA. Title III authorizes electronic surveillance in the context of law enforcement, while FISA authorizes electronic surveillance in the context of gathering foreign intelligence. Both Title III and FISA also provide prospective civil immunity for individuals that assist or conduct electronic surveillance under the auspices of either statutory framework.[4402]

Plaintiffs suing telecommunications providers, and others, argue that the TSP was not lawful under either Title III or FISA. Many of the details of the TSP remain classified, but it apparently authorized the surveillance of international communications without a judicially issued warrant if there was a "reasonable basis to conclude that one party to the conversation [was] a member of al Qaeda."[4403] That determination appears to have been made by intelligence officials, and was reported to have been reviewed every 45 days.[4404] In contrast, Title III and FISA only allow warrantless surveillance for shorter periods of time in most circumstances.[4405] Statements by officials in the Bush Administration appear to acknowledge that the TSP was conceived and operated outside of the procedures authorized by either Title III or FISA.[4406]

---

during emergency situations or after congressional declarations of war. Infra, note 19. For a thorough description and analysis of federal wiretapping laws, see, CRS Report 98-326, Privacy: An Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping, by Gina Stevens and Charles Doyle.

[4402] 18 U.S.C. § 2511(2)(a)(ii) bars civil actions against telecommunications providers that give assistance pursuant to a court order or certification issued under Title III. FISA bars civil actions against the same type of defendants for assistance given pursuant to surveillance authorized by that statute. 50 U.S.C. § 1805(h).

[4403] Press Briefing, infra note 20.

[4404] President George W. Bush, Press Conference, Dec. 19, 2005, available at [http://www.whitehouse.gov/news/releases/2005/12/20051219-2.html].

[4405] See, 18 U.S.C. § 2518(7) (authorizing warrantless electronic surveillance for 48 hours in situations involving immediate danger to persons, threats to national security, or organized crime); 50 U.S.C. § 1805(e) (authorizing emergency warrantless electronic surveillance for up to 72 hours while a court order is sought); and 50 U.S.C. § 1811 (authorizing warrantless electronic surveillance for 15 days following a Congressional declaration of war). But, see, discussion of authority to conduct warrantless electronic surveillance for up to one year, supra, note 15.

[4406] For example, Attorney General Alberto Gonzales made the following statement: [FISA] is a very important tool that we continue to utilize. Our position is that we are not legally required to do [sic], in this particular case, because the law requires that we — FISA requires that we get a court order, unless authorized by a statute, and we believe that authorization has occurred. General Michael Hayden, Principal Deputy Director for National Intelligence, elaborated further on that statement: [B]ecause of the speed, because of the procedures, because of the processes and requirements set up in the FISA process, I can say unequivocally that we have used this program [the TSP] in lieu of that [FISA] and this program has been successful. Attorney General

Executive Authority and the Authorization for Use of Military Force

Nonetheless, the Bush Administration has argued, in support of the TSP, that the Constitution grants the executive the inherent power to conduct electronic surveillance to gather foreign intelligence and the AUMF reflects a congressional intent to give the executive the authority to take all measures necessary to combat terrorism. A full exposition of the support for these propositions is beyond the scope of this report.[4407] However, one should note that the question would require reconciling the assertions of the Bush Administration with the legislative history and statutory text of FISA and Title III which identify those statutes as the exclusive means of conducting electronic surveillance.[4408] Here, it is sufficient to note that it is an issue that would likely require extensive litigation in order to be resolved.

The State Secrets Privilege

In some cases, the confidential subject matter of a suit may prevent a court from hearing it. Under the judicially created state secrets privilege, "public policy forbids the maintenance of any suit ... the trial of which would inevitably lead to the disclosure of matters which the law itself regards as confidential."[4409] Insofar as many of the details of the TSP remain classified, it is likely that the state secrets privilege would be central to the disposition of the suits against telecommunications providers discussed above.

The state secrets privilege is held by the government, meaning that only the government can assert it to preclude litigation.[4410] If claimed by the federal government, the effect of the state secrets privilege can range from the exclusion of certain information from discovery or admission at trial to the complete dismissal of a civil action.[4411] For example, in *Totten v. United States*, a former spy brought suit to enforce a secret contract with the federal government for

---

Alberto Gonzales and General Michael Hayden, Press Briefing, Dec. 19, 2005, available at [http://www.whitehouse.gov/news/releases/2005/12/20051219-1.html].

[4407] For a detailed analysis of the Bush Administration's arguments, see, CRS Congressional Distribution Memo, Presidential Authority to Conduct Warrantless Electronic Surveillance to Gather Foreign Intelligence Information, by Elizabeth B. Bazan and Jennifer K. Elsea (Jan. 5, 2008).

[4408] Id. at 40-41.

[4409] Totten v. United States, 92 U.S. 105, 107 (1876) (applying the privilege to bar a suit to enforce a secret contract for espionage).

[4410] United States v. Reynolds, 345 U.S. 1, 7 (1953).

[4411] See, Id. at 11 n.26 (quoted by Hepting v. AT&T, 439 F. Supp. 2d 974, 984 (N.D. Cal. 2006)).

espionage services. Ultimately, in that case, the Supreme Court held that the subject of litigation, namely the contract for espionage, was itself a secret and any litigation on that subject was barred.[4412]

In other circumstances, the state secrets privilege applies only to certain items of evidence, rather than to the subject of litigation at large. In *Halkin v. Helms*, the D.C. Circuit was confronted with a claim of privilege regarding the NSA's alleged interception of international communications to and from persons who had been targeted by the CIA.[4413] After deciding that the claim of privilege was valid, the court of appeals affirmed the protection of that information from discovery, while permitting other evidence that the plaintiffs were targeted by the CIA.[4414] In the end, however, the court dismissed the suit after deciding that without the privileged information, the plaintiffs would not be able to make a prima facie case.

A similar result may occur if the state secrets privilege requires the exclusion of evidence central to a defendant's case. In *Molerio v. Federal Bureau of Investigation*, a job seeker alleged that the FBI had disqualified him based upon his father's political ties to socialist organizations in violation of his father's First Amendment rights.[4415] In response, the FBI asserted that it had a lawful reason to disqualify the plaintiff, but claimed that its reason was protected by the state secrets privilege. After reviewing the FBI's claim in camera, the D.C. Circuit agreed that the evidence of a nondiscriminatory reason was protected and that its exclusion would deprive the FBI of a valid defense. Therefore, the dismissal of that action was required.[4416]

Although it is not possible to accurately determine whether the state secrets privilege would necessitate dismissal of the telecommunications cases discussed above, several courts presented with lawsuits regarding the TSP have issued preliminary rulings regarding the applicability of the state secrets privilege.

In *Hepting v. AT&T*, the district court was presented with an assertion of the state secrets privilege.[4417] The court first examined whether the information requested was actually secret, given the amount of media publicity regarding the

---

[4412] Totten, 92 U.S. at 107.

[4413] Halkin v. Helms, 690 F.2d 977 (D.C. Cir. 1982).

[4414] The other evidence of CIA targeting was never claimed to be privileged by the government. Id. at 997.

[4415] Molerio v. FBI, 749 F. 2d 815, 824-825 (D.C. Cir. 1984).

[4416] Id. at 825.

[4417] Hepting v. AT&T, 439 F. Supp. 2d 974 (N.D. Cal. 2006).

TSP and public statements made by the Bush Administration and the defendant.[4418] While the specifics of the TSP may remain classified, the court noted that the general subject of the litigation, specifically that such a program existed at all, was no longer a secret given the admissions made by the government and the defendant. Therefore, this case was distinguishable from *Totten*, and dismissal of the case at the outset of litigation was inappropriate.[4419] While the privilege may limit the plaintiffs' discovery efforts or the defendant's assertion of a defense at a later date, the court declined to rule on whether that would ultimately necessitate dismissal.[4420]

FISA may preempt the state secrets privilege. In *In re National Security Agency Telecommunications Records Litigation*, the court considered 50 U.S.C. § 1806(f), which mandates a legislatively created procedure for courts to consider sensitive material, the disclosure of which might damage the national security of the United States.[4421] Section 1806(f), which was left unmodified by the FISA Amendments Act, requires sensitive information to be reviewed by courts ex parte and in camera with adequate procedures to safeguard against inadvertent disclosure.[4422] The court found that this legislative framework trumped the judicially created state secrets privilege, despite arguments that the privilege was of constitutional origin.[4423] The court did not preclude assertion of the privilege where FISA did not apply.[4424] In the case before it, the plaintiffs had yet to show standing as "aggrieved persons" under FISA. Therefore, the court continued to bar the privileged information, but only until the plaintiffs had the opportunity to show, through other evidence, whether they are "aggrieved persons."[4425]

[4418] Id. at 986.

[4419] Id. at 993.

[4420] Id. at 994.

[4421] See, In re National Security Agency Telecommunications Records Litigation, No. 06-1791 VRW, slip op. at 18 (N.D. Cal. July 2, 2008) (holding that FISA's procedures for a court's in camera review of classified information preempts the common law state secrets privilege).

[4422] 50 U.S.C. § 1806(f).

[4423] In re National Security Agency Telecommunications Records Litigation, supra, note 35, at 20-22.

[4424] Id. at 17.

[4425] Id. at 48-49. See, 50 U.S.C. § 1801(k) (defining "aggrieved persons").

Retroactive Immunity Under the FISA Amendments Act of 2008

Title II of the FISA Amendments Act lays out a procedure for the Attorney General to seek the dismissal of lawsuits alleging unlawful participation in the TSP by telecommunications providers. The process begins when the Attorney General certifies, to the court where the lawsuit is pending, two fundamental facts regarding the defendant's alleged assistance. First, the assistance must have been given in connection with the TSP between September 11, 2001, and January 17, 2007. Second, the defendant must have been given written assurances that the TSP was authorized by the President and determined to be lawful. Alternatively, the Attorney General can certify that the alleged assistance was not in fact provided by the defendant. All parties are permitted to submit documents and arguments which the court may consider, and dismissal is required if the court finds, based upon its review, that the certification was supported by "substantial evidence." What constitutes substantial evidence is discussed in the section below regarding standards of review.

Alternative Retroactive Immunity Proposals

Before the passage of H.R. 6304 by the Senate, that body had previously included retroactive immunity for telecommunications providers in its amendment to H.R. 3773. Additionally, three amendments were proposed to H.R. 6304 that would have modified the retroactive immunity provisions. This section examines the different approaches to retroactive immunity in that bill and the proposed amendments.

Senate Amendment to H.R. 3773

In February of 2008, the Senate passed an amendment in the nature of a substitute to H.R. 3773. Like H.R. 6304, this Senate amendment would have required courts to dismiss lawsuits against telecommunications providers if sufficient grounds for dismissal were certified to the court by the Attorney General.[4426] With respect to the lawsuits alleging assistance provided under the TSP, the grounds for dismissal were identical to those required under H.R. 6304. But, H.R. 3773 did not provide a means for others to submit arguments or documents in opposition to dismissal, and certifications would only be subject to review for an abuse of discretion.[4427] What qualifies as an abuse of discretion is discussed in the section below regarding standards of review.

Proposed Amendments to H.R. 6304

[4426] H.R. 6304, § 201, 110th Cong.

[4427] H.R. 3773, § 202(a) as amended by the Senate, 110th Cong.

Three amendments offering variations on the retroactive immunity mechanism were introduced in the Senate during the debate over H.R. 6304, but were not adopted.

S.Amdt. 5059

Introduced by Senator Specter, S.Amdt. 5059 would have added a second component to a court's review of a certification by the Attorney General. Under this amendment, dismissal would not be appropriate if the court determined that the underlying intelligence activity that the defendant had participated in was unconstitutional. Because this would have been a legal determination, the court would have been permitted to address this question *de novo* without relying upon or giving deference to any interpretations of the Constitution made by the Attorney General in the certification or elsewhere.

S.Amdt. 5060

Introduced by Senator Whitehouse, S.Amdt. 5060 would have required that the Attorney General additionally certify that the defendant had provided assistance based on a "good faith and reasonable belief" that its conduct was lawful. Like the rest of the certification, this finding would have needed to be supported by "substantial evidence" in order to result in a dismissal.

S.Amdt. 5066

Introduced by Senator Bingaman, S.Amdt. 5066 would have left the certification mechanism of H.R. 6304 in place, but would have delayed certification by the Attorney General in cases involving the TSP until 90 days after the inspectors general of various intelligence and national security agencies had reviewed the TSP and submitted a comprehensive report to Congress detailing their findings. Additionally, all TSP lawsuits would have been stayed during this time. The review and report are still mandated by a separate provision of H.R. 6304, § 301, and are required to be completed within one year of the date of enactment, but does not require any TSP lawsuits to be stayed.

Comparison of Retroactive Immunity Provisions

Timing of Certifications

Although alternative proposals to retroactive immunity followed the same general procedure as the FISA Amendments Act with respect to how and by whom a certification is made, the question of when a certification is made may vary substantially. Generally, the certification would appear to be permissible at any stage of litigation before final judgment. Note, however, that the act requires certifications to be made to the court in which the action is pending. That clause could possibly be read to disallow certifications in anticipation of any litigation. In contrast, the Senate amendment to H.R. 3773 did not appear to contain such language. The import of this difference may be magnified as a change in Administration is imminent. This may create the possibility that, under the law as passed, a potential plaintiff could forestall filing suit in the hope that a new

Administration, opposed to retroactive immunity, would take office. If anticipatory certifications are not permitted because no action is pending, suits filed after the Administration changes could still be dismissed, but only at the discretion of a newly appointed Attorney General.

Similarly, the delay proposed by S.Amdt. 5066 also raised the possibility that a change in Administration could have affected the certification of a lawsuit alleging that participation in the TSP was unlawful. S.Amdt. 5066 would have disallowed certifications until 90 days after a report detailing the specifics of the TSP is received by Congress. Depending upon how long it actually took for that report to be completed, certifications might not have been permissible until some time after the current Administration had left office.

Standards of Review

The Senate amendment to H.R. 3773 would have instructed the court to review certifications using an "abuse of discretion standard." In contrast, the enacted FISA Amendments Act requires certifications to be supported by "substantial evidence." Two important characteristics of any standard of review are the level of scrutiny given and the scope of the universe in which such review takes place. An analysis of each standard of review and its potential effect on the pending litigation at issue is discussed below.

Abuse of Discretion

In the judicial context, appellate courts commonly review discretionary rulings of lower courts under an abuse of discretion standard. For example, a federal trial judge's decision to exclude evidence because it is unfairly prejudicial is reversible error only if the trial court made an error of law or acted in an unprincipled, arbitrary, or irrational manner.[4428] In the words of the Supreme Court, it is "deference that is the hallmark of abuse of discretion review."[4429]

But, the Senate amendment to H.R. 3773 deals with judicial review of the actions of an executive branch official, namely the Attorney General. Therefore, an examination of the standards for judicial review of administrative action under the Administrative Procedure Act (APA) may be more illustrative than comparisons to review of actions by lower courts. Unless specifically excluded from review by statute, the APA authorizes courts to set aside agency actions that are "arbitrary, capricious, or an abuse of discretion."[4430] The Supreme Court of

[4428] See, e.g., Republic of the Phil. v. Pimentel, 128 S. Ct. 2180, 2189 (2008); United States v. York, 933 F.2d 1343 (7th Cir. 1991); United States v. Coiro, 922 F.2d 1008 (2nd Cir. 1991).

[4429] G.E. v. Joiner, 522 U.S. 136, 143 (1997) (addressing whether appellate court properly evaluated trial court's actions using an abuse of discretion standard).

[4430] 5 U.S.C. § 706(2)(A).

the United States had the opportunity to expound upon the meaning of this standard in Citizens to Preserve Overton Park, Inc. v. Volpe, a case involving a challenge to the construction of a highway through a public park.[4431] The Court held that this standard of review required the reviewing court to

> *consider whether the decision was based upon a consideration of the relevant factors and whether there has been a clear error of judgment. Although this inquiry into the facts is to be searching and careful, the ultimate standard of review is a narrow one. The court is not empowered to substitute its judgment for that of the agency.*[4432]

Therefore, in the case of certifications by the Attorney General, a court reviewing for an abuse of discretion would have likely examined the Attorney General's consideration of the assistance provided by the defendants, the types of representations made by intelligence officials concurrently with requests for assistance, and the facts surrounding any other findings required by the certification.

Note that the Senate amendment to H.R. 3773 did not indicate what record, if any, the court would be able to review in gauging the propriety of the Attorney General's certification. The only documentation the Attorney General would have been required to present is the certification itself, and no other provision would have allowed opposing parties to present contradictory evidence or arguments. Because of these limitations, it is not clear on what basis, if any, a court could have found a certification under H.R. 3773 to be an abuse of discretion.

Substantial Evidence

In contrast, "substantial evidence" is a standard of review frequently used by courts to review formal findings of fact by federal agencies.[4433] It is less stringent than de novo review, which would allow a court to look at the evidence anew and come to its own conclusions. Nevertheless, the Supreme Court has described "substantial evidence" as requiring "more than a mere scintilla" of support and comparable to the standard a trial judge must meet to sustain a jury's verdict.[4434]

[4431] Citizens to Preserve Overton Park, Inc. v. Volpe, 401 U.S. 402 (1971) (overruled on other grounds by Califano v. Sanders, 430 U.S. 99, 105 (1977)).

[4432] Id. at 416.

[4433] In Overton Park, the Supreme Court remarked that substantial evidence review was not appropriate because the agency had not taken undertaken formal rulemaking or an adjudicatory hearing. Overton Park, 401 U.S. at 414.

[4434] Consolidated Edison Co. v. NLRB, 305 U.S. 197, 229 (1938); NLRB v. Columbian Enameling & Stamping Co., 306 U.S. 292, 300 (1939).

In the federal courts, a jury verdict will not be disturbed if "reasonable and fair-minded persons in exercise of impartial judgment" might have come to the same conclusion as the jury.[4435] Therefore, under the "substantial evidence" test, if a court reviewing an Attorney General's certification under the FISA Amendments Act found that an objectively reasonable person could conclude that the facts in the certification were true, the court would be required to dismiss the suit.

In the administrative context, substantial evidence review and abuse of discretion review occur in factually distinct circumstances. Substantial evidence is required when an agency engages in either formal rulemaking or an adjudicatory hearing. In contrast, abuse of discretion applies in cases of informal rulemaking and decisions. Therefore, it may be difficult to directly compare the two standards in terms of stringency. Although some courts appear to consider substantial evidence a more demanding standard than abuse of discretion, the consistent theme of both standards is that the court is not free to substitute its judgment in place of the agency's.[4436] However, any apparent similarity between the level of deference afforded by a reviewing court under either standard should not overshadow important differences in the scope of the record available to the court.

The scope of the record viewed by the court is a critical factor affecting the search for "substantial evidence." In *Universal Camera v. National Labor Relations Board*, the Supreme Court interpreted the Taft-Hartley Act's use of the phrase "substantial evidence on the record considered as a whole."[4437] A previous version of the act stated only that findings by the National Labor Relations Board be "supported by evidence" and had been read by some courts to mean that if any evidence exists to support the agency's findings, then they are valid, regardless of what contradictory evidence also exists. But, in Universal Camera, the Supreme Court found that the addition of the phrase "on the record considered as a whole" indicated that Congress intended courts to review agency findings of fact based upon a holistic view of the record, evaluating supporting evidence in light of available contradictory information.[4438]

[4435] E.g., Kosmynka v. Polaris Industries, Inc., 462 F.3d 74, 79-82 (2nd Cir. 2006) (upholding jury's finding that a manufacturer was negligent for failing to warn that its all-terrain vehicle might upend itself despite uncontested evidence that the manufacturer had received no reports of such incidents).

[4436] See, e.g., Frontier Fishing Corp. v. Evans, 429 F. Supp. 2d 316, n.7 (citing Indus. Union Dep't v. API, 448 U.S. 607, 705 (1980) (Marshall, J., dissenting, asserting that substantial evidence is more stringent, but is ultimately a deferential standard)).

[4437] Universal Camera v. NLRB, 340 U.S. 474 (1951) (emphasis added).

[4438] Id. at 490.

The FISA Amendments Act requires that certifications be supported by "substantial evidence provided to the court pursuant to this section." The act goes on to permit a reviewing court to examine documentation, certifications, briefs and arguments submitted by all parties when determining if substantial evidence supports the certification. One could reasonably conclude that the availability of contradictory evidence would indicate the intent to apply the more stringent Universal Camera definition of substantial evidence. On the other hand, the text of the act may not require the court to consider extraneous material.[4439]

Therefore, as compared with the Senate amendment to H.R. 3773, the FISA Amendments Act provides the possibility of a broader factual record in which to conduct judicial review of a certification by the Attorney General, but may leave much of the discretion to view that record to the court itself. Under the FISA Amendments Act, it seems possible that a court could lawfully dismiss a case upon certification by the Attorney General, if the court finds the substantial evidence standard is satisfied after looking only at the information provided by the Attorney General.

[4439] Compare, 50 U.S.C. § 1885a(b)(2) ("the court may examine [supplemental materials]") (emphasis added) with 50 U.S.C. § 1185a(c) ("the court shall review such certification and the supplemental materials in camera and ex parte") (emphasis added).

Cyber-Espionage and Cyber-Warfare by U.S. Intelligence Agencies: Still a Largely Unregulated Area of Operations

Internet Privacy: Overview and Legislation in the 109th Congress, 1st Session, RL31408 (January 26, 2006).

MARCIA S. SMITH, CONG. RESEARCH SERV., INTERNET PRIVACY: OVERVIEW AND LEGISLATION IN THE 109TH CONGRESS, 1ST SESSION (2006), *available at* http://www.intelligencelaw.com/library/secondary/crs/pdf/RL31408_1-26-2006.pdf.

Order Code RL31408
CRS Report for Congress

Updated January 26, 2006

Marcia S. Smith
Specialist in Aerospace and Telecommunications Policy
Resources, Science, and Industry Division
Congressional Research Service
The Library of Congress

Summary

Internet privacy issues encompass several types of concerns. One is the collection of personally identifiable information (PII) by website operators from visitors to government and commercial websites, or by software that is surreptitiously installed on a user's computer ("spyware") and transmits the information to someone else. Another is the monitoring of electronic mail and Web usage by the government or law enforcement officials, employers, or email service providers.

The September 11, 2001 terrorist attacks intensified debate over the issue of monitoring by the government and law enforcement officials, with some advocating increased tools to help them track down terrorists, and others cautioning that fundamental tenets of democracy, such as privacy, not be endangered in that pursuit. Congress passed the 2001 USA PATRIOT Act (P.L. 107-56) that, inter alia, makes it easier for law enforcement officials to monitor Internet activities. That act was amended by the Homeland Security Act (P.L. 107-296), loosening restrictions as to when, and to whom, Internet Service Providers may voluntarily release the content of communications if they believe there is a danger of death or injury. Some provisions of the USA PATRIOT Act, including two that relate to Internet use, would have expired on December 31, 2005. Congress passed a brief extension (to February 3, 2006) in P.L. 109-160.

Debate over whether civil liberties protections need to be added if the provisions are to be made permanent is expected to continue in the second session of the 109th Congress. Revelations that President Bush directed the National Security Agency to monitor some communications, including e-mails, in the United States without warrants may affect those deliberations.

The debate over website information policies concerns whether industry self regulation or legislation is the best approach to protecting consumer privacy. Congress has considered legislation that would require commercial website operators to follow certain fair information practices, but the only law that has been enacted (COPPA, P.L. 105-277) concerns the privacy of children under 13, not the general public. Legislation has passed regarding information practices for federal government websites, including the E-Government Act (P.L. 107-347).

The growing controversy about how to protect computer users from "spyware" without creating unintended consequences is discussed briefly in this report, but in more detail in CRS Report RL32706. Another issue, identity theft, is not an Internet privacy issue per se, but is often debated in the context of whether the Internet makes identity theft more prevalent. For example, Internet-based practices called "phishing" and "pharming" may contribute to identity theft. Identity theft is briefly discussed in this report; more information is available in CRS Report RS22082, CRS Report RL31919, and CRS Report RL32535. Wireless privacy issues are discussed in CRS Report RL31636.

This is the final edition of this report. It provides an overview of Internet privacy issues and related laws passed in previous Congresses, and discusses legislative activity in the first session of the 109th Congress.

Introduction

Internet privacy issues encompass several concerns. One is the collection of personally identifiable information (PII) by website operators from visitors to government and commercial websites, or by software that is surreptitiously installed on a user's computer ("spyware") and transmits the information to someone else. Another is the monitoring of electronic mail and Web usage by the government or law enforcement officials, employers, or e-mail service providers. Another issue, identity theft, is not an Internet privacy issue per se, but is often debated in the context of whether the Internet makes identity theft more prevalent. For example, Internet-based practices called "phishing" and "pharming" may contribute to identity theft.

This report provides an overview of Internet privacy-related issues and related laws passed in previous Congresses, and discusses legislative activity in the first session of the 109th Congress. Background information on Internet privacy issues is available in an archived CRS Report RL30784, Internet Privacy: An Analysis of Technology and Policy Issues, by Marcia Smith (available from author); and CRS Report RL31289, The Internet and the USA PATRIOT Act:

Potential Implications for Electronic Privacy, Security, Commerce, and Government, by Marcia Smith, et al.

Internet: Commercial Website Practices

One aspect of the Internet ("online") privacy debate focuses on whether industry self regulation or legislation is the best route to assure consumer privacy protection. In particular, consumers appear concerned about the extent to which website operators collect "personally identifiable information" (PII) and share that data with third parties without their knowledge. Although many in Congress and the Clinton Administration preferred industry self regulation, the 105th Congress passed legislation (COPPA, see below) to protect the privacy of children under 13 as they use commercial websites. Many bills have been introduced since that time regarding protection of those not covered by COPPA, but the only legislation that has passed concerns federal government, not commercial, websites.

Children's Online Privacy Protection Act (COPPA), P.L. 105-277

Congress, the Clinton Administration, and the Federal Trade Commission (FTC) initially focused their attention on protecting the privacy of children under 13 as they visit commercial websites. Not only are there concerns about information children might divulge about themselves, but also about their parents. The result was the Children's Online Privacy Protection Act (COPPA), Title XIII of Division C of the FY1999 Omnibus Consolidated and Emergency Supplemental Appropriations Act, P.L. 105-277.[4440] The FTC's final rule implementing the law became effective April 21, 2000 [http://www.ftc.gov/os/1999/10/64fr59888.htm]. Commercial websites and online services directed to children under 13, or that knowingly collect information from them, must inform parents of their information practices and obtain verifiable parental consent before collecting, using, or disclosing personal information from children. The Commission adopted a "sliding scale" for complying with the verifiable consent requirement depending on how the data would be used. That is, if the information was for internal use only, the verifiable consent could be obtained from the parent by e-mail, plus an additional step to ensure the person giving consent is, in fact, the parent. If the website operator planned to disclose the information publicly or to third parties, a higher standard was set. This sliding scale was set to expire in 2002 with the expectation that better verification technologies would become available. However, in 2002, the FTC determined that such technologies still were not available, and the sliding scale was extended to April 12, 2005. In 2005, the Commission extended it

[4440] COPPA should not be confused with COPA — the Child Online Protection Act — which addresses protecting children from unsuitable material, such as pornography, on the Internet. COPA is discussed in CRS Report RS21328, Internet: Status of Legislative Attempts to Protect Children from Unsuitable Material on the Web, by Marcia S. Smith.

again, and is seeking public comment on how to proceed, as part of its overall review of the COPPA rule.[4441]

The law also provides for industry groups or others to develop self-regulatory "safe harbor" guidelines that, if approved by the FTC, can be used by websites to comply with the law. The FTC approved self-regulatory guidelines proposed by the Better Business Bureau on January 26, 2001. On June 11, 2003, then-FTC Chairman Timothy Muris stated in testimony to the Senate Commerce Committee that the FTC had brought eight COPPA cases, and obtained agreements requiring payment of civil penalties totaling more than $350,000.[4442]

As required by COPPA, on April 21, 2005, the Commission issued a request for public comment on its final rule, five years after the rule's effective date.[4443] Comments were requested on the costs and benefits of the rule; whether it should be retained, eliminated, or modified; and its effect on practices relating to the collection of information relating to children, children's ability to access information of their choice online, and the availability of websites directed to children.

FTC Activities and Fair Information Practices

The FTC conducted or sponsored several surveys between 1997 and 2000 to determine the extent to which commercial website operators abided by four fair information practices — providing notice to users of their information practices before collecting personal information, allowing users choice as to whether and how personal information is used, allowing users access to data collected and the ability to contest its accuracy, and ensuring security of the information from unauthorized use. Some include enforcement as a fifth fair information practice. Regarding choice, the term "opt-in" refers to a requirement that a consumer give affirmative consent to an information practice, while "opt-out" means that permission is assumed unless the consumer indicates otherwise. See archived CRS Report RL30784, Internet Privacy: An Analysis of Technology and Policy Issues, by Marcia Smith (available from author), for more information on the FTC surveys and fair information practices. The FTC's reports are available on its website [http://www.ftc.gov].

[4441] "FTC Seeks Public Comment on Children's Online Privacy Rule." FTC press release, April 21, 2005. See [http://www.ftc.gov/opa/2005/04/coppacomments.htm]. (Hereafter cited as FTC Seeks Public Comment on Children's Online Privacy Rule).

[4442] Prepared statement of Timothy Muris, Chairman, Federal Trade Commission, p. 10, available at [http://commerce.senate.gov/hearings/witnesslist.cfm?id=807].

[4443] FTC Seeks Public Comment on Children's Online Privacy Rule.

Briefly, the first two FTC surveys (December 1997 and June 1998) created concern about the information practices of websites directed at children and led to the enactment of COPPA (see above). The FTC continued monitoring websites to determine if legislation was needed for those not covered by COPPA. In 1999, the FTC concluded that more legislation was not needed at that time because of indications of progress by industry at self-regulation, including creation of "seal" programs (see below) and by two surveys conducted by Georgetown University. However, in May 2000, the FTC changed its mind following another survey that found only 20% of randomly visited websites and 42% of the 100 most popular websites had implemented all four fair information practices. The FTC voted to recommend that Congress pass legislation requiring websites to adhere to the four fair information practices, but the 3-2 vote indicated division within the Commission. On October 4, 2001, Timothy Muris, who had recently become FTC Chairman, stated that he did not see a need for additional legislation at that time. (Mr. Muris was succeeded as FTC Chairman on August 16, 2004 by Deborah Platt Majoras.)

Advocates of Self Regulation

In 1998, members of the online industry formed the Online Privacy Alliance (OPA) to encourage industry self regulation. OPA developed a set of privacy guidelines, and its members are required to adopt and implement posted privacy policies. The Better Business Bureau (BBB), TRUSTe, and WebTrust have established "seals" for websites. To display a seal from one of those organizations, a website operator must agree to abide by certain privacy principles (some of which are based on the OPA guidelines), a complaint resolution process, and to being monitored for compliance. Advocates of self regulation argue that these seal programs demonstrate industry's ability to police itself.

Technological solutions also are being offered. P3P (Platform for Privacy Preferences) is one such technology. It essentially creates machine-readable privacy policies through which users can match their privacy preferences with the privacy policies of the websites they visit. One concern is that P3P requires companies to produce shortened versions of their privacy policies, which could raise issues of whether the shortened policies are legally binding, since they may omit nuances and "sacrifice accuracy for brevity."[4444] For more information on P3P, see [http://www.w3.org/P3P/].

Advocates of Legislation

Consumer, privacy rights and other interest groups believe self regulation is insufficient. They argue that the seal programs do not carry the weight of law,

---

[4444] Clark, Drew. "Tech, Banking Firms Criticize Limitations of Privacy Standard." NationalJournal.com, November 11, 2002.

and that while a site may disclose its privacy policy, that does not necessarily equate to having a policy that protects privacy. The Center for Democracy and Technology (CDT, at [http://www.cdt.org]) and the Electronic Privacy Information Center (EPIC, at [http://www.epic.org]) each released reports on this topic. EPIC's most recent report, Privacy Self Regulation: A Decade of Disappointment, argues that the National Do Not Call list, which restricts telemarketing phone calls, demonstrates that government regulation can be more effective than industry self regulation. Calling telemarketing a 20th century problem, the report concludes that the FTC has given self regulation a decade to work in the Internet privacy arena, and it is time for the agency "to apply the lessons from telemarketing and other efforts to address the 21st century [sic] problem of Internet privacy."[4445]

Some privacy interest groups, such as EPIC, also feel that P3P is insufficient, arguing that it is too complex and confusing and fails to address many privacy issues. An EPIC report from June 2000 further explains its findings [http://www.epic.org/reports/prettypoorprivacy.html].

Privacy advocates have been particularly concerned about online profiling, where companies collect data about what websites are visited by a particular user and develop profiles of that user's preferences and interests for targeted advertising. Following a one-day workshop on online profiling, FTC issued a two-part report in the summer of 2000 that also heralded the announcement by a group of companies that collect such data, the Network Advertising Initiative (NAI), of self-regulatory principles. At that time, the FTC nonetheless called on Congress to enact legislation to ensure consumer privacy vis a vis online profiling because of concern that "bad actors" and others might not follow the self-regulatory guidelines.

Congressional Action

Many Internet privacy bills were considered by the 107th and 108th Congresses. Other than extending an existing prohibition regarding federal websites (see next section), none cleared Congress. Several bills were introduced in the first session of the 109th Congress (see table at end of report).

Internet: Federal Government Website Information Practices

Under a May 1998 directive from President Clinton and a June 1999 Office of Management and Budget (OMB) memorandum, federal agencies must ensure that their information practices adhere to the 1974 Privacy Act. In June 2000, however, the Clinton White House revealed that contractors for the Office of

[4445] EPIC. "Privacy Self Regulation: A Decade of Disappointment," by Chris Jay Hoofnagle. March 4, 2005. [http://www.epic.org/reports/decadedisappoint.pdf], p. 5.

National Drug Control Policy (ONDCP) had been using "cookies" (small text files placed on users' computers when they access a particular website) to collect information about those using an ONDCP site during an anti-drug campaign. ONDCP was directed to cease using cookies, and OMB issued another memorandum reminding agencies to post and comply with privacy policies, and detailing the limited circumstances under which agencies should collect personal information. A September 5, 2000 letter from OMB to the Department of Commerce further clarified that "persistent"cookies, which remain on a user's computer for varying lengths of time (from hours to years), are not allowed unless four specific conditions are met. "Session" cookies, which expire when the user exits the browser, are permitted.

At the time, Congress was considering whether commercial websites should be required to abide by FTC's four fair information practices. The incident sparked interest in whether federal websites should adhere to the same requirements. In the FY2001 Transportation Appropriations Act (P.L. 106-346), Congress prohibited funds in the FY2001 Treasury-Postal Appropriations Act from being used to collect, review, or create aggregate lists that include PII about an individual's access to or use of a federal website or enter into agreements with third parties to do so, with exceptions. Similar language has been included in subsequent appropriations bills. For FY2006, it is Section 832 of the Transportation-Treasury Appropriations Act (P.L. 109-115).

Nonetheless, in December 2005, the Associated Press (AP) reported that a privacy advocate, Daniel Brandt, had discovered that the National Security Agency (NSA) was using permanent cookies on its website.[4446] The AP quoted an NSA spokesman as saying that it resulted from a recent software upgrade and the agency was not aware that permanent cookies were being set. C|NET News.Com reported a week later that, based on its own investigation, "dozens" of agencies were setting permanent cookies or "web bugs."[4447] The article identified the White House, the Air Force, and the Treasury Department as examples, and reported that some of the agencies changed their practices after being contacted, and many seemed to have no idea that their software was setting cookies.

Section 646 of the FY2001 Treasury-Postal Appropriations Act (P.L. 106-554) required Inspectors General (IGs) to report to Congress on activities by those agencies or departments relating to their own collection of PII, or entering into

---

[4446] Jesdanun, Anick. NSA Inadvertently Uses Banned Data-Tracking "Cookies" At website. Associated Press, December 28, 2005, 15:35 (via Factiva).

[4447] McCullagh, Declan. Government Web Sites Are Keeping an Eye On You. C|NET News.com, January 5, 2006. Available on the news.com.com website at [http://news.com.com/Government+Web+sites+are+keeping+an+eye+on+you/2100-102 8_3-6018702.html]. Web bugs are very small (i.e., not visible) graphic images placed on HTML pages or in e-mails that allow third parties to track user behavior.

agreements with third parties to obtain PII about use of websites. Then-Senator Fred Thompson released two reports in April and June 2001 based on the findings of agency IGs who discovered unauthorized persistent cookies and other violations of government privacy guidelines on several agency websites. An April 2001 GAO report (GAO-01-424) concluded that most of the 65 sites it reviewed were following OMB's guidance.

The E-Government Act (P.L. 107-347) sets requirements on government agencies regarding how they assure the privacy of personal information in government information systems and establish guidelines for privacy policies for federal websites. The law requires federal websites to include a privacy notice that addresses what information is to be collected, why, its intended use, what notice or opportunities for consent are available to individuals regarding what is collected and how it is shared, how the information will be secured, and the rights of individuals under the 1974 Privacy Act and other relevant laws. It also requires federal agencies to translate their website privacy policies into a standardized machine-readable format, enabling P3P to work (see above discussion of P3P), for example.

Monitoring of E-mail and Web Usage

By Government and Law Enforcement Officials

Another concern is the extent to which electronic mail (e-mail) exchanges or visits to websites may be monitored by law enforcement agencies or employers. In the wake of the September 11 terrorist attacks, the debate over law enforcement monitoring has intensified. Previously, the issue had focused on the extent to which the Federal Bureau of Investigation (FBI), with legal authorization, used a software program, called Carnivore (later renamed DCS 1000), to intercept e-mail and monitor Web activities of certain suspects. The FBI would install the software on the equipment of Internet Service Providers (ISPs). Privacy advocates were concerned about whether Carnivore-like systems can differentiate between e-mail and Internet usage by a subject of an investigation and similar usage by other people. Technical details of the system were not publicly available, meaning that privacy groups were unable to independently determine exactly what the system could or could not do, leading to their concerns. Section 305 of the 21st Century Department of Justice Appropriations Authorization Act (P.L. 107-273) required the Justice Department to report to Congress at the end of FY2002 and FY2003 on its use of Carnivore/DCS 1000 or any similar system. EPIC obtained the reports in January 2005 under the Freedom of Information Act and placed them on its website.[4448] The reports indicate that the Justice Department no longer uses Carnivore/DCS 1000, using commercially available software instead. The Justice Department

[4448] See [http://www.epic.org/privacy/carnivore/2002_report.pdf], and [http://www.epic.org/privacy/carnivore/2003_report.pdf].

reported that it used commercial software to conduct court-ordered electronic surveillance five times in FY2002 and eight times in FY2003.

The USA PATRIOT Act

Following the terrorist attacks, Congress passed the Uniting and Strengthening America by Providing Appropriate Tools to Intercept and Obstruct Terrorism (USA PATRIOT) Act, P.L. 107-56, which expands law enforcement's ability to monitor Internet activities. Inter alia, the law modifies the definitions of "pen registers" and "trap and trace devices" to include devices that monitor addressing and routing information for Internet communications. Carnivore-like programs may now fit within the new definitions. The Internet privacy-related provisions of the USA PATRIOT Act, included as part of Title II, are as follows:

- Section 210, which expands the scope of subpoenas for records of electronic communications to include records commonly associated with Internet usage, such as session times and duration.
- Section 212, which allows ISPs to divulge records or other information (but not the contents of communications) pertaining to a subscriber if they believe there is immediate danger of death or serious physical injury or as otherwise authorized, and requires them to divulge such records or information (excluding contents of communications) to a governmental entity under certain conditions. It also allows an ISP to divulge the contents of communications to a law enforcement agency if it reasonably believes that an emergency involving immediate danger of death or serious physical injury requires disclosure of the information without delay. This section was amended by the Cyber Security Enhancement Act — see below.
- Section 216, which adds routing and addressing information (used in Internet communications) to dialing information, expanding what information a government agency may capture using pen registers and trap and trace devices as authorized by a court order, while excluding the content of any wire or electronic communications. The section also requires law enforcement officials to keep certain records when they use their own pen registers or trap and trace devices and to provide those records to the court that issued the order within 30 days of expiration of the order. To the extent that Carnivore-like systems fall with the new definition of pen registers or trap and

trace devices provided in the act, that language would increase judicial oversight of the use of such systems.

- Section 217, which allows a person acting under color of law to intercept the wire or electronic communications of a computer trespasser transmitted to, through, or from a protected computer under certain circumstances, and
- Section 224, which sets a four-year sunset period for many of the Title II provisions. Sections 210 and 216 are excluded from the sunset. Sections 212 and 217 are not, and therefore will expire on December 31, 2005. As discussed below, Congress is considering legislation that would amend this sunset clause, making either more or fewer sections subject to it.

The Cyber Security Enhancement Act, section 225 of the 2002 Homeland Security Act (P.L. 107-296), amends section 212 of the USA PATRIOT Act. It lowers the threshold for when ISPs may voluntarily divulge the content of communications. Now ISPs need only a "good faith" (instead of a "reasonable") belief that there is an emergency involving danger (instead of "immediate" danger) of death or serious physical injury. The contents can be disclosed to "a Federal, state, or local governmental entity" (instead of a "law enforcement agency").

Privacy advocates are especially concerned about the language added by the Cyber Security Enhancement Act. EPIC notes, for example, that allowing the contents of Internet communications to be disclosed voluntarily to any governmental entity not only poses increased risk to personal privacy, but also is a poor security strategy. Another concern is that the law does not provide for judicial oversight of the use of these procedures.[4449] A Senate Judiciary Committee hearing on September 23, 2004 explored some of these concerns.

Several House and Senate committees held hearings in the first session of the 109th Congress on various provisions of the USA PATRIOT Act, and more are expected in the second session, as Congress debates whether to extend the "sunset date," or expiration date, of several provisions of that act. Under Section 224, a number of sections would have expired on December 31, 2005, including Section 212 and 217. Section 210 and Section 216 are not subject to the sunset clause (i.e., they are permanent).

[4449] [http://www.epic.org/alert/EPIC_Alert_9.23.html]. See entry under "[3] Homeland Security Bill Limits Open Government, and click on hyperlink to EPIC's February 26, 2002 letter to the House Judiciary Committee.

Several bills were introduced to modify the sunset clause by making temporary provisions permanent, by making permanent provisions temporary, or by modifying reporting requirements or otherwise enhancing oversight of how the provisions are implemented. As December 31, 2005 approached, the issue became very contentious. The House passed a permanent extension (i.e., it repealed the sunset clause) in H.R. 3199. The Senate, however, passed only a six-month extension (S. 2167) to allow time for further consideration of concerns by some Senators that more civil liberties protections are needed. The House did not agree with the Senate action, and amended S. 2167 so that the extension was only for five weeks (through February 3, 2006) to ensure that the Congress dealt with the issue early in the second session. Debate may be influenced by revelations in December 2005 that President George W. Bush directed the National Security Agency to monitor phone calls and e-mails in the United States without warrants. (For further information on the debate over warrantless searches, see the CRS general distribution memorandum at this CRS website: [http://www.crs.gov/products/browse/documents/WD00002.pdf].

The 9/11 Commission Report, and Creation of the Privacy and Civil Liberties Oversight Board

On July 22, 2004, the "9/11 Commission" released its report on the terrorist attacks.[4450] The Commission concluded (pp. 394-395) that many of the USA PATRIOT Act provisions appear beneficial, but that "Because of concerns regarding the shifting balance of power to the government, we think that a full and informed debate on the Patriot Act would be healthy." The Commission recommended that "The burden of proof for retaining a particular governmental power should be on the executive, to explain (a) that the power actually materially enhances security and (b) that there is adequate supervision of the executive's use of the powers to ensure protection of civil liberties. If the power is granted, there must be adequate guidelines and oversight to properly confine its use." The Commission also called for creation of a board within the executive branch "to oversee adherence to the guidelines we recommend and the commitment the government makes to defend our civil liberties." The commissioners went on to say that "We must find ways of reconciling security with liberty, since the success of one helps protect the other. The choice between security and liberty is a false choice, as nothing is more likely to endanger America's liberties than the success of a terrorist attack at home. Our history has shown us that insecurity threatens liberty. Yet, if our liberties are curtailed, we lose the values that we are struggling to defend."

The 108th Congress passed legislation implementing many of the Commission's recommendations. Called the Intelligence Reform and Terrorism Prevention Act (S. 2845, P.L. 108-458), Section 1061 creates a Privacy and Civil Liberties

---

[4450] National Commission on Terrorist Attacks Upon the United States. The 9/11 Commission Report. 585 p. [http://www.9-11commission.gov/report/911Report.pdf].

Oversight Board as part of the Executive Office of the President. According to the bill's sponsor, Senator Collins, the Board's purpose is to "ensure that privacy and civil liberties concerns are appropriately considered in the implementation of all laws, regulations, and policies that are related to efforts to protect the Nation against terrorism."[4451] It must report to Congress annually on an unclassified basis to the greatest extent possible. It will be composed of five members, two of which (the chairman and vice-chairman) must be confirmed by the Senate. All must come from outside the government to help ensure their independence.

National Journal reported on January 13, 2006 that although the five members of the Board have been appointed, the chairman and vice chairman have not yet been confirmed by the Senate.[4452] An August 2005 Reuters report cited critics (including a former 9/11 Commissioner, Members of the House and Senate, and others) as concluding that the panel is a "toothless, underfunded shell with inadequate support" from the President.[4453]

H.R. 1310 (Maloney) was introduced in the first session of the 109th Congress to make a number of changes, including establishing the Board as an independent agency in the executive branch, instead of part of the Executive Office of the President; setting out certain qualifications for Board members; and requiring that all of the Board members be confirmed by the Senate, not just the chairman and vice-chairman. There was no legislative action on the bill during the first session. As with debate over the USA PATRIOT Act, this discussion may be influenced by the controversy over warrantless searches (see above).

Government Access to Search Engine Data (e.g. Google)

In January 2006, Internet search engine company Google indicated that it was resisting a Justice Department subpoena requiring the company to provide the government with data on searches made by users.[4454] The Justice Department reportedly is seeking the data to help it in a court case to uphold the Child Online Protection Act (COPA), which was enacted to protect children using the Internet

---

[4451] Congressional Record, December 8, 2004, p. S11974.

[4452] Friel, Brian. Civil Liberties Board Has Yet To Get Off the Ground. National Journal, January 13, 2006. Available on the govexec.com website at [http://www.govexec.com/story_page.cfm?articleid=33176&dcn=todaysnews].

[4453] Drees, Caroline. "U.S. Civil Liberties Board Struggles Into Existence." Reuters, August 4, 2005, 12:33 (via Factiva).

[4454] Delaney, Kevin. Google to Buck U.S. on Data Request — Firm Resists Agency's Efforts to Obtain Scaled-Back List of Web Sites, Search Queries. Wall Street Journal, January 20, 2006, p. A3 (via Factiva).

from objectionable material such as pornography.[4455] According to various media reports, other search engine companies, including Yahoo!, MSN, and America Online, did comply with the government's request. Although much of the publicity focused on the extent to which the privacy of Internet users would be undermined if the government could access such data, some observers pointed out that the data are anonymous, and Google's response might be stimulated more by business concerns (e.g., revealing proprietary information) than privacy concerns.[4456] Nevertheless, public response suggests that some consumers now worry about what search terms they use, lest the government track their activities and draw erroneous conclusions.[4457]

By Employers

There also is concern about the extent to which employers monitor the e-mail and other computer activities of employees. The public policy concern appears to be not whether companies should be able to monitor activity, but whether they should notify their employees of that monitoring. A 2005 survey of 526 companies by the American Management Association and the ePolicy Institute found that 76% monitor Web usage, and 55% retain and review e-mail messages.[4458] The survey found that 26% of the companies had fired employees for misusing the Internet, and 25% had fired workers for e-mail misuse. Regarding notice, the survey reported that 80% of the companies inform workers that they are monitoring content, keystrokes, and time spent at the keyboard; 82% inform workers that computer files are stored and reviewed; 86% inform workers that e-mail is monitored; and 89% inform workers that Web usage is tracked. One criticism is that top level employees may not be subject to the same monitoring as rank and file workers.[4459]

By E-Mail Service Providers: The "Councilman Case"

In what is widely-regarded as a landmark ruling concerning Internet privacy, the U.S. Court of Appeals for the First Circuit in Massachusetts ruled (2-1) on June

---

[4455] For a discussion of COPA, see CRS Report RS21328, Internet: Status of Legislative Attempts to Protect Children from Unsuitable Material on the Web, by Marcia S. Smith.

[4456] Liptak, Adam. In Case About Google's Secrets, Yours Are Safe. New York Times, January 26, 2006, p. 1 (via Factiva).

[4457] Hafner, Katie. After Subpoenas, Internet Searches Give Some Pause. New York Times, January 25, 2006, p. 1 (via Factiva).

[4458] American Management Association. "2005 Electronic Monitoring & Surveillance Survey." Press Release, May 18, 2005. [http://www.amanet.org/press/amanews/ems05.htm].

[4459] Sandberg, Jared. "Monitoring of Workers is Boss's Right But Why Not Include Top Brass?," Wall Street Journal, May 18, 2005, p. B1 (via Factiva).

29, 2004 that an e-mail service provider did not violate federal wiretapping statutes when it intercepted and read subscribers' e-mails to obtain a competitive business advantage. The ruling upheld the decision of a lower court to dismiss the case.

The case involved an e-mail service provider, Interloc, Inc., that sold out-of-print books. According to press accounts[4460] and the text of the court's ruling,[4461] Interloc used software code to intercept and copy e-mail messages sent to its subscribers (who were dealers looking for buyers of rare and out-of-print books) by competitor Amazon.com. The e-mail was intercepted and copied prior to its delivery to the recipient so that Interloc officials could read the e-mails and obtain a competitive advantage over Amazon.com. Interloc Vice President Bradford Councilman was charged with violating the Wiretap Act.[4462] The court's majority opinion noted that the parties stipulated that, at all times that the Interloc software was performing operations on the e-mails, they existed in the random access memory or in hard drives within Interloc's computer system.

The case turned on the distinction between the e-mail being in transit, or in storage (and therefore governed by a different law).[4463] The government argued that the e-mails were copied contemporaneously with their transmission, and therefore were intercepted under the meaning of the Wiretap Act. Judges Torruella and Cyr concluded, however, that they were in temporary storage in Interloc's computer system, and therefore were not subject to the provisions of the Wiretap Act. They further stated that "We believe that the language of the statute makes clear that Congress meant to give lesser protection to electronic communications than wire and oral communication. Moreover, at this juncture, much of the protection may have been eviscerated by the realities of modern technology.... However, it is not the province of this court to graft meaning onto the statute where Congress has spoken plainly." (p. 14-15). In his dissent, Judge Lipez stated, conversely, that he did not believe Congress intended for e-mail that is temporarily stored as part of the transmission process to have less privacy than messages as they are in transit. He agreed with the government's contention that

---

[4460] (1) Jewell, Mark. "Interception of E-Mail Raises Questions." Associated Press, June 30, 2004, 9:14 pm. (2) Zetter, Kim. "E-Mail Snooping Ruled Permissible." Wired News, June 30, 2004, 08:40. (3) Krim, Jonathan. "Court Limits Privacy of E-Mail Messages; Providers Free to Monitor Communications." Washington Post, July 1, 2004, E1 (via Factiva).

[4461] U.S. v. Bradford C. Councilman. U.S. Court of Appeals for the First Circuit. No. 03-1383. [http://www.ca1.uscourts.gov/pdf.opinions/03-1383-01A.pdf].

[4462] The Wiretap Act,18 U.S.C. §§ 2510-2522, is Title I of the Electronic Communications Privacy Act (ECPA), P.L. 99-508. According to Jewell, op. cit., two other defendants — Alibris, which bought Interloc in 1998, and Interloc's systems administrator — pleaded guilty.

[4463] Stored communications are covered by the Stored Communications Act, which is Title II of ECPA, 18 U.S.C. §§ 2701-2711.

an "intercept" occurs between the time the author hits the "send" button and the message arrives in the recipient's in-box. He concluded that "Councilman's approach to the Wiretap Act would undo decades of practice and precedent ... and would essentially render the act irrelevant.... Since I find it inconceivable that Congress could have intended such a result merely by omitting the term 'electronic storage' from its definition of 'electronic communication,' I respectfully dissent."[4464]

Privacy advocates expressed deep concern about the ruling. Electronic Frontier Foundation (EFF) attorney Kevin Bankston stated that the court had "effectively given Internet communications providers free rein to invade the privacy of their users for any reason and at any time."[4465] The five major ISPs (AOL, Earthlink, Microsoft, Comcast, and Yahoo) all reportedly have policies governing their terms of service that state that they do not read subscribers' e-mail or disclose personal information unless required to do so by law enforcement agencies.[4466] The U.S. Department of Justice appealed the court's decision; and several civil liberties filed a "friend of the court" brief in support of the government's appeal. In August 2005, the First Circuit Court of Appeals overturned the lower court's decision 5-2.[4467]

Two bills were introduced in the 108th Congress that would have affected this debate by amending either the Wiretap Act or the Stored Communications Act. There was no action on either bill.

In the first session of the 109th Congress, H.R. 3503/S. 936 were introduced to amend the Wiretap Act to clarify that it applies "contemporaneous with transit, or on an ongoing basis during transit, through the use of any electronic, mechanical, or other device or process, notwithstanding that the communication may simultaneously be in electronic storage." There was no action on the bills in 2005.

Spyware

Spyware is discussed in more detail in CRS Report RL32706, *Spyware: Background and Policy Issues for Congress*, by Marcia Smith. The term "spyware" is not well defined. One example of spyware is software products that include, as part of the software itself, a method by which information is collected

---

[4464] U.S. v. Bradford C. Councilman, p. 53.

[4465] Online Privacy "Eviscerated" by First Circuit Decision. June 29, 2004. [http://www.eff.org/news/archives/2004_06.php#001658].

[4466] Krim, op. cit.

[4467] McCullagh, Declan. "E-mail Wiretap Case Can Proceed, Court Says." c|net News.com, August 11, 2005, 14:30:00 PDT.

about the use of the computer on which the software is installed. Some products may collect personally identifiable information (PII). When the computer is connected to the Internet, the software periodically relays the information back to the software manufacturer or a marketing company. Some software traces a user's Web activity and causes advertisements to suddenly appear on the user's monitor — called "pop-up" ads — in response. Such software is called "adware," and one aspect of the spyware debate is whether adware should be included in the definition of spyware. Software programs that include spyware can be sold or provided for free, on a disk (or other media) or downloaded from the Internet. Typically, users have no knowledge that spyware is on their computers.

A central point of the debate is whether new laws are needed, or if industry self-regulation, coupled with enforcement actions under existing laws such as the Federal Trade Commission Act, is sufficient. The lack of a precise definition for spyware is cited as a fundamental problem in attempting to write new laws. FTC representatives and others caution that new legislation could have unintended consequences, barring current or future technologies that might, in fact, have beneficial uses. They further insist that, if legal action is necessary, existing laws provide sufficient authority. Consumer concern about control of their computers being taken over by spyware leads others to conclude that legislative action is needed.

Utah and California have passed spyware laws, but there is no specific federal law regarding spyware. In the 108th Congress, the House passed two bills (H.R. 2929 and H.R. 4661) and the Senate Commerce Committee reported S. 2145. There was no further action.

Two bills passed the House in the first session of the 109th Congress : H.R. 29 (Bono) and H.R. 744 (Goodlatte). Two bills specific to spyware were introduced in the Senate: S. 687 (Burns-Wyden), and S. 1004 (Allen). A Senate Commerce Committee hearing on S. 687 was held on May 11, 2005. On November 17, 2005, the committee ordered reported S. 687, and defeated S. 1004, with committee Chairman Stevens reportedly saying that he hoped a compromise could be reached before the issue was debated on the floor.[4468] Meanwhile, the FTC endorsed a different bill, S. 1608, at a hearing before a Senate Commerce subcommittee on October 5, 2005. That bill deals not only with spyware, but with other Internet-related fraud, including spam. Its focus is enhancing the FTC's ability to investigate and prosecute perpetrators who are located abroad or who use foreign intermediaries. For more information, see CRS Report RL32706, Spyware: Background and Policy Issues for Congress, by Marcia Smith.

[4468] Stables, Eleanor. Panel Approves Slew of Transportation, Spyware and Other Bills in Markup. CQ.com, November 17, 2005.

Identity Theft (Including Phishing and Pharming)

Identity theft is not an Internet privacy issue, but the perception that the Internet makes identity theft easier means that it is often discussed in the Internet privacy context. The concern is that the widespread use of computers for storing and transmitting information is contributing to the rising rate of identity theft over the past several years, where one individual assumes the identity of another using personal information such as credit card and Social Security numbers (SSNs). The FTC has a toll free number (877-ID-THEFT) to help victims.[4469]

The extent to which the Internet is responsible for the increase in cases is debatable. Some attribute the rise instead to carelessness by businesses in handling personally identifiable information, and by credit issuers that grant credit without proper checks. More traditional methods of acquiring someone's personal information — from lost or stolen wallets, or "dumpster diving" — also are used by identity thieves. Three high profile incidents that became public in early 2005 where the security of consumer PII was compromised reinforced existing fears about identity theft. The companies involved are ChoicePoint, Bank of America, and LexisNexis. These incidents are described in CRS Report RS22082, Identity Theft: The Internet Connection, by Marcia Smith.

Identity Theft Statistics

In a 2003 survey for the FTC, Synovate found that 51% of victims knew how their personal information was obtained by the thief: 14% said their information was obtained from lost or stolen wallets, checkbooks, or credit cards; 13% said the personal information was obtained during a transaction; 4% cited stolen mail; and 14% said the thief used "other" means (e.g. the information was misused by someone who had access to it such as a family member or workplace associate).[4470]

Another survey, conducted by the Council of Better Business Bureaus and Javelin Strategy & Research, was released in January 2005.[4471] The 2005 Identity Fraud Survey is based on data collected in 2004 by Synovate using questions that

---

[4469] See also CRS Report RL31919, Remedies Available to Victims of Identity Theft; and CRS Report RS21083, Identity Theft and the Fair Credit Reporting Act: an Analysis of TRW v. Andrews and Current Legislation, both by Angie Welborn.

[4470] Synovate. " Federal Trade Commission — Identity Theft Survey Report." September 2003. pp. 30-31. [http://www.ftc.gov/opa/2003/09/idtheft.htm]

[4471] An abbreviated "complimentary" version of the report is available at [http://www.javelinstrategy.com/reports/2005IdentityFraudSurveyReport.html]. A Better Business Bureau press release is at [http://www.bbb.org/alerts/article.asp?ID=565]. The survey was sponsored Checkfree, Visa, and Wells Fargo & Company, but the report emphasizes that although those companies were invited to comment on the content of the questionnaire, they were not involved in the tabulation, analysis, or reporting of final results.

closely mirrored those used in the 2003 FTC survey, plus several new questions. The survey found that computer crime accounted for 11.6% of identity theft cases in 2004, compared with 68% from paper sources. It further found that the average loss for online identity theft was $551 compared to $4,543 from paper sources. In cases where the perpetrator could be identified, family members were responsible for 32% of cases; complete strangers outside the workplace for 24%; friends, neighbors, and in-home employees for 18%; someone at a company with access to personal information for 13%; someone at the victim's workplace for 4%; or "someone else" for 8%. The study concluded that, contrary to popular perception, identity theft is not getting worse. For example, it reported that the number of victims declined from 10.1 million in 2003 to 9.3 million in 2004, and the annual dollar volume, adjusted for inflation, is "highly similar" ($52.6 billion) in the 2003 survey and this survey.

On January 25, 2006, the FTC released its most recent data about the top ten consumer fraud complaints.[4472] Identity theft represented 37% of the 686,683 complaints filed with the FTC in 2005. Although the total number of ID theft complaints was higher than in the two previous years (255,565 in 2005 compared with 246,847 in 2004 and 215,177 in 2004), as a percentage of complaints filed with the FTC, the 2005 figure was less (37% in 2005 compared with 38% in 2004 and 40% in 2003). Credit card fraud was identified as the most common form of identity theft (26%), compared with phone or utilities fraud (18%), bank fraud (17%), employment fraud (12%), government documents/benefits fraud (9%), and loan fraud (5%).

"Phishing" and "Pharming"

One method used to obtain PII is called "phishing." It refers to an Internet-based practice in which someone misrepresents their identity or authority in order to induce another person to provide PII. Some common phishing scams involve e-mails that purport to be from financial institutions or ISPs claiming that a person's record has been lost. The e-mail directs the person to a website that mimics the legitimate business' website and asks the person to enter a credit card number and other PII so the record can be restored. In fact, the e-mail or website is controlled by a third party who is attempting to extract information that will be used in identity theft or other crimes. The FTC issued a consumer alert on phishing in June 2004.[4473] An "Anti-Phishing Working Group" industry association has been established to collectively work on solutions to phishing [http://www.antiphishing.org/].

[4472] FTC. Consumer Fraud and Identity Theft Complaint Data: January -December 2005. [http://www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf].

[4473] FTC. "How Not to Get Hooked by a 'Phishing" Scam." June 2004. [http://www.ftc.gov/bcp/conline/pubs/alerts/phishingalrt.pdf].

A version of phishing, dubbed "pharming," involves fraudulent use of domain names.[4474] In pharming, hackers hijack a legitimate website's domain name, and redirect traffic intended for that website to their own. The computer user sees the intended website's address in the browser's address line, but instead, he or she is connected to the hacker's site and may unknowingly provide PII to the hacker.[4475]

Existing Laws

The FTC enforces three federal laws that restrict disclosure of consumer information and require companies to ensure the security and integrity of the data in certain contexts — Section 5 of the Federal Trade Commission Act, the Fair Credit Reporting Act (FCRA), and Title V of the Gramm-Leach-Bliley Act. FTC Chairwoman Deborah Platt Majoras summarized these laws as they pertain to identity theft at a March 10, 2005 hearing before the Senate Committee on Banking, Housing, and Urban Affairs.[4476] She identified two other laws that are not enforced by the FTC, but which also restrict the disclosure of certain types of information: the Driver's Privacy Protection Act, and the Health Insurance Portability and Accountability Act.

Congress also has passed laws specifically regarding identity theft: the 1998 Identity Theft and Assumption Deterrence Act; the 2003 Fair and Accurate Credit Transactions (FACT) Act; and the 2004 Identity Theft Penalty Enhancement Act. Those laws are summarized in CRS Report RL31919, Remedies Available to Victims of Identity Theft, by Angie Welborn. Briefly, the Identity Theft and Assumption Deterrence Act (P.L.105-318) directed the FTC to establish a central repository for identity theft complaints, and provide victim assistance and consumer education.

The FACT Act (P.L. 108-159) contains perhaps the most comprehensive identity theft provisions in federal law. Implementation of that act is discussed in CRS Report RL32535, Implementation of the Fair and Accurate Credit Transactions (FACT) Act, by Angie Welborn. Among its identity theft-related provisions, the law:

- requires consumer reporting agencies (CRAs) to follow certain procedures concerning when to place, and what to do in response to, fraud alerts on consumers' credit files;

[4474] For more on domain names, and the DNS, see CRS Report 97-868, Internet Domain Names: Background and Policy Issues, by Lennard G. Kruger.

[4475] For more on pharming, see, for example, Delio, Michelle. "Pharming Out-Scams Phishing." March 14, 2005 [http://www.wired.com/news/infostructure/0,1377,66853,00.html].

[4476] Available at [http://banking.senate.gov/_files/majoras.pdf].

- allows consumers one free copy of their consumer report each year from nationwide CRAs as long as the consumer requests it through a centralized source under rules to be established by the FTC;[4477]
- allows consumers one free copy of their consumer report each year from nationwide specialty CRAs (medical records or payments, residential or tenant history, check writing history, employment history, and insurance claims) upon request pursuant to regulations to be established by the FTC;
- requires credit card issuers to follow certain procedures if additional cards are requested within 30 days of a change of address notification for the same account;
- requires the truncation of credit card numbers on electronically printed receipts;
- requires business entities to provide records evidencing transactions alleged to be the result of identity theft to the victim and to law enforcement agencies authorized by the victim to take receipt of the records in question;
- requires CRAs to block the reporting of information in a consumer's file that resulted from identity theft and to notify the furnisher of the information in question that it may be the result of identity theft;
- requires federal banking agencies, the FTC, and the National Credit Union Administration to jointly develop guidelines for use by financial institutions, creditors and other users of consumer reports regarding identity theft; and
- extends the statute of limitations for when identity theft cases can be brought.

The Identity Theft Penalty Enhancement Act (P.L. 108-275) makes aggravated identity theft in conjunction with felonies a crime, and establishes mandatory sentences — two additional years beyond the penalty for the underlying crime, or five additional years for those who steal identities in conjunction with a terrorist act.[4478]

At the March 10, 2005 Senate Banking Committee hearing,[4479] FTC Chairwoman Majoras discussed the"complicated maze" of laws that governs consumer data, noting whether particular legal provisions apply depends on the type of company or institution involved, the type of data collected or sold, and the purpose for which it will be used. She conceded that it is not clear if data brokers like

---

[4477] The FTC rules on free credit reports were issued on June 4, 2004 and are available at [http://www.ftc.gov/opa/2004/06/freeannual.htm].

[4478] "Senate Clears Tougher Penalties for Identity Theft in Conjunction with Felony." CQ Weekly, June 26, 2004, p. 1561.

[4479] The hearing can be viewed on the committee's website at [http://banking.senate.gov/index.cfm?Fuseaction=Hearings.Detail&HearingID=142].

ChoicePoint come under the FTC's jurisdiction, and concluded that additional legislation may be necessary, particularly regarding notice and security. A witness from the Secret Service also testified about his agency's jurisdiction over identity theft crimes.

Legislation in the 109th Congress, 1st Session

Congress continues to consider ways to reduce the incidence of identity theft. Legislative approaches include strengthening penalties for identity theft or for the misuse of SSNs;[4480] increasing regulation of data brokers, such as by requiring them to notify individuals whose PII has been breached, or to obtain a consumer's consent before selling PII; limiting the use of SSNs or allowing individuals to choose an identifier other than their SSN for Medicare purposes, for example; or making phishing unlawful.

Despite the widespread attention to these issues, and the introduction of many bills, no legislation to further address identity theft or to regulate data brokers passed during the first session of the 109th Congress. Four bills were acted upon in committee or subcommittee, however (H.R. 4127, S. 1326, S. 1408, and S. 1789). According to the Wall Street Journal, legislative action stalled because of differing views among the various stakeholders in the debate.

> *Consumer groups are pushing for credit protections that financial institutions oppose. Small banks are arguing with larger ones about who picks up the 'reissuing costs' when credit or debit cards must be replaced. And everyone with a stake in the issue is debating the 'notification trigger,' specifying what breaches require altering customers.*[4481]

The markup of H.R. 4127 (Stearns) by the House Energy and Commerce Subcommittee on Commerce, Trade, and Consumer Protection was spirited, and the vote split on party lines.[4482] The Senate Judiciary Committee reported S. 1326 (Sessions) without amendment and without written report on October 20, 2005. By contrast, the markup of S. 1789 (Specter) by the same committee on October 27, 2005 involved considerable debate.[4483] The Senate Commerce, Science, and

---

[4480] For more on Social Security numbers, see CRS Report RL30318, The Social Security Number: Legal Developments Affecting Its Collection, Disclosure, and Confidentiality, by Kathleen S. Swendiman.

[4481] Conkey, Christopher. Identity-Theft Bills Stall in Congress. Wall Street Journal, November 26, 2005, p. A4 (via Factiva).

[4482] Krim, Jonathan. Parties Split on Data-Protection Bill. Washington Post, November 4, 2005, p. D 4 (via Factiva).

[4483] Ibid.

Transportation Committee reported S. 1408 (Smith), amended, on December 8, 2005. See Table 1 for brief descriptions of the bills and associated report numbers.

For more on legislative action, see CRS Report RL31919, Remedies Available to Victims of Identity Theft, by Angie Welborn.

Summary of Internet Privacy-Related Legislation in the 109th Congress, 1st Session

The following table provides summary information on Internet privacy-related legislation introduced in the first session of the 109th Congress. It should be noted that although some bills have similar titles or intents, the details may vary. For example, some bills seek to protect "personal information," while others protect "personally identifiable information" (PII). Some concern "data," while others concern "electronic data." Definitions may vary, or, in some cases, the FTC is directed to determine a definition.

(*Tables excluded)

Terrorism: Internet Privacy: Law Enforcement Monitoring of E- Mail and Web Usage, EBTER135 (August 17, 2004).

MARCIA S. SMITH, CONG. RESEARCH SERV., TERRORISM: INTERNET PRIVACY: LAW ENFORCEMENT MONITORING OF E- MAIL AND WEB USAGE (2004), *available at* http://www.intelligencelaw.com/library/secondary/crs/pdf/EBTER135_8-17-2004.pdf.

EBTER135 Updated August 17, 2004
Congressional Research Service

Issue Definition

To what extent should law enforcement and government officials be permitted to monitor individuals' Internet usage, including electronic mail and website visits, and how have the terrorist attacks of September 11, 2001 affected this debate?

Current Situation

On October 26, 2001, six weeks after the terrorist attacks, President Bush signed into law the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act, P.L _107-56. Among its many provisions, the Act gives law enforcement authorities additional authority to monitor individuals' Internet activity, including e-mail and website visits. Amendments passed the next year as part of the Homeland Security Act (P.L. 107-296) expanded the circumstances under which Internet Service Providers may voluntarily divulge the content of communications, and to whom. The Congress and civil liberties groups are monitoring how the Act is implemented. Some of the Act's provisions, including several related to the Internet, are subject to a December 31, 2005, sunset clause. S. 1695 (Leahy) and S.. ._1709 (Craig) would sunset more of the sections, while S. 2476 (Kyl) would repeal the sunset clause. The July 2004 "9/11 Commission report" called for a full and informed debate about the PATRIOT Act, and concluded that security and liberty must be reconciled.

Policy Analysis

The September 11, 2001, terrorist attacks sharpened the debate over how to strike a balance between law enforcement's need to investigate criminals, and protecting what most citizens believe to be their "right" to privacy. Internet privacy is only one part of this debate, but it was highlighted in the summer of 2000 by the revelation that the FBI was using a software program called Carnivore (later renamed DCS 1000) that it installed on the equipment of Internet Service Providers to monitor electronic mail (e-mail) and website visits of suspects. Privacy advocates worried that the software was not sufficiently sophisticated to distinguish between the e-mail and Web activity of a suspect and that of other ISP subscribers, thereby violating the latter's privacy.

Prior to the terrorist attacks, congressional attention focused on requiring reports from the Department of Justice on its use of Carnivore or similar systems to help assess whether the FBI was exceeding its authority to monitor Internet usage. However, some policymakers had sought expansion, rather than limitation, of law enforcement authority to monitor wire and electronic communications. Following the terrorist attacks, they accelerated efforts to provide law enforcement officials with additional authorities. Many of these were provided in the PATRIOT Act. Some Members of Congress and privacy advocates were concerned that, in an emotionally charged climate, Congress was passing legislation too hurriedly. Groups such as the American Civil Liberties Union (ACLU), Center for Democracy and Technology (CDT), and Electronic Privacy Information Center (EPIC) urged caution, fearful that, in an attempt to track down and punish the terrorists who threaten American democracy, one of the fundamental tenets of that democracy --privacy --may itself be threatened.

On July 13, 2004, Attorney General Ashcroft released Report from the Field: The USA PATRIOT Act At Work providing an overview of "how the Act has been instrumental in the effort to combat terrorism and make Americans safer." The report cites several instances in which Sec. 210, Sec. 212, and Sec. 216 were instrumental in law enforcement actions. Some critics noted that the report did not address all aspects of the PATRIOT Act, particularly a controversial topic that was the subject of House floor debate in July 2004 (specifically, access to library records, which is outside the scope of this briefing book entry).

On July 22, 2004, the 9/11 Commission issued its report on the terrorist attacks (Final Report of the National Commission on Terrorist Attacks Upon the United States) .The Commission concluded (pp. 394-395) that many of the PATRIOT Act provisions appear beneficial, but that "Because of concerns regarding the shifting balance of power to the government, we think that a full and informed debate on the Patriot Act would be healthy." The Commission recommended that "The burden of proof for retaining a particular governmental power should be on the executive, to explain (a) that the power actually materially enhances security and (b) that there is adequate supervision of the executive's use of the powers to ensure protection of civil liberties. If the power is granted, there must be adequate guidelines and oversight to properly confine its use." The Commission also called for creation of a board within the executive branch "to oversee adherence to the guidelines we recommend and the commitment the government makes to defend our civil liberties." The commissioners went on to say that "We must find ways of reconciling security with liberty, since the success of one helps protect the other. The choice between security and liberty is a false choice, as nothing is more likely to endanger America's liberties than the success of a terrorist attack at home. Our history has shown us that insecurity threatens liberty. Yet, if our liberties are curtailed, we lose the values that we are struggling to defend."

Options and Implications for U.S. Policy

Attention is focused on oversight of implementation of the PATRIOT Act's provisions, and whether certain provisions should expire ("sunset") after a specified period of time. Sec. 224 of the law includes a sunset date of December 31, 2005 for certain provisions . Some want to repeal the sunset date, while others want to extend it to other provisions of the law (see below).

Role of Congress/Legislation

As described above, in 2001 Congress passed the USA PATRIOT Act (P .k. 107.-56) that, inter a/ia, makes it easier for law enforcement officials to monitor Internet activities . Relevant provisions of Title II are:

- **Section 210**, which expands the scope of subpoenas for records of electronic communications to include records commonly associated with Internet usage, such as session times and duration.
- **Section 212**, which allows ISPs to divulge records or other information (but not the contents of communications) pertaining to a subscriber if they believe there is immediate danger of death or serious physical injury or as otherwise authorized, and requires them to divulge such records or information (excluding contents of communications) to a governmental entity under certain conditions . It also allows an ISP to divulge the contents of communications to a law enforcement agency if it reasonably believes that an emergency involving immediate danger of death or serious physical injury requires disclosure of the information without delay. [This section was amended by the Cyber Security Enhancement Act, seebelow.]
- **Section 216**, which adds routing and addressing information (used in Internet communications) to dialing information, expanding what information a government agency may capture using pen registers and trap and trace devices as authorized by a court order, while excluding the content of any wire or electronic communications . The section also requires law enforcement officials to keep certain records when they use their own pen registers or trap and trace devices and to provide those records to the court that issued the order within 30 days of expiration of the order. To the extent that Carnivore-like systems fall with the new definition of pen registers or trap and trace devices provided in the Act, that language would increase judicial oversight of the use of such systems.
- **Section 217**, which allows a person acting under color of law to intercept the wire or electronic communications of a computer trespasser transmitted to, through, or from a protected computer under certain circumstances, and
- **Section 224**, which sets a four-year sunset period (December 31, 2005) for many of the Title II provisions. Among the sections excluded from the sunset are Sections 210 and 216.

In 2002, Congress passed the Cyber Security Enhancement Act (H.R.. 348_2_) as part of the Homeland Security Act (P.L. 1 7-226). It amends Section 212,

lowering the threshold for when ISPs may divulge the content of communications, and to whom. Now ISPs need only a "good faith" belief(instead of a "reasonable" belief) that there is an emergency involving danger (instead of "immediate" danger) of death or serious physical injury . The contents can be disclosed to "a Federal, state, or local governmental entity" (instead of a "law enforcement agency"). Privacy advocates are concerned about the language for a number of reasons. For example, EPIC noted that allowing such information to be disclosed to any governmental entity not only poses increased risk to personal privacy but also is a poor security strategy and that the language does not provide for judicial oversight of the use of these procedures.

Under the current law, Sec. 212 and Sec. 217 are subject to the December 31, 2005, sunset date in Sec. 224, while Sec. 210 and Sec. 216 are not. S 1695 (Leahy) would amend the sunset provision such that Sec . 210 and Sec. 216 also would sunset. S,_1709 (Craig) would include Sec . 216 in the sunset clause. By contrast, S. 2476 (Kyl), would repeal Sec. 224 so that none of the provisions sunset.

CRS Products

CRS Report RL31408. Internet Privacy: Overview and Pending Legislation.
CRS Report RL31289(pdf). The Internet and the USA PATRIOT Act: Potential Implications for Electronic Privacy, Security, Commerce, and Government.
CRS Report RL31200(pdf). Terrorism : Section by Section Analysis of the USA PATRIOT Act.
CRS Report 98-326 (pdf). Privacy: an Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping.

Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations, R40427 (March 10, 2009).

JOHN ROLLINGS & ANNA C. HENNING, CONGRESSIONAL RESEARCH SERV., COMPREHENSIVE NATIONAL CYBERSECURITY INITIATIVE: LEGAL AUTHORITIES AND POLICY CONSIDERATIONS (2009), *available at* http://www.intelligencelaw.com/library/secondary/crs/pdf/R40427_3-10-2009.pdf.

John Rollins
Specialist in Terrorism and National Security
jrollins@crs.loc.gov, 7-5529

Anna C. Henning
Legislative Attorney
ahenning@crs.loc.gov, 7-4067

March 10, 2009

Summary

Federal agencies report increasing cyber-intrusions into government computer networks, perpetrated by a range of known and unknown actors. In response, the President, legislators, experts, and others have characterized cybersecurity as a pressing national security issue.

Like other national security challenges in the post-9/11 era, the cyber threat is multi-faceted and lacks clearly delineated boundaries. Some cyber attackers operate through foreign nations' military or intelligence-gathering operations, whereas others have connections to terrorist groups or operate as individuals. Some cyber threats might be viewed as international or domestic criminal enterprises.

In January 2008, the Bush Administration established the Comprehensive National Cybersecurity Initiative (the CNCI) by a classified joint presidential directive. The CNCI establishes a multi-pronged approach the federal government is to take in identifying current and emerging cyber threats, shoring up current and future telecommunications and cyber vulnerabilities, and responding to or proactively addressing entities that wish to steal or manipulate protected data on secure federal systems. On February 9, 2009, President Obama initiated a 60-day interagency cybersecurity review to develop a strategic framework to ensure the CNCI is being appropriately integrated, resourced, and coordinated with Congress and the private sector.

In response to the CNCI and other proposals, questions have emerged regarding: (1) the adequacy of existing legal authorities—statutory or constitutional—for responding to cyber threats; and (2) the appropriate roles for the executive and legislative branches in addressing cybersecurity. The new and emerging nature of cyber threats complicates these questions. Although existing statutory provisions might authorize some modest actions, inherent constitutional powers currently provide the most plausible legal basis for many potential executive responses to national security related cyber incidences. Given that cyber threats originate from various sources, it is difficult to determine whether actions to prevent cyber-attacks fit within the traditional scope of executive power to conduct war and foreign affairs. Nonetheless, under the Supreme Court jurisprudence, it appears that the President is not prevented from taking action in the cybersecurity arena, at least until Congress takes further action. Regardless, Congress has a continuing oversight and appropriations role. In addition, potential government responses could be limited by individuals' constitutional rights or international laws of war. This report discusses the legal issues and addresses policy considerations related to the CNCI.

Introduction

Cybersecurity has been called "one of the most urgent national security problems facing the new administration."[4484] Cyber and telecommunications activities are sometimes conflated to indicate the same meaning or capability. One might distinguish the term cyber from that of telecommunications with the former being the data or applications residing on the latter which is the electronic medium in which the activity occurs. Electronic information systems, also termed "information infrastructures," now support a wide range of security and economic assets in the public and private sectors.

Such systems have been successfully infiltrated in recent years by a range of attackers, some of whom are suspected to have been working in coordination with foreign military organizations or (foreign) state intelligence services. Thus, like the changing nature of U.S. enemies in the post9/11 environment, the nature of military and economic vulnerabilities has changed: intelligence-gathering battles in cyberspace now also play a crucial role in national security.

In January 2008, the Bush Administration initiated the Comprehensive National Cybersecurity Initiative (the CNCI) to make the United States more secure against cyber threats. The Homeland Security Presidential Directive 23 and National Security Presidential Directive 54 establishing the CNCI are classified. Some details of the Initiative have been made public in Departmental press releases, speeches by executive branch leaders, and analysis and insight offered by individuals that follow cyber security and terrorism related issues. The CNCI

[4484] Center for Strategic and International Studies, Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency (2008).

"establishes the policy, strategy, and guidelines to secure federal systems."[4485] The CNCI also delineates "an approach that anticipates future cyber threats and technologies, and requires the federal government to integrate many of its technical and organizational capabilities to better address sophisticated threats and vulnerabilities."[4486] Subsequent to the issuance of the classified directives, congressional committees have held hearings regarding the CNCI and heard testimony from a commission established to address necessary cybersecurity reforms.[4487]

In a speech during his presidential campaign, President Obama promised to "make cyber security the top priority that it should be in the 21st century … and appoint a National Cyber Advisor who will report directly" to the President.[4488] Although the Obama Administration might craft a new approach to cybersecurity, some experts have urged the new administration to build on the CNCI, which they note is a "major step toward improving federal cybersecurity."[4489] On February 9, 2009, President Obama directed a 60-day interagency cybersecurity review to develop a strategic framework to ensure the CNCI is being appropriately integrated, resourced, and coordinated with Congress and the private sector.[4490]

The new administration's focus on cybersecurity would continue recent emphasis on the issue by the executive and legislative branches. This recent focus emerged partly in response to events such as attacks by outside hackers against a Pentagon computer network and the CyberWar against Estonia, which garnered significant

---

[4485] Department of Homeland Security, Fact Sheet: DHS 2008 End of Year Accomplishments (Dec. 18, 2008), http://www.dhs.gov/xnews/releases/pr_1229609413187.shtm.

[4486] Id.

[4487] See, e.g., House Permanent Select Committee on Intelligence, Cyber Security: Hearing on the Nation's Cyber Security Risks, 110th Cong. (Sept. 18, 2008); House Homeland Security Committee, Cybersecurity Recommendations for the Next Administration: Hearing Before the Subcommittee on Emerging Threats, Cybersecurity and Science and Technology, 110th Cong. (Sept. 16, 2008).

[4488] July 17, 2008 speech at Purdue University. As of the date of this report a national Cyber Security Advisor has not been named.

[4489] Center for Strategic and International Studies, Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency 3 (2008) (including "do not start over" as one of its recommendations for the 44th presidency).

[4490] The White House, Office of the press Secretary, President Obama Directs the National Security and Homeland Security Advisors to Conduct Immediate Cyber Security Review (Feb. 9, 2009), http://www.whitehouse.gov/the_press_office/AdvisorsToConductImmediateCyberSecurityReview/.

media attention. Agency reports of large numbers of attempts to infiltrate government cyberspace have also prompted action. Both the high-profile attacks and more routine infiltrations have shed light on the vulnerability of critical information infrastructures. For example, the Defense Science Board noted that the U.S. military's information infrastructure is the "Achilles' heel of our otherwise overwhelming military might."[4491]

Background on Cyber Threats and Calls for Executive Action

Threats to the U.S. cyber and telecommunications infrastructure are constantly increasing[4492] and evolving as are the entities that show interest in using a cyber-based capability to harm the nation's security interests.[4493] Concerns have been raised since the 1990s regarding the use of the internet and telecommunications components to cause harm to the nation's security interests. Activities producing undesirable results include unauthorized intrusion to gain access and view protected data, stealing or manipulating information contained in various databases, and attacks on telecommunications devices to corrupt data or cause infrastructure components to operate in an irregular manner. Of paramount concern to the national and homeland security communities is the threat of a cyber related attack against the nation's critical government infrastructures – "systems and assets, physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health and safety, or any combination of those matters."[4494] Early concerns noted attacks on components of the energy grid, infrastructure control systems, and military

---

[4491] Department of Defense, Defense Science Board, Defense Imperatives for the New Administration 3 (2008), http://www.acq.osd.mil/dsb/reports/2008-11-Defense_Imperatives.pdf.

[4492] Peter Eisler, Reported Raids on Federal Computer Data Soar, USA Today (Feb. 17, 2009), http://www.usatoday.com/news/washington/2009-02-16-cyber-attacks_N.htm?csp=34. Based on data reportedly provided to USA Today, the U.S. Computer Emergency Readiness Team (US-CERT), a Department of Homeland Security entity, found that known cyberattacks on U.S. government networks rose 40% in 2008 compared to 2007. While this survey focused on U.S. government computer systems, telecommunications networks are maintained by private industry, and any degradation to these services or components would necessarily have negative implications for both public and private cyber activities.

[4493] For more information on cyberattackers' capabilities, see CRS Report RL33123, Terrorist Capabilities for Cyberattack: Overview and Policy Issues, by John Rollins and Clay Wilson.

[4494] 42 U.S.C . §5195c(e). For more on U.S. efforts to protect critical infrastructures, see CRS Report RL30153, Critical Infrastructures: Background, Policy, and Implementation, by John D. Moteff.

equipment as examples of telecommunications based threats to physical infrastructures.[4495]

In response, the Department of Energy conducted an experiment in 2007 in which the control system of an unconnected generator, containing similar components as that of larger generators connected to many power grids in the nation supplying electricity, was damaged and became inoperable.[4496] While data from federal agencies demonstrate that the majority of attempted and successful cyber attacks to date have targeted virtual information resources rather than physical infrastructures,[4497] many security experts are concerned that the natural progression of those wishing to harm U.S. security interests will transition from stealing or manipulating data to undertaking action that temporarily or permanently disables or destroys the telecommunication network or affects infrastructure components. Many security observers agree that the United States currently faces a multi-faceted, technologically based vulnerability in that "our information systems are being exploited on an unprecedented scale by state and non-state actors [resulting in] a dangerous combination of known and unknown vulnerabilities, strong adversary capabilities, and weak situational awareness."[4498] This, coupled with security observers' contention that the United States lacks the capability to definitively ascertain perpetrators who might unlawfully access a database or cause harm to a network, leaves the nation increasingly at risk. It also causes acts or discussions related to deterring cyberattacks to be ignored or negated by entities exploiting known or newly found vulnerabilities.

Prominent national security experts have emphasized the vulnerability of U.S. infrastructures. As recently as January 2009, former Director of National Intelligence (DNI) Mike McConnell equated "cyber weapons" with weapons of mass destruction when he expressed concern about terrorists' use of technology

---

[4495] Of note, many of the cyber-related incidences that were found to have negatively affected control systems connected to physical infrastructure components were resolved as being the work of current or former employees who had access to and knowledge of the architecture of the affected network.

[4496] Jeanne Meserve, Staged Cyber Attack Reveals Vulnerability in Power Grid, CNN online (Sep. 26, 2007), http://www.cnn.com/2007/US/09/26/power.at.risk/index.html#cnnSTCVideo. A video of the experiment, named Project Aurora, and the resulting damage to the generator is available on the CNN website.

[4497] See Center for Strategic and International Studies, Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency 12 (2008) ("we expected damage from cyber attacks to be physical (opened floodgates, crashing airplanes) when it was actually informational").

[4498] House Permanent Select Committee on Intelligence, Cyber Security: Hearing on the Nation's Cyber Security Risks, 110th Cong. (Sept. 18, 2008) (statement of Paul Kurtz, Former Senior Director, Critical Infrastructure Protection, White House Homeland Security Council).

to degrade the nation's infrastructure. In distinguishing between individuals gaining access to U.S. national security systems or corporate data for purposes of exploitation for purposes of competitive advantage, former Director McConnell noted that terrorists aim to damage infrastructure and that the "time is not too far off when the level of sophistication reaches a point that there could be strategic damage to the United States."[4499]

Similarly, in elaborating on the potential consequences of a cyber attack, newly confirmed DNI Dennis Blair offered the following statement during the Annual Threat Assessment of the Intelligence Community for the Senate Select Committee on Intelligence:

> *Growing connectivity between information systems, the Internet, and other infrastructures creates opportunities for attackers to disrupt telecommunications, electrical power, energy pipelines, refineries, financial networks, and other critical infrastructures. Over the past several years we have seen cyber attacks against critical infrastructure abroad, and many of our own infrastructures are as vulnerable as their foreign counterparts. A successful attack against a major financial service provider could severely impact the national economy, while cyber attacks against physical infrastructure computer systems such as this that control power grids or oil refineries have the potential to disrupt services for hours to weeks.*[4500]

Also describing the evolving threat to U.S. security interests from a cyber-facilitated incident, Melissa Hathaway, Senior Advisor to the DNI and Chair of the Nation Cyber Study Group and President Obama's appointee to lead the 60-day interagency strategic cyber review, wrote that "both state and non-state adversaries are targeting our information systems and infrastructure for exploitation and potential disruption or destruction."[4501] During the question and answer period of the most recent DNI Annual Threat Assessment of the Intelligence Community, Director Blair stated that a "cyber capability is not one in which I feel [terrorists] have the skills for the greatest destruction. I think that they have other terrible things they can do to us that they are working on harder, they're better able to do, and they seem to be more motivated to do. So [a cyber terrorist attack is] possible, but I don't think the combination of terror and cyber

---

[4499] The Charlie Rose Show, "Interview of Mr. Mike McConnell, Director of National Intelligence," PBS, January 8, 2009.

[4500] U.S. Congress, Senate Select Committee on Intelligence, Annual Threat Assessment of the Intelligence Community: Hearing on the Threats to the Nation, 111th Cong. (Feb. 12, 2009).

[4501] Melissa Hathaway, Cyber Security – An Economic and National Security Crisis, Intelligencer: Journal of U.S. Intelligence Studies, Fall 2008 at 31-6.

is the nexus that we are most worried about."[4502] However, threats could originate from foreign military or intelligence operatives rather than from terrorist groups.

In response to reports of the increasing pace and volume of cyber intrusions and a recognition that recent cyber-based threats have compelled the U.S. government to take security related actions that may negatively affect an agency's ability to perform its national security duties,[4503] legislators and analysts have expressed concerns that the current statutory framework inadequately addresses modern cybersecurity threats. One prominent voice is the Center for Strategic and International Studies' (CSIS) Commission on Cybersecurity for the 44th President, whose members testified before House and Senate committees and released its formal recommendations in fall 2008. The Commission recommended that federal cyber-crime provisions should be reexamined and that the "President should propose legislation that eliminates the current legal distinction between technical standards for national security systems and civilian agency systems and adopt a risk-based approach to federal computer security."[4504] In addition, it characterized the current statutory framework, particularly the Federal Information Security Management Act, enacted in 2002 to establish agency-level defenses against cyber threats, as too weak to effectively prevent cyber intrusions.[4505]

Legislators made some attempts during the 110th Congress to strengthen or "modernize" the existing statutory framework. For instance, a bill introduced by

---

[4502] U.S. Congress, Senate Select Committee on Intelligence, Annual Threat Assessment of the Intelligence Community: Hearing on the Threats to the Nation, 111th Cong. (Feb. 12, 2009).

[4503] In November, 2008, it was reported that the Department of Defense notified all organizations to stop using portable storage devices as it has become "apparent that over time, our posture to protect networks and associated information infrastructure has not kept pace with adversary efforts to penetrate, disrupt, interrupt, exploit or destroy critical elements of the global information grid." Noah Shachtman, Military USB Ban Meant to Stop Adversary Attacks, Wired Blog Network (Nov. 20, 2008), http://blog.wired.com/defense/2008/11/military-usb-ba.html. Also, it has recently been reported that some U.S. military units have resorted to disconnecting computer networks from the internet for fear of cyber related risks and a concern that the affected organization may not be managing its network properly thus "making everyone else vulnerable" to an attack. Noah Shachtman, Air Force Unplugs Bases' Internet Connections, Wired Blog Network (Feb. 18, 2000), http://blog.wired.com/defense/2009/02/air-force-cuts.html.

[4504] See Center for Strategic and International Studies, Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency 12 (2008) at 67.

[4505] See, e.g., Id. at 69 (stating that the Act "has become a paperwork exercise rather than an effective measure of network security"). The Federal Information Security Management Act is Title III of the E-Government Act of 2002, P.L. 107-347, 116 Stat. 2899 (codified at 44 U.S.C. §3541 et. seq.). Among other things, it created a position of Chief Information Officer within each federal agency.

Senator Carper, the Federal Information Security Management Act of 2008,[4506] would have added a "Chief Information Security Officer" position to supplement the Chief Information Officer position required in each federal agency under the Federal Information Security Management Act of 2002 and the Clinger-Cohen Act of 1996.[4507] However, analysts have argued that ultimately, no change to the existing statutory scheme will adequately equip executive agencies to prevent infiltrations into U.S. cyberspace. They argue that "only the White House has the necessary authority and oversight for cybersecurity."[4508]

Comprehensive National Cybersecurity Initiative and Concerns Regarding Transparency and Effectiveness

As of the date of this report, unclassified versions of the January 2008 directives establishing the CNCI have yet to be released. While the Initiative has yet to be legislatively recognized, presidential directives, sometimes considered types of executive orders and visa versa, have the force of law if they are supported by constitutional or statutory authority.[4509] Although much remains unknown about the CNCI due to the classified nature of the presidential directives and supporting implementation documents, federal government agency press releases and statements by government officials provide a bit of insight regarding the program. Some security observers are concerned that because the CNCI is focused on developing and adhering to strategies and policies to secure the federal systems, many of which rely on private sector telecommunications networks for service and support, and identifying current and emerging threats and vulnerabilities, it is incumbent on the federal government to improve its coordination activities with non-federal entities and undertake enhanced sharing of timely and relevant cybersecurity related plans and risk data.

Few details have been publicly released regarding the implementation activities or status of CNCI efforts since the establishment of the initiative. According to one media account, Steven Chabinsky, Deputy Director of the Joint Interagency

---

[4506] Federal Information Security Management Act of 2008, S. 3474, 110th Cong. (2008). The bill was favorably reported by the Senate Homeland Security and Government Affairs Committee and was placed on the Senate calendar. It has not yet been reintroduced during the 111th Congress.

[4507] 44 U.S.C. §3506 (requiring Chief Information Officer positions). The Clinger-Cohen Act is the name given to the Federal Acquisition Reform Act of 1996 and the Information Technology Management Reform Act of 1996, which passed as Sections D and E, respectively, of the National Defense Authorization Act for Fiscal Year 1996, P.L. 104106, 110 Stat. 642, 679 (1996).

[4508] House Homeland Sec. Comm., Cybersecurity Recommendations for the Next Administration: Hearing Before the Subcommittee on Emerging Threats, Cybersecurity and Science and Technology, 110th Cong. (Sept. 16, 2008) (statement of James A. Lewis, Director and Senior Fellow, Center for Strategic and International Studies).

[4509] For more information on presidential directives, see CRS Report 98-611, Presidential Directives: Background and Overview, by Harold C. Relyea.

Cyber Task Force for the Office of the DNI, stated at an information technology security conference that there are 12 objectives supporting the Initiative's goal of comprehensively addressing the nation's cyber security concerns. They are:

1. Move towards managing a single federal enterprise network;
2. Deploy intrinsic detection systems;
3. Develop and deploy intrusion prevention tools;
4. Review and potentially redirect research and funding;
5. Connect current government cyber operations centers;
6. Develop a government-wide cyber intelligence plan;
7. Increase the security of classified networks;
8. Expand cyber education;
9. Define enduring leap-ahead technologies;
10. Define enduring deterrent technologies and programs;
11. Develop multi-pronged approaches to supply chain risk management; and
12. Define the role of cyber security in private sector domains.[4510]

One question often raised is whether the CNCI objectives are being pursued concurrently. Some security observers are concerned that the government's focus to date has been on securing federal security systems at the expense of other networks that have similar vulnerabilities. The disruption, or perceived accessing or manipulating of data in non-federal networks that contain personal financial information or manage the control systems of the nation's critical infrastructure could have significant economic, safety, and confidence-in-government implications. It is often noted that in the homeland security and law enforcement communities, where a great deal of post9/11 emphasis is placed on continuous information exchange and collaboration, efforts to secure the federal technology systems, while relegating state, local, and private sector organizations to lower standards of security, will simply redirect or delay risk that inevitably accompanies increased collaboration. This concern is often expressed by non-federal governmental entities which rely on and routinely coordinate efforts with the U.S. government but have not been apprised of the plans or resources accompanying the CNCI.

Given the secretive nature of the CNCI, one of the common concerns voiced by many security experts is the extent to which non-federal entities should have a role in understanding the threat to the nation's telecommunications and cyber infrastructure and assist with providing advice, assistance, and coordination in preparation and response for ongoing and future intrusions and attacks.[4511] As

---

[4510] Wyatt Kash, Government Computer News, Details Merge About the President's Cyber Plan (Nov. 21, 2008), http://gcn.com/Articles/2008/11/21/Details-emerge-about-Presidents-Cyber-Plan.aspx?Page=4.

[4511] It is unknown whether non-federal entities have been invited to participate in the previously mentioned President's 60-day cyber security review that commenced on February 9, 2009.

telecommunications providers and internet service providers are corporate entities residing in the private sector, and are relied upon heavily to support federal government activities and services, many cyber-security observers suggest that a comprehensive approach to an effective monitoring, defending, and responding regime is not possible without the collaboration and expertise of the nation's cyber sector owners and operators. As evidenced in the twelve objectives of CNCI, it appears the federal government focus is on the prevention aspects of addressing potential threats to the nation's cyber and telecommunications infrastructure. In contrast, the primary response and recovery activities associated with previous network breaches have been addressed by the private sector entity that has been the victim of the attack. In an apparent admission of the need for further transparency and enhanced public-private partnership to better fulfill the goals of the CNCI, former President Bush's Assistant Secretary of Cybersecurity and Telecommunications at the Department of Homeland Security (DHS), Greg Garcia, recently stated that "there was too much classified (about the CNCI) which was not helpful politically and not helpful in getting the word out." Acknowledging the balance between incorporating the view of non-federal entities and the concern of allowing those that wish to use cyber activities to cause harm, Assistant Secretary Garcia went on to further state that the Department had to "walk the line between raised awareness of what was being accomplished and not letting out too much information that could cause us to be targeted. Still, too much was kept secret."[4512]

Based on the number of unknowns concerning the CNCI and the apparent lack of inclusiveness with the private sector telecommunication and internet providers, some analysts are concerned that future opportunities for successfully ascertaining known and future threats and developing a comprehensive set of legal and policy responses may not be achievable. An apparent Obama Administration goal for the current 60-day cyber security review is a more transparent and coordinated approach to the nation's cyber security risks with the perceived end result being that all affected parties are consulted and given the opportunity to provide advice and assistance in proposing changes to existing legislation, policy, and processes.[4513]

[4512] Jill Aitoro, Bush's Cyber Chief Calls National Security Initiative Too Secret, Nextgov (Feb. 11, 2009), http://www.nextgov.com/nextgov/ng_20090211_6858.php.

[4513] See Press Release, White House, President Obama Directs the National Security and Homeland Security Advisors to Conduct Immediate Cyber Security Review, (Feb. 9, 2009), http://www.whitehouse.gov/the_press_office/AdvisorsToConductImmediateCyberSecurityReview/.

Legal Authorities for Executive Branch Responses to Cyber Threats

As discussed, the CSIS report on Securing Cyberspace for the 44th Presidency recommends executive action to protect U.S. cyberspace.[4514] This and other calls for executive action, together with the 60-day review of the CNCI, implicate questions regarding legal authorities and the appropriate roles of the two political branches in the cybersecurity context. Questions concern the adequacy of existing statutes and the potential need for new legislation to address the modern threat. In addition, for actions not authorized by the existing statutory framework, questions arise regarding the extent of inherent authority for executive-branch responses under the U.S. Constitution.

To be legally authorized, the CNCI and any other executive-branch action must have some basis in statutory or constitutional law.[4515] Several disparate legal authorities offer potential bases for executive responses to cyber threats. These include: (1) various provisions in the criminal code that establish federal cybercrime offenses and authorize prosecution; (2) statutes, such as the Federal Information Security Management Act,[4516] which direct executive agencies to establish specific administrative procedures to prevent cyber attacks; (3) more general statutes authorizing executive management of federal agencies; (4) the Authorization for Use of Military Force passed by Congress in 2001,[4517] which empowered the President to use "all necessary and appropriate" force against perpetrators of the 9/11 terrorist attacks or those who harbor them; and (4) executive powers inherent in the Commander-in-Chief clause or other constitutional provisions.

[4514] U.S. Department of Homeland Security, DHS Data Privacy and Integrity Advisory Committee, Letter to the Secretary Regarding Data Privacy and Integrity Recommendations, Executive Summary, Feb. 5, 2009, p. 4.; Center for Strategic and International Studies, Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency.

[4515] Because the federal government is a government of limited powers, executive actions must find support in either: (1) a power enumerated under Article II of the U.S. Constitution; or (2) authority delegated to the executive by Congress pursuant to one or more of Congress' enumerated Article I powers. Within this framework, some actions are impliedly authorized as means to achieve ends authorized by enumerated powers. See McCulloch v. Maryland, 17 U.S. 316 (1819) (upholding Congress' creation of a National Bank as a constitutionally valid means by which to exercise enumerated Article I powers).

[4516] 44 U.S.C. §3541 et. seq.

[4517] Authorization for Use of Military Force, P.L. 107-40, 115 Stat. 224 (2001). For background information on authorizations for use of military force and differences between such authorizations and declarations of war, see CRS Report RL31133, Declarations of War and Authorizations for the Use of Military Force: Historical Background and Legal Implications, by Jennifer K. Elsea and Richard F. Grimmett.

Because the CNCI objectives appear to include broad governmental reforms and enhanced partnerships with the private sector, at least some actions contemplated by the CNCI likely fall outside of the relatively straightforward and narrow delegations of authority granted by statutes that specifically address cybersecurity, such as federal criminal law provisions and the Federal Information Security Management Act. As previously noted, the Federal Information Security Management Act requires federal agencies to take steps, such as establishing a Chief Information Officer position, to protect their computer systems from cyber intrusions.[4518] In the criminal law context, the federal computer fraud and abuse statute outlaws intrusions upon the security of government computer systems, and in some cases upon the security of computers used in interstate commerce, by trespassing, threats, damage, espionage, or corrupt use of government computers as instruments of fraud.[4519] It is likely that some cybersecurity measures envisioned by the CNCI objectives fall outside the scope of both statutory schemes. Most criminal provisions are reactive by nature; they generally do not authorize preventative measures to defend against potential cyber threats, and jurisdictional and practical hurdles could hamper law enforcement's authority over a computer hacker operating abroad. In contrast, the Federal Information Security Management Act and related statutes, like the CNCI, take a preventative approach to stopping cyber intrusions. However, they require federal agencies to take administrative measures that are relatively modest compared with the objectives of the CNCI.

It is possible that some measures contemplated by the CNCI would find authority in statutes that do not explicitly address cyber threats. For example, statutes authorizing executive management of the civil service might authorize some changes to government internet portals or changes in agency personnel.[4520] However, such statutes do not address cybersecurity explicitly, nor do they authorize actions taken outside the realm of administrative measures in federal agencies.

Therefore, the existing statutory framework may not provide adequate authority for at least some responses contemplated by CNCI objectives. To fill that possible gap, or to adopt alternative or supplemental approaches, Congress may determine that new legislation is appropriate. Potential legislative approaches are

---

[4518] 44 U.S.C. §3541 et. seq.

[4519] 18 U.S.C. §1030. For an overview of federal cybercrime provisions, see CRS Report 97-1025, Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws, by Charles Doyle.

[4520] Statutes authorizing executive management of the civil service are codified in Title 5 of the U.S. Code.

discussed infra.[4521] However, even if current statutory law is inadequate to protect the country against cyber attacks, it is not necessarily inadequate in the sense of providing insufficient legal authority for the CNCI, because inherent constitutional powers provide an alternative source of legal authority for some executive branch actions. Thus, Congress could decline to act legislatively in some areas, perhaps choosing instead to work with the executive branch in a cooperative or oversight role. If it did so, the executive branch could act in a number of situations by relying on inherent powers under Article II of the U.S. Constitution or, in very limited circumstances, on the 2001 Authorization to Use Military Force.[4522]

The Supreme Court's separation-of-powers jurisprudence makes clear that the President may occasionally act pursuant to his inherent powers under the Constitution without express or implied authorization from Congress.[4523] Powers most relevant to the CNCI include the President's war and foreign affairs powers.

Separation of Powers in National Security Matters

The Constitution divides powers relating to national security between the executive and legislative branches. Article I of the U.S. Constitution empowers Congress to "declare war," "raise and support armies," "provide and maintain a navy," and "make rules for the government and regulation of the land and naval forces."[4524] Article II states that the "President shall be Commander in Chief of the Army and Navy of the United States, and of the Militia of the several States."[4525] As a preliminary matter, invocation of war powers begs a question regarding the scope of the Commander in Chief's role in a modern conflict that, not least in the context of cyber warfare, defies traditional military strategies. Many facets of the CNCI – such as components directing planning, development, and education – fall outside of traditional definitions of war. In addition, war powers would likely not apply to actions which mandate private sector security

---

[4521] The extent of any new law would be limited by individual constitutional rights and by international laws of war.

[4522] If the President has authority to act pursuant to powers inherent in the U.S. Constitution, then authority under the Authorization to Use Military Force is unnecessary, and visa versa. Under either source, the scope of executive power might depend upon the intent of and actions taken by Congress.

[4523] The executive and legislative branches typically resolve disputes regarding the extent of executive authority without involving the courts. However, the Supreme Court is the final arbiter in such disputes. See David J. Barron and Martin S. Lederman, The Commander in Chief at the Lowest Ebb – Framing the Problem, Doctrine, and Original Understanding, 121 Harv. L. Rev. 689, 722-237 (2008).

[4524] U.S. Const. Art. I, §8.

[4525] U.S. Const. Art. II, §2, cl.1.

measures. However, many believe the Commander in Chief power extends beyond warfare to encompass a broad conception of national security. In addition, although the phrase "war powers" evokes international conflicts, it seems that the President's war powers authorize at least some domestic action. For example, some have argued that the President's Commander in Chief power authorizes him to create a domestic intelligence agency.[4526]

Alternatively, the President's foreign affairs powers might provide an inherent constitutional authorization for executive action on cybersecurity. Given modern communications technology and the ease of travel, it is increasingly difficult to draw clean lines between foreign and domestic affairs. Congress' attempts to distinguish between foreign and domestic actors in other areas impacted by rapidly changing technological environments serve as examples. For instance, in the context of electronic surveillance, statutory provisions have progressed from drawing definitive distinctions between people located in the United States versus abroad in the original Foreign Intelligence Surveillance Act to a 2007 amendment excluding from the scope of foreign surveillance any person "reasonably believed" to be located abroad.[4527]

Finally, the President might assert that his oath-based obligation to defend the nation from imminent threats, sometimes termed the "emergency theory," provides a constitutional basis for executive action to prevent cyber intrusions or attacks. Presidents have relied on this authority very rarely.[4528]

Assuming that the President's war or foreign affairs powers extend to national security efforts such as the CNCI, the next question is whether, and in what circumstances, the executive branch exercise of such powers might be constrained by congressional action. As discussed, Congress and the President share powers to address matters of national security, and no precise line divides the powers of the two political branches. Some have identified a narrow sphere of

---

[4526] RAND Corp., The Challenge of Domestic Intelligence in a Free Society: A Multidisciplinary Look at the Creation of a U.S. Domestic Counterterrorism Intelligence Agency 108 (2009) (arguing that for establishing a domestic intelligence agency, the Constitution "tilts the balance of power toward the President by virtue of the Commander-in-Chief clause").

[4527] The Foreign Intelligence Surveillance Act of 1978, P.L. 95-511, 92 Stat. 1783 (1978) (codified as amended at 50 U.S.C. §§1801 et seq.); see also Protect America Act, P.L. 110-55 (2007).

[4528] Some attorneys within the Bush Administration relied on the emergency powers argument to assert that President Bush had inherent authority to use military force in the war on terror. See, e.g., Memorandum Opinion for the Deputy Counsel to the President, The President's Constitutional Authority to Conduct Military Operations Against Terrorists and Nations Supporting Them (Sept. 25, 2001), http://www.usdoj.gov/olc/warpowers925.htm.

Article II authority, sometimes called "preclusive" power,[4529] which congressional action cannot limit. For most situations, however, Justice Robert Jackson's concurring opinion in Youngstown Steel & Tube Co.[4530] establishes the leading doctrine governing the executive's inherent constitutional authority vis-a-vis Congress.[4531] Justice Jackson's three-category framework requires courts to evaluate, where possible, the interplay between congressional intent and executive action in the context of the Constitution's allocation of powers. This exercise is made more difficult by the murky nature of a small category of inherent constitutional powers some believe are reserved to the President alone.

During the Korean War, President Truman signed an executive order directing the Commerce Secretary to take control of the nation's steel mills in order to prevent a national steelworkers' strike. In Youngstown, also known as the "Steel Seizure Case," the government claimed that presidential powers inherent in Article II provisions, most notably the Commander-in-Chief power, authorized President Truman's action.[4532] To prove this claim, the government characterized the industry seizure as an action of a Commander in Chief, prompted by exigencies of war: steel production was necessary for military operations in Korea.[4533] The Supreme Court rejected this claim,[4534] but justices reached the conclusion by different analytical routes.

Writing for the majority, Justice Black took the hard-line view that the Commander-in-Chief clause gives the President no substantive authority. He emphasized that controlling private property to affect labor disputes "is a job for the nation's lawmakers."[4535]

[4529] The term "preclusive" appeared in Justice Jackson's concurring opinion in Youngstown Steel and Tube Co., 343 U.S. 579 (1952), when he referred to Article I authorities that, if exercised, would preclude a conflicting action by Congress as "at once so conclusive and preclusive [that they] must be scrutinized with caution." 343 U.S. at 638 (Jackson, J., concurring).

[4530] 343 U.S. 579 (1952).

[4531] See Hamdan v. Rumsfeld, 548 U.S. 557, 638 (2006) ("The proper framework for assessing whether executive actions are authorized is the three-part scheme used by Justice Jackson in his opinion in Youngstown").

[4532] 343 U.S. at 587.

[4533] Id.

[4534] Id. The Court noted that "'theater of war' [is] an expanding concept." Id. Nonetheless, the Court "[could not] with faithfulness to our constitutional system hold that the Commander in Chief of the armed forces has the ultimate power as such to take possession of private property in order to keep labor disputes from stopping production." Id.

[4535] Id.

In contrast, Justice Jackson argued that the President's inherent constitutional powers "fluctuate," from relatively high when authorized by Congress, to their "lowest ebb" when a president "takes measures incompatible with the express or implied will of Congress."[4536] Specifically, Justice Jackson articulated three categories of executive action: (1) action supported by an express or implied grant of authority from Congress; (2) a "zone of twilight" between the other categories, in which "congressional inertia" can occasionally "enable, if not invite, measures on independent presidential responsibility"; and (3) action that conflicts with statutes or congressional intent.[4537] Actions in the first category enjoy congressional support and thus might not need to rely solely on an inherent constitutional powers argument; assuming that Congress acted pursuant to an enumerated Article I power in delegating the authority, these actions are clearly authorized unless they violate another constitutional provision. Actions in the second, "zone of twilight"[4538] category prompt a complicated, totality-of-the circumstances inquiry, in which courts determine congressional intent vis-a-vis executive action. Actions that fall within the third category – that is, actions that conflict with statutory law – generally lack constitutional authority, unless the action is one of the few types of actions over which the President has exclusive authority. In Youngstown, Justice Jackson found that President Truman's actions fit within the third category, because Congress had not left the issue of property seizure during labor disputes to an "open field"; rather, Congress had passed statutes designed to stabilize markets when government required supplies.[4539] On this basis, Justice Jackson joined the majority to strike down President Truman's seizure of the steel industry.[4540]

Given the existing statutory framework, at least some potential responses to cyber threats would likely fall outside of the first of Justice Jackson's categories. Congress has not expressly authorized the cybersecurity reforms proposed by the CNCI, nor do the Federal Information Security Management Act or related statutes appear to impliedly authorize all potential cybersecurity protections. In addition, although the use of cyber force might have congressional authorization

---

[4536] Id. at 635-38 (Jackson, J., concurring).

[4537] Id.

[4538] The phrase "zone of twilight" refers to the mesopelagic region of the ocean – the last region which light reaches, but it also has a non-scientific definition of an indefinite area between two conditions. Under Justice Jackson's framework, the President and Congress might have concurrent authority in this category, such that it is not always clear what, if any, power one branch has to supersede actions of the other.

[4539] Id. at 639 (Jackson, J., concurring).

[4540] Id.

under the 2001 Authorization for Use of Military Force[4541] if directed against an al Qaeda or Taliban operative, the Supreme Court has appeared to foreclose reliance on the Authorization as a basis for any action that is not a "fundamental" incident to the use of force against those responsible for the 9/11 attacks. The 2001 joint resolution authorized the use of "all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided" the 9/11 attacks.[4542] In Hamdi v. Rumsfeld, the Supreme Court held that capture and detention of Taliban members constituted "so fundamental and accepted an incident to war as to be an exercise of the 'necessary and appropriate force' Congress has authorized the President to use."[4543] The Court seemed reluctant to interpret the Authorization as extending to detentions beyond this "limited category."[4544] Cyber security efforts that focus on information gathering activities may parallel the role of intelligence collection as a "central component of the war on terrorism."[4545] However, not all cybersecurity threats fit logically within the scope of the so-called War on Terror. Cyber intrusions conducted by individual computer hackers, not supported by or aligned with a nation or terrorist organization, are perhaps best characterized as ordinary criminal activity whereas orchestrated intrusions by foreign security or intelligence entities might belong in a category of routine foreign-intelligence gathering. Neither activity appears to fit the mold of wartime operations. On the other hand, to the extent that the primary aim of the War on Terror is to prevent terrorists from harming U.S. civilians or assets, one might argue that defending the United States against threats to the U.S. cyber and telecommunications infrastructure fits squarely within the War's parameters.[4546] Nonetheless, it seems unlikely that all aspects of the CNCI would fit within the Hamdi interpretation of the 2001 Authorization.

On the other hand, unless Congress takes legislative action that contravenes a proposed executive response, the third category in Justice Jackson's framework is

---

[4541] P.L. 107-40, 115 Stat. 224 (2001).

[4542] P.L. 107-40, 115 Stat. 224 (2001).

[4543] 542 U.S. 507, 518 (2004). However, the Hamdi court held that such authority is limited by detainees' rights under the due process clause. Id.

[4544] Id.

[4545] David J. Barron and Martin S. Lederman, The Commander in Chief at the Lowest Ebb – Framing the Problem, Doctrine, and Original Understanding, 121 Harv. L. Rev. 689, 714 (2008) ("a central component of the war against terrorism is, by its nature, the collection of intelligence").

[4546] See Id. (noting that the war on terrorism differs from conventional conflicts, in part, because "the Executive has identified its principal goal in this conflict not as defeating the enemy in battle, but as preventing the enemy from 'fighting' in the first place").

inapplicable. In contrast to intelligence collection efforts through the use of electronic surveillance, which Congress explicitly limited in the Foreign Intelligence Surveillance Act,[4547] Congress has not expressly limited executive action on cybersecurity. Although Congress has not left the cybersecurity arena an entirely "open field," by virtue of its modest actions with regard to the Federal Information Security Management Act and related provisions, it has not occupied the field to the extent that it had occupied the arena of labor regulation at issue in Youngstown.

Therefore, the CNCI and other potential executive actions taken to address cybersecurity likely fall within Justice Jackson's second, "zone of twilight" category, in which the executive and legislative branches have shared authority to act. A 1981 case, Dames & Moore v. Regan, refined the Supreme Court's approach to evaluating actions that lie within this "zone of twilight."[4548] In Dames, then-Justice Renquist, writing for the majority, clarified that in "zone of twilight" cases, the analysis, at least so far as separation-of-powers principles are concerned, "hinges on a consideration of all the circumstances which might shed light on the views of the legislative branch toward [the executive's] action, including 'congressional inertia, indifference or quiescence.'"[4549] Thus, the inquiry in such cases becomes a balancing act, aimed toward ascertaining Congress' relationship to the subject matter at issue. In the context of the CNCI, Congress' actions to date on cybersecurity have been primarily criminal or administrative and do not represent a comprehensive response to the issue. In addition, the CNCI involves intelligence and foreign affairs issues that traditionally lie within the purview of the executive branch. Therefore, at least until Congress takes further action in the cybersecurity area, it appears that the executive branch is not precluded from implementing the CNCI or other cybersecurity responses under Justice Jackson's Youngstown framework.

A final issue is whether responses to cybersecurity intrusions or attacks might be part of the narrow realm of "preclusive" constitutional powers belonging to the President.[4550] Although the scope of, and even the constitutional authority for, such powers has never been fully defined, scholars have noted that a few key rules form a "rarely questioned narrative" regarding arenas in which Congress

---

[4547] 50 U.S.C. §§1801 et seq.

[4548] 453 U.S. 654 (1981).

[4549] Id. at 669.

[4550] Scholars have expressed doubts regarding the framers' intent to imbue the President with "preclusive" constitutional powers but nonetheless have argued that long-standing assumptions that such powers exist have solidified their constitutional standing. See, e.g., David J. Barron and Martin S. Lederman, The Commander in Chief at the Lowest Ebb – Framing the Problem, Doctrine, and Original Understanding, 121 Harv. L. Rev. 689, 802 (2008).

traditionally defers to executive action.[4551] For example, traditional notions dictate executive direction of wartime campaigns.[4552] Likewise, the Supreme Court has characterized the President as the "sole organ" of the country in conducting foreign affairs.[4553] In addition, some have suggested a distinction between offensive utilization of cyber weapons versus defensive shield to stop attacks:[4554] whereas the President must obtain congressional authorization before committing

U.S. armed forces in an offensive action, the President's has the exclusive power to repel attacks made against the United States.

Despite this narrative, however, no definitive boundaries have been defined for any such preclusive powers. Perhaps for that reason, Justice Jackson made clear in his Youngstown concurrence that the realm of any such preclusive powers must be carefully scrutinized.[4555] Thus, although many executive actions in the cyber area would likely fall within the scope of Article II powers for ensuring national security, most actions would probably falls outside of the narrow categories of exclusive executive authority to conduct wartime campaigns and international relations. Similarly, even if the President has an exclusive power to lead the military in defensive actions, actions might not be clearly enough a

---

[4551] See, e.g Id. at 698. For more information regarding divisions between Congress' and the President's war powers and an analysis of that division in the context of the President's authority to use commit armed forces in Iraq, see CRS Report RL33837, Congressional Authority to Limit U.S. Military Operations in Iraq, by Jennifer K. Elsea, Michael John Garcia, and Thomas J. Nicola.

[4552] See Hamdan v. Rumsfeld, 548 U.S. 557, 591-92 (2006) (citing Ex Parte Milligan, 71 U.S. 2, 139-40 (1866)). But see War Powers Resolution, 50 U.S.C. §§1541-1548, discussed infra.

[4553] See United States v. Curtiss-Wright Export Co., 299 U.S. 304, 319 (1936) ("'The President is the sole organ of the nation in its external relations, and its sole representative with foreign nations.'" (citing Annals, 6th Cong., col. 613 (statement of John Marshall))). However, the Curtiss-Wright case involved executive action that fell in the first of Justice Jackson's Youngstown categories – i.e., where Congress and the President acted in concert. Thus, although the case has helped to form a narrative regarding executive-branch prerogative in international relations and has occasionally been cited to support the proposition that the President has some preclusive foreign affairs powers under the Constitution, it would misstate the Curtiss-Wright holding to assume that it recognized any broad preclusive foreign relations power.

[4554] Aside from the operational distinction that may be made with respect to the types of cyber activities the U.S. may undertake, the offensive versus defensive distinction may also be worth considering from an organizational perspective. Agencies responsible for protecting the government's websites and launching counter-offensive attacks may not be the same entities responsible for assisting in the recovery phase of an attack of national security significance on a U.S. cyber or telecommunications hosted network.

[4555] 343 U.S. at 638 (Jackson, J., concurring).

defensive response to a military threat to trigger an exclusive presidential power.[4556]

Thus, it appears that the Youngstown framework would apply to a review of the President's authority to implement responses such as the CNCI. Thus, if Congress passed conflicting legislation in the cybersecurity area, some executive actions could be constrained. Alternatively, congressional legislation granting explicit authority for cybersecurity measures would more firmly confirm the executive authority to act in that area.

It is possible that the Supreme Court will address the constitutional authorities for national security in a future case. Youngstown represents one of only a small number of cases in which the Supreme Court has reached questions regarding the political branches' shared powers under the Constitution. Modern threats might necessitate new definitions within the Court's separation-ofpowers jurisprudence. For example, as cyber activities and telecommunication architectures are networked globally, with it often being difficult to ascertain where an attack or intrusion emanates, distinctions based on notions of conventional war may seem increasingly inconsistent with the modern Commander-in-Chief role.

Congressional Constraints on Executive Action

Even if the CNCI or future cybersecurity initiatives are grounded in statutory or constitutional authority, questions will nonetheless arise regarding the degree to which legislative oversight is appropriate. Congress has attempted to obligate the President to report to relevant congressional leaders for actions taken pursuant to war powers or as part of intelligence operations. In 1973, Congress passed the War Powers Resolution to "fulfill the intent of the framers of the Constitution of the United States and insure that the collective judgment of both the Congress and the President will apply to the introduction of United States Armed Forces into hostilities."[4557] Although presidents since the Resolution's passage have maintained that the Resolution unconstitutionally limits presidential authority,

---

[4556] In the context of modern national security threats, the line between offensive and defensive action is not easily deciphered. For example, the United States captured and detained a large number of alleged enemy combatants in the course of post-September 11th military operations. Is the ongoing detention of such persons, often referred to as "preventative detention," an offensive action? The Supreme Court has upheld executive authority for such detentions on statutory rather than constitutional grounds; it has not addressed offensive versus defensive distinction. Hamdi, 542 U.S. 507. Thus, even if some components of the CNCI qualify as war-related activity, perhaps because they target cyber terrorists, little guidance exists regarding which actions might qualify as defensive rather than offensive actions under the traditional war powers analysis.

[4557] War Powers Resolution, P.L. 93-148, 87 Stat. 555 (1973) (codified at 50 U.S.C. §§1541-1548); 50 U.S.C. §1541(a).

presidents have in many cases submitted documents for Congress that are "consistent with" the Resolution's requirements.[4558]

Similarly, after the Iran-Contra affair, Congress passed legislation increasing congressional oversight of intelligence activities, including significant and anticipated intelligence activities, and covert actions.[4559] To the extent consistent with due regard for preventing unauthorized disclosure of classified information regarding sensitive intelligence sources and methods, current law requires that congressional intelligence committees be kept fully informed regarding intelligence activities. If the President determines that it is essential to meet extraordinary circumstances affecting vital U.S. interests, a presidential finding regarding a covert action may be limited to a small number of congressional leaders.[4560]

With respect to the CNCI, a key question is whether ongoing or potential U.S. cyber activities, defensive and offensive, may fall within the sphere of a covert activity or an intelligence activity and thus trigger reporting requirements. The statutory definition of "covert actions" includes "activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly," but excludes activities conducted for the purpose of gathering intelligence and "traditional" diplomatic, military, or law enforcement activities.[4561] The definition of "intelligence activity" is broader; it includes covert actions and "financial intelligence activities."[4562] Because the definitions focus on the influence, rather than the presence, of conditions abroad, it appears that cyber actions targeting or even defending against cyber threats, even if conducted inside the United States, could trigger reporting requirements.

In addition to the potential application of ongoing reporting requirements, Congress could elicit information regarding executive actions by virtue of its enumerated power to control spending. The 110th Congress took several steps to obtain information regarding the CNCI in that manner. A continuing resolution, passed by Congress and signed into law in September 2008, withholds $127 million of a $313.5 million appropriation for cybersecurity until House and

---

[4558] For information Presidential actions vis-a-vis the War Powers Resolution, see CRS Report RL33532, War Powers Resolution: Presidential Compliance, by Richard F. Grimmett.

[4559] Fiscal Year 1991 Intelligence Authorization Act, P.L. 102-88, 105 Stat. 429 (1991) (codified as amended at 50 U.S.C. §§413, 413a, 413b).

[4560] For more information on congressional oversight of covert actions, see CRS Report RL33715, Covert Action: Legislative Background and Possible Policy Questions, by Alfred Cumming.

[4561] 50 U.S.C. §413b(e).

[4562] 50 U.S.C. §413(f).

Senate appropriations committees "receive and approve a plan for expenditure for [the CNCI] that describes the strategic context of the program; the specific goals and milestones set for the program; and the funds allocated to achieving each of those goals."[4563] In addition, the Senate Committee on Homeland Security and Governmental Affairs held a closed hearing in March 2008 regarding the CNCI and later obtained answers to some questions regarding the initiative.[4564] Finally, as part of a larger Homeland Security Authorization bill, S. 3623, Senator Lieberman introduced legislation during the 110th Congress that would provide for congressional oversight of the CNCI and establish "a robust National Cyber Security Center with the mission of coordinating and enhancing federal efforts to protect government networks."[4565] As an authorization bill for the DHS has not been passed since the creation of the Department, whether the proposed legislative oversight efforts will be effective remains to be seen. Also, as with many programs associated with intelligence community activities and defense, concerns regarding committee jurisdiction in the areas of oversight, authorization, and appropriations might be raised for the CNCI.

Policy Considerations and Congressional Options

As with executive control over covert actions, foreign affairs, and intelligence gathering, strong justifications support the assertion that the executive branch is best suited to take reasonable and necessary actions to defend the country against cyber-based threats. One such justification stems from the broad diversity of cybersecurity threats: the President is arguably best positioned to take a leadership role or create a uniform response to span the range of cyber vulnerabilities. In addition, the executive branch is likely most able to integrate intelligence-gathering, military, and other vehicles for addressing the cybersecurity challenge. However, in order for Congress to maintain ongoing awareness of CNCI plans and activities and to effectively perform its constitutional duties of oversight based on a thorough understanding of executive branch activities, some security experts suggest a range of legislative activities that might be required. Congress might choose to:

[4563] Consolidated Security, Disaster Assistance, and Continuing Appropriations Act of 2009, P.L. 110-329, (2008).

[4564] NSPD-54/HSPD-23 and the Comprehensive National Cyber Security Initiative: Hearing Before the Sen. Homeland Security and Governmental Affairs Comm., 110th Cong. (March 4, 2008).

[4565] S. 3623, 110th Cong. §§601-08 (2008); 154 Cong. Rec. S9687 (daily ed. Sept. 26, 2008) (statement of Sen. Lieberman).

- determine the most appropriate and effective organizational entity in which the nation's principal cybersecurity prevention, response, and recovery responsibilities should reside;[4566]
- require the senior U.S. government official in charge of all CNCI related activities be a Senate confirmable position to facilitate ongoing information exchange regarding Initiative plans and areas of progress and difficulty;
- enact legislative language recognizing and defining the classified and unclassified aspects of the CNCI and the need for greater transparency and inclusiveness;
- require the new Administration to develop and revise annually a classified and unclassified national cyber security strategy and intelligence community generated National Intelligence Estimate that provides Congress, the telecommunications industry, and the American public information related to the CNCI, the current and strategic cyber threats facing the nation, and programs being implemented to prepare for evolving technological risks;
- define the privacy and civil liberty considerations that should accompany all aspects of the CNCI;
- include legislative language in applicable authorizations bills to establish a programmatic foundation for CNCI related programs and suggest funding for current and future year's activities; or
- identify and codify relevant laws defining a national security related cyber offense against the United States, offensive versus defensive cyber activities, and the situations in which the Congress should be notified prior to the United States undertaking an offensive or counteroffensive cyber act.

Conclusion

As discussed, multiple policy considerations, including the novel and dispersed nature of cyber threats, might justify an executive-led response to cybersecurity. In response to calls for executive action, questions have arisen regarding the adequacy of legal authorities justifying executive responses to cyber threats. Although existing statutes might support some executive actions, the current statutory framework likely does not address all potential actions. Thus, the extent of inherent powers under Article II of the Constitution and the appropriate roles of the two political branches in this emerging national security arena are relevant considerations. Arguably, both the statutory framework and separation of powers

---

[4566] Possible organizational constructs for such an entity range from a single entity placed in charge of all phases of U.S. cyber activity to a coordination office with the authority and responsibility to compel other organizations to adhere to the President's cyber strategy. Entities often noted as having a significant contribution to the U.S. cyber activity, which could add capability and resources to the CNCI's capabilities, include the cyber and telecommunications industries, intelligence and law enforcement communities, and academia.

analyses might need to be modernized to address appropriate roles in protecting the United States against modern cyber threats.

Finally, even if executive branch responses are authorized, Congress retains an oversight role vis-à-vis the CNCI or other presidential initiatives, for several reasons. First, if Congress passed statutes in contravention of the President's efforts, the President's authority to proceed with those efforts would become more questionable under the Youngstown framework. Second, as with covert actions, Congress likely has a legislative oversight role, even if that role merely requires notice of significant actions. Finally, Congress could ultimately withhold funding for the CNCI or specific aspects of the program should it not receive the necessary information to make an assessment of the activities related to each of the twelve objectives.

Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues, RL31787 (March 20, 2007).

CLAY WILSON, CONGRESSIONAL RESEARCH SERV., INFORMATION OPERATIONS, ELECTRONIC WARFARE, AND CYBERWAR: CAPABILITIES AND RELATED POLICY ISSUES (2007), *available at* http://www.intelligencelaw.com/library/secondary/crs/pdf/RL31787_3-20-2007.pdf.

Order Code RL31787
Updated March 20, 2007

Clay Wilson
Specialist in Technology and National Security
Foreign Affairs, Defense, and Trade Division

Summary

This report describes the emerging areas of information operations, electronic warfare, and cyberwar in the context of U.S. national security. It also suggests related policy issues of potential interest to Congress.

For military planners, the control of information is critical to military success, and communications networks and computers are of vital operational importance. The use of technology to both control and disrupt the flow of information has been generally referred to by several names: information warfare, electronic warfare, cyberwar, netwar, and Information Operations (IO). Currently, IO activities are grouped by the Department of Defense (DOD) into five core capabilities: (1) Psychological Operations, (2) Military Deception, (3) Operational Security, (4) Computer Network Operations, and (5) Electronic Warfare.

Current U.S. military doctrine for IO now places increased emphasis on Psychological Operations, Computer Network Operations, and Electronic Warfare, which includes use of non-kinetic electromagnetic pulse (EMP) weapons, and nonlethal weapons for crowd control. However, as high technology is increasingly incorporated into military functions, the boundaries between all five IO core capabilities are becoming blurred.

DOD has noted that military functions involving the electromagnetic spectrum take place in what is now called the cyber domain, similar to air, land, and sea. This cyber domain is the responsibility of the new Air Force Cyber Command and includes cyberwarfare, electronic warfare, and protection of U.S. critical

infrastructure networks that support telecommunications systems, utilities, and transportation.

This report will be updated to accommodate significant changes.

Introduction
Background

Control of information has always been part of military operations, and the U.S. Strategic Command views information operations as a core military competency, with new emphasis on (1) use of electromagnetic energy, (2) cyber operations, and (3) use of psychological operations to manipulate an adversary's perceptions. Department of Defense (DOD) officials now consider cyberspace to be a domain for warfare, similar to air, space, land, and sea.[4567]

The DOD views information itself as both a weapon and a target in warfare. In addition, Psychological Operations (PSYOP) provides the ability to rapidly disseminate persuasive information to directly influence the decisionmaking of diverse audiences, and is seen as a means for deterring aggression, and important for undermining the leadership and popular support for terrorist organizations.[4568]

However, new technologies for military IO also create new national security policy issues, including (1) consideration of psychological operations used to affect friendly nations or domestic audiences; and (2) possible accusations against the U.S. of war crimes if offensive military computer operations or electronic warfare tools severely disrupt critical civilian computer systems, or the systems of non-combatant nations.

This report describes DOD capabilities for conducting military information operations, and gives an overview of related policy issues. This report will be updated as events warrant.

[4567] Jason Ma, "Information Operations To Play a Major Role in Deterrence Posture,"Inside Missile Defense, Dec. 10, 2003 [http://www.insidedefense.com/secure/defense_docnum.asp?f=defense_2002.ask&docnum=MISSILE-9-25-4]. Todd Lopez, Air Force Leaders to Discuss new 'Cyber Command', Air Force News, Nov 5, 2006, [http://www.8af.acc.af.mil/news/story_print.asp?storyID=123031988].

[4568] DOD Information Operations Roadmap, October 30, 2004, p.3. This document was declassified January, 2006, and obtained through FOIA by the National Security Archive at George Washington University. [http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB177/info_ops_roadmap.pdf].

DEFINITIONS

Information

Information is a resource created from two things: phenomena (data) that are observed, plus the instructions (systems) required to analyze and interpret the data to give it meaning. The value of information is enhanced by technology, such as networks and computer databases, which enables the military to (1) create a higher level of shared awareness, (2) better synchronize command, control, and intelligence, and (3) translate information superiority into combat power.

DOD Information Operations

The current DOD term for military information warfare is "Information Operations" (IO). DOD information operations are actions taken during time of crisis or conflict to affect adversary information, while defending one's own information systems, to achieve or promote specific objectives.[4569] The focus of IO is on disrupting or influencing an adversary's decision-making processes.

An IO attack may take many forms, for example: (1) to slow adversary computers, the software may be disrupted by transmitting a virus or other malicious code; (2) to disable sophisticated adversary weapons, the computer circuitry may be overheated with directed high energy pulses; and (3) to misdirect enemy sensors, powerful signals may be broadcast to create false images. Other methods for IO attack may include psychological operations such as initiating TV and radio broadcasts to influence the opinions and actions of a target audience, or seizing control of network communications to disrupt an adversary's unity of command.

Computer Network Defense (CND) is the term used to describe activities that are designed to protect U.S. forces against IO attack from adversaries. Part of CND is information assurance (IA), which requires close attention to procedures for what is traditionally called computer and information security.

DOD places new emphasis on the importance of dominating the entire electromagnetic spectrum with methods for computer network attack and electronic warfare. DOD also emphasizes that because networks are increasingly the operational center of gravity for warfighting, the U.S. military must be prepared to "fight the net".[4570] Because the recently declassified source document containing this phrase has some lines blacked out, it is not clear if "...net"means the Internet. If so, then this phrase may be a recognition by DOD that Psychological Operations, including public affairs work and public diplomacy,

---

[4569] From the DOD Dictionary of Military and Associated Terms, Jan. 2003 [http://www.dtic.mil/doctrine/jel/doddict/data/i/index.html].

[4570] DOD Information Operations Roadmap, October 30, 2003, p.6-7. [http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB177/info_ops_roadmap.pdf].

must be employed in new ways to counter the skillful use of the Internet and the global news media by U.S. adversaries.

DOD INFORMATION OPERATIONS CORE CAPABILITIES

DOD identifies five core capabilities for conduct of information operations; (1) Psychological Operations, (2) Military Deception, (3) Operations Security, (4) Computer Network Operations, and (5) Electronic Warfare. These capabilities are interdependent, and increasingly are integrated to achieve desired effects.

Psychological Operations (PSYOP)

DOD defines PSYOP as planned operations to convey selected information to targeted foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals.[4571] For example, during the Operation Iraqi Freedom (OIF), broadcast messages were sent from Air Force EC-130E aircraft, and from Navy ships operating in the Persian Gulf, along with a barrage of e-mail, faxes, and cell phone calls to numerous Iraqi leaders encouraging them to abandon support for Saddam Hussein.

At the same time, the civilian Al Jazeera news network, based in Qatar, beams its messages to well over 35 million viewers in the Middle East, and is considered by many to be a "market competitor" for U.S. PSYOP. Terrorist groups can also use the Internet to quickly place their own messages before an international audience. Some observers have stated that the U.S. will continue to lose ground in the global media wars until it develops a coordinated strategic communications strategy to counter competitive civilian news media, such as Al Jazeera.[4572]

Partly in response to this observation, DOD now emphases that PSYOP must be improved and focused against potential adversary decisionmaking, sometimes well in advance of times of conflict. Products created for PSYOP must be based on in-depth knowledge of the audience's decision-making processes. Using this knowledge, the PSYOPS products then must be produced rapidly, and disseminated directly to targeted audiences throughout the area of operations.[4573]

[4571] DOD Dictionary of Military Terms [http://www.dtic.mil/doctrine/jel/doddict/].

[4572] Air Force, Operation Iraqi Freedom Information Operations Lessons Learned: First Look, AFC2ISRC/CX, July 23, 2003 [http://www.insidedefense.com/secure/data_extra/pdf3/dplus2004_265.pdf].

[4573] DOD Information Operations Roadmap, October 30, 2003, p.6. [http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB177/info_ops_roadmap.pdf].

DOD policy prohibits the use of PSYOP for targeting American audiences. However, while military PSYOP products are intended for foreign targeted audiences, DOD also acknowledges that the global media may pick up some of these targeted messages, and replay them back to the U.S. domestic audience. Therefore, a sharp distinction between foreign and domestic audiences cannot be maintained.[4574]

Military Deception (MILDEC)

Deception guides an enemy into making mistakes by presenting false information, images, or statements. MILDEC is defined as actions executed to deliberately mislead adversary military decision makers with regard to friendly military capabilities, thereby causing the adversary to take (or fail to take) specific actions that will contribute to the success of the friendly military operation.

As an example of deception during Operation Iraqi Freedom (OIF), the U.S. Navy deployed the Tactical Air Launched Decoy system to divert Iraqi air defenses away from real combat aircraft.

Operational Security (OPSEC)

OPSEC is defined as a process of identifying information that is critical to friendly operations and which could enable adversaries to attack operational vulnerabilities. For example, during OIF, U.S. forces were warned to remove certain information from DOD public websites, so that Iraqi forces could not exploit sensitive but unclassified information.

Computer Network Operations (CNO)

CNO includes the capability to: (1) attack and disrupt enemy computer networks; (2) defend our own military information systems; and (3) exploit enemy computer networks through intelligence collection, usually done through use of computer code and computer applications. The Joint Information Operations Warfare Command (JIOWC) and the Joint Functional Component Command for Network Warfare (JFCCNW) are responsible for the evolving mission of Computer Network Attack.[4575] The exact capabilities of the JIOWC and JFCCNW are highly classified, and DOD officials have reportedly never admitted to launching a cyber attack against an enemy, however many computer security officials believe the organization can destroy networks and penetrate enemy

---

[4574] DOD Information Operations Roadmap, October 30, 2003, p.26. [http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB177/info_ops_roadmap.pdf].

[4575] John Lasker, U.S. Military's Elite Hacker Crew, Wired News, April 18, 2005, [http://www.wired.com/news/privacy/0,1848,67223,00.html], U.S. Strategic Command Fact File [http://www.stratcom.mil/fact_sheets/fact _jtf _gno.html] and [http://www.stratcom.mil/fact_sheets/fact_jioc.html].

computers to steal or manipulate data, and take down enemy command-and-control systems. They also believe that the organization consists of personnel from the CIA, National Security Agency, FBI, the four military branches, and civilians and military representatives from allied nations.[4576]

Computer Network Defense (CND)

CND is defined as defensive measures to protect information, computers, and networks from disruption or destruction. CND includes actions taken to monitor, detect, and respond to unauthorized computer activity. Responses to IO attack against U.S. forces may include use of passive information assurance tools, such as firewalls or data encryption, or may include more intrusive actions, such as monitoring adversary computers to determine their capabilities before they can attempt an IO attack against U.S. forces.

Some DOD officials believes that CND may lack sufficient policy and legal analysis for guiding appropriate responses to intrusions or attacks on DOD networks. Therefore, DOD has recommended that a legal review be conducted to determine what level of intrusion or data manipulation constitutes an attack. The distinction is necessary in order to clarify whether an action should be called an attack or an intelligence collection operation, and which aggressive actions can be appropriately taken in self-defense. This legal review should also determine if appropriate authorities permit U.S. forces to retaliate through manipulation of unwitting third party computer hosts. And finally, DOD has recommended structuring a legal regime that applies separately to domestic and to foreign sources of computer attack against DOD or the U.S. critical. infrastructure.[4577]

Computer Network Exploitation (CNE)

CNE is an area of IO that is not yet clearly defined within DOD. Before a crisis develops, DOD seeks to prepare the IO battlespace through intelligence, surveillance, and reconnaissance, and through extensive planning activities. This involves intelligence collection, that in the case of IO, is usually performed through network tools that penetrate adversary systems to gain information about system vulnerabilities, or to make unauthorized copies of important files. Tools used for CNE are similar to those used for computer attack, but configured for intelligence collection rather than system disruption.

Computer Network Attack (CNA)

[4576] John Lasker, U.S. Military's Elite Hacker Crew, April 18, 2005, Wired News, [http://www.wired.com/news/privacy/0,67223-0.html?tw=wn_story_page_prev2].

[4577] DOD Information Operations Roadmap, October 30, 2003, p52. [http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB177/info_ops_roadmap.pdf].

CNA is defined as effects intended to disrupt or destroy information resident in computers and computer networks. As a distinguishing feature, CNA normally relies on a data stream used as a weapon to execute an attack. For example, sending a digital signal stream through a network to instruct a controller to shut off the power flow is CNA, while sending a high voltage surge through the electrical power cable to short out the power supply is considered Electronic Warfare (However, a digital stream of computer code or a pulse of electromagnetic power can both be used to also create false images in adversary computers).

During Operation Iraqi Freedom, U.S. and coalition forces reportedly did not execute any computer network attacks against Iraqi systems. Even though comprehensive IO plans were prepared in advance, DOD officials stated that top-level approval for several CNA missions was not granted until it was too late to carry them out to achieve war objectives.[4578] U.S. officials may have rejected launching a planned cyber attack against Iraqi financial computers because Iraq's banking network is connected to a financial communications network also located in Europe. Consequently, according to Pentagon sources, an information operations attack directed at Iraq might also have brought down banks and ATM machines located in parts of Europe as well. Such global network interconnections, plus close network links between Iraqi military computer systems and the civilian infrastructure, reportedly frustrated attempts by U.S. forces to design a cyber attack that would be limited to military targets only in Iraq.[4579]

In a meeting held in January 2003, at the Massachusetts Institute of Technology, White House officials sought input from experts outside government on guidelines for use of cyber-warfare. Officials have stated they are proceeding cautiously, since a cyberattack could have serious cascading effects, perhaps causing major disruption to networked civilian systems.[4580] In February 2003, the Bush Administration announced national-level guidance for determining when and how the United States would launch computer network attacks against foreign adversary computer systems. The classified guidance, known as National Security Presidential Directive 16, is intended to clarify circumstances under which a disabling computer attack would be justified, and who has authority to launch such an attack.

[4578] Elaine Grossman, "Officials: Space, Info Targets Largely Cobbled On-The-Fly for Iraq," Inside the Pentagon, May 29, 2003.

[4579] Charles Smith, "U.S. Information Warriors Wrestle with New Weapons," NewsMax.com, March 13, 2003 [http://www.newsmax.com/archives/articles/2003/3/12/134712.shtml].

[4580] Bradley Graham, "Bush Orders Guidelines for Cyber-Warfare," Washington Post, February 7, 2003, Section A, p.1.

Electronic Warfare (EW)

EW is defined by DOD as any military action involving the direction or control of electromagnetic spectrum energy to deceive or attack the enemy. High power electromagnetic energy can be used as a tool to overload or disrupt the electrical circuitry of almost any equipment that uses transistors, micro-circuits, or metal wiring.[4581] Directed energy weapons amplify, or disrupt, the power of an electromagnetic field by projecting enough energy to overheat and permanently damage circuitry, or jam, overpower, and misdirect the processing in computerized systems. The Electronic Warfare Division of the Army Asymmetric Warfare Office has responsibility for creating electronic warfare policy, and for supporting development of new electromagnetic spectrum concepts that can be translated into equipment and weapons.

Domination of the Electromagnetic Spectrum

DOD now emphasizes maximum control of the entire electromagnetic spectrum, including the capability to disrupt all current and future communication systems, sensors, and weapons systems. This may include: (1) navigation warfare, including methods for offensive space operations where global positioning satellites may be disrupted; or, (2) methods to control adversary radio systems; and, (3) methods to place false images onto radar systems, block directed energy weapons, and misdirect unmanned aerial vehicles (UAVs) or robots operated by adversaries.[4582]

For example, recent military IO testing examined the capability to secretly enter an enemy computer network and monitor what their radar systems could detect. Further experiments tested the capability to take over enemy computers and manipulate their radar to show false images.[4583]

Electromagnetic Non-Kinetic Weapons

Non-kinetic weapons emit directed electromagnetic energy that, in short pulses, may permanently disable enemy computer circuitry. For example, an electromagnetic non-kinetic weapon mounted in an aircraft, or on the ground, might disable an approaching enemy missile by directing a High Power Microwave (HPM) beam that burns out the circuitry, or that sends a false

---

[4581] CRS Report RL32544, High Altitude Electromagnetic Pulse (EMP) and High Power Microwave (HPM) Devices: Threat Assessments, by Clay Wilson.

[4582] DOD Information Operations Roadmap, October 30, 2003, p.61. [http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB177/info_ops_roadmap.pdf].

[4583] These programs were called Suter 1 and Suter 2, and were tested during Joint Expeditionary Forces Experiments held at Nellis Air Force Base in 2000 and 2002. David Fulghum, "Sneak Attack," Aviation Week & Space Technology, June 28, 2004, p. 34.

telemetry signal to misdirect the targeting computer.[4584] Also, at reduced power, electromagnetic non-kinetic weapons can also be used as a non-lethal method for crowd control.

The Active Denial System (ADS), developed by the Air Force, is a vehicle-mounted nonlethal, counter-personnel directed energy weapon. Currently, most non-lethal weapons for crowd control, such as bean-bag rounds, utilize kinetic energy. However, the ADS projects a focused beam of millimeter energy waves to induce an intolerable burning sensation on an adversary's skin, repelling the individual without causing injury. Proponents say the ADS is safe and effective at ranges between 50 and 1,600 feet. The nonlethal capabilities of the ADS are designed to protect the innocent, minimize fatalities, and limit collateral damage.[4585]

The Pentagon reportedly has requested immediate deployment of at least 8 ADS devices to Iraq to assist Marines in guarding posts, countering insurgent snipers and protecting convoys. The ADS system would be the first operationally deployed directed-energy weapon for counter-personnel missions.[4586]

NEW U.S.A.F. CYBER COMMAND

Secretary of the Air Force Michael W. Wynne recently stated that the new mission of the U.S. Air Force is to "fly and fight in air, space, and cyberspace." This means that military action in cyberspace now includes defending against malicious activity on the Internet, and anywhere across the entire electromagnetic spectrum (including the energy spectrum bands for radio, microwaves, infrared, X-ray, and all other options for directed energy), where national security is threatened.[4587] Secretary Wynne stated that cyberwarfare flows naturally from the Air Force's traditional missions, such as downloading data from platforms in space, and that U.S. capabilities should be expanded to also enable the shut down of enemy electronic networks. Consequently, the 8th Air Force, headquartered at Barksdale Air Force Base, La., has been designated as the operational Cyber Command, responsible for organizing, training, and

---

[4584] David Fulghum, "Sneak Attack," Aviation Week & Space Technology, June 28, 2004, p.34.

[4585] Active Denial System, Fact Sheet, Air Force Research Lab, Office of Public Affairs, Kirtland Air Force Base, [http://www.de.afrl.af.mil/Factsheets/ActiveDenial.pdf].

[4586] Jason Sherman, Pentagon Considering Sending Non-Lethal Ray Gun to Iraq, Inside Defense, Mar 2, 2007.

[4587] John Bennett and Carlo Munoz, USAF Sets Up First Cyberspace Command, Military.com, Nov 4, 2006, [http://www.military.com/features/0,15240,118354,00.html].

equipping the Air Force for cyberspace operations.[4588] The new Cyber Command will draw on resources from all Air Force commands to gather needed expert capabilities.

Air Force officials, led by the Air Force Chief of Staff Gen. Michael Mosley, met at the Pentagon in a "cyberwarfare-themed summit" during November 2006, to make plans for the new Air Force Cyber Command.[4589] General Elder stated that the planning session may require approximately four months of work, and will include an assessment of offensive and defensive cyberwarfare requirements, as well as a review of current capabilities and future needs.[4590]

Homeland security reportedly will also be a large part of the Cyber Command's new responsibility, including protection of telecommunications systems, utilities, and transportation. Several issues to be considered may include: (1) what kind of educational skills, technical skills, and training are needed for staff at the Cyber Command; and (2), what kind of career path can be offered to those in the Air Force who want to participate in defending the new cyber domain.

In addition, the Air Force Materiel Command will review the research now ongoing at the 8th Air Force headquarters to identify which work should receive funding as part of the new cyberwarfare function.[4591] Some examples of systems or projects that could be affected by the cyber command mission include (1) the Airborne Laser System at Edwards AFB, (2) the Active Denial System at Moody AFB, (3) the Joint Surveillance Target Attack Radar System at Robins AFB, and (4) efforts to protect against damage to computer systems due to electromagnetic pulse attack.

Officials at the 8th Air Force report that as of January 2007, the new U.S.A.F. cyber command has not yet been officially activated, and the final command structure has not been determined.[4592] Initially, the new organization will operate on an equal footing with other numbered Air Force headquarters. However, eventually the new organization will become a major command that will stand

---

[4588] Todd Lopez, 8th Air Force to become New Cyber Command, Air Force Link, Nov 3, 2006, [http://www.af.mil/news/story.asp?storyID=123030505]. Dave Ahearn, Air Force Forms Cyberspace Unit, Defense Daily, Nov 3, 2006.

[4589] Contact for Dr. Lani Kass, Director of Air Force Cyberspace Task Force, and Special Assistant to General Michael Moseley, is through Maj. Gary Conn, Gary.Conn@pentagon.af.mil, 703-697-3143.

[4590] Personal communication with Air Force Public Affairs Office, January 26, 2007.

[4591] Head Quarters at Wright Patterson AFB, 937-522-3252, [http://www.wpafb.af.mil/].

[4592] Personal communication, Public Affairs Office at the 8th Air Force, which can be reached at 318-456-2145, [http://www.8af.acc.af.mil].

alongside the Air Force Space Command and the Air Combat Command. Precise future command relationships are still being decided in the ongoing planning effort, and more details will be forthcoming.[4593]

JOINT COMMAND STRUCTURE FOR CYBERWARFARE

Currently, the U.S. Strategic Command (USSTRATCOM), which is a unified combatant command for U.S. strategic forces, controls military information operations, space command, strategic warning and intelligence assessments, global strategic operations planning, and also has overall responsibility for Computer Network Operations (CNO).[4594]

Beneath USSTRATCOM are several Joint Functional Component Commands (JFCCs): (1) space and global strike integration; (2) intelligence, surveillance and reconnaissance; (3) network warfare; (4) integrated missile defense; and (5) combating weapons of mass destruction.[4595]

The JFCC-Network Warfare (JFCC-NW), and the JFCC-Space & Global Strike (JFCC-SGS) have responsibility for overall DOD cyber security. Under the JFCC-NW are the Joint Task Force-Global Network Operations (JTF-GNO) and the Joint information Operations Warfare Center (JIOWC), both of which have direct responsibility for defense against cyber attack.[4596] The JTF-GNO defends the DOD Global Information Grid, while the JIOWC assists combatant commands with an integrated approach to information operations. These include operations security, psychological operations, military deception, and electronic warfare. The JIOWC also coordinates network operations and network warfare with the JTF-GNO and with JFCC-NW.

DOD AND THE US CRITICAL INFRASTRUCTURE

DOD officials have noted that because 80 percent of U.S. commerce goes through the Internet, DOD systems must develop a capability to adequately protect them.[4597] Currently, to assist commercially-owned telecommunications networks, communications satellite systems, and other civilian critical infrastructure

---

[4593] Personal communication with Air Force Public Affairs Office, January 26, 2007.

[4594] The Public Affairs Office for the Air Force at the Pentagon can be contacted at 703-5712776.

[4595] United State Strategic Command, July 2006, [http://www.stratcom.mil/organization-fnc_comp.html].

[4596] Clark A. Murdock et. al, Beyond Goldwater-Nichols: U.S. Government and Defense Reform for a New Strategic Era, Phase 2 Report, July 2005,Center for Strategic and International Studies, p.128, [http://www.ndu.edu/lIbrary/docs/ BeyondGoldwaterNicholsPhase2Report.pdf].

[4597] John Doyle, Air Force To Elevate Status Of Cyberspace Command, Aerospace Daily & Defense Report, Mar 22, 2007.

systems, DOD contracts with Carnegie Mellon's Software Engineering Institute to operate the Computer Emergency Response Team (CERT-CC), while DHS in partnership with private industry operates a parallel organization called US-CERT. Both organizations monitor trends in malicious code and cyber crime, send out alerts about threats to computer systems, and provide guidance for recovery after an attack.

INFORMATION OPERATIONS BY ADVERSARIES

The low cost of entry (for example, a laptop connected to the Internet), and the ability to operate anonymously, are factors that makes cyberspace attractive to adversaries who know they cannot challenge the United States in a symmetrical contest. Potential adversaries, such as China, Russia, Cuba, Iran, Iraq, Libya, North Korea, and several non-state terrorist groups are reportedly developing capabilities to attack or degrade U.S. civilian and military networks. "Moonlight Maze" and "Titan Rain" are examples of successful attacks against non-classified military systems which DOD officials claim were directed by other governments.[4598]

According to the Defense Department's annual report to Congress on China's military prowess, the Chinese military is enhancing its information operations capabilities.[4599] The report finds that China is placing specific emphasis on the ability to perform information operations designed to weaken an enemy force's command and control systems.[4600]

Terrorist groups also use wireless electronics to detonate roadside bombs (Improvised Explosive Devices). They also use the Internet to transmit financial transactions, and use free Global Positioning System (GPS) signals and commercial satellite video and images to direct their ground attacks against U.S. and coalition troops.[4601]

[4598] Elinor Abreu, Epic cyberattack reveals cracks in U.S. defense, CNN.com, May 10, 2001, [http://archives.cnn.com/2001/TECH/internet/05/10/3.year.cyberattack.idg/]. Declan McCullagh, Feds Say Fidel Is Hacker Threat, WiredNews.com, Feb, 09, 2001, [http://www.wired.com/news/politics/0,1283,41700,00.html]. Staff, Cyberattack could result in military response , USAToday, Feb 14, 2002, [http://www.usatoday.com/tech/news/2002/02/14/cyberterrorism.htm].

[4599] See the FY2004 Report to Congress on PRC Military Power, [http://www.defenselink.mil/pubs/d20040528PRC.pdf].

[4600] John Bennett, "Commission: U.S. Should Push Beijing to up Pressure on North Korea," Inside the Pentagon, June 17, 2004.

[4601] Daniel Helmer, The Poor Man's FBCB2: R U Ready 4 the 3G Celfone?, Armor, Nov/Dec 2006, p.7.

Some observers have stated that terrorist groups, through use of the Internet, are now challenging the monopoly over mass communications that both state-owned and commercial media have long exercised. A strategy of the terrorists is to propagate their messages quickly and repeat them until they have saturated cyberspace. Internet messages by terrorist groups have become increasingly sophisticated through use of a cadre of Internet specialists who operate computer servers worldwide. Other observers have also stated that al-Qaeda now relies on a Global Islamic Media Unit to assist with its public outreach efforts.[4602]

LAW AND PROPORTIONALITY FOR INFORMATION OPERATIONS

The new U.S. Cyber Command reportedly will follow the law of Armed Conflict, meaning a response taken after receiving an electronic or cyber attack will be scaled in proportion to the attack received, and distinctions will be maintained between combatants and civilians.[4603] However, protection against attack through cyberspace is a new task for the military, and the offensive tools and other capabilities used by DOD to stage retaliatory strikes against enemy systems are highly classified. Experience has shown that a reactive defense is not very effective against increasingly powerful and rapid malicious cyber attacks, or against other malicious activity using the electromagnetic spectrum. A more effective defense against these attacks is to incorporate predictive, active, and pre-emptive measures that allow DOD defenders to prevent, deflect, or minimize the efforts of the attacker.

CYBERWARRIOR EDUCATION

As more U.S. military systems become computerized and linked to networks, there is a growing need for qualified Electronic Warfare operators.[4604] Each year, DOD conducts a Cyber Defense Exercise, where teams of students from the nation's military academies advance their cyber skills in practice competition

---

[4602] Jacquelyn S. Porth, Terrorists Use Cyberspace as Important Communications Tool, U.S. Department of State, USInfo.State.Gov, May 5, 2006, [http://usinfo.state.gov/is/Archive/2006/May/08-429418.html].

[4603] The Law of Armed Conflict (LOAC) is a part of public international law that regulates the conduct of armed hostilities between nations, and is intended to protect civilians, the wounded, sick, and shipwrecked. LOAC training for U.S. military is a treaty obligation for the United States under provisions of the 1949 Geneva Conventions. Also, under 18 U.S. Code 2441, war crimes committed by or against Americans may violate U.S. criminal law. James Baker, When Lawyers Advise Presidents in Wartime, Naval War College Review, Winter 2002, Vol. LV, No. 1. Terry Kiss, ed., Law of Armed Conflict, Air University Library, Maxwell AFB, Jan 2005, [http://www.au.af.mil/au/aul/bibs/loacots.htm]. Josh Rogin, Air Force to Create Cyber Command, FCW.COM, Nov 13, 2006, [http://www.fcw.com/article96791-11-13-06-Print&printLayout].

[4604] Patience Wait, Army Shores up EM spectrum skills, Government Computer News, Mar 19, 2007.

where they deliberately hack into test networks, and also protect these test networks against intrusions by other teams. However, DOD must attract, train, and retain skilled information technology professionals beyond those enrolled in the military academies.

In an attempt to solve this problem, the Air Force Research Laboratory (AFRL) Cyber Operations Branch offers a 10-week summer program each year for university students, consisting of intensive studies in cyber security. The Advanced Course in Engineering (ACE) Cyber Security Boot Camp has been held at Rome, NY for the past 4 years, and involves between 40 and 60 student applicants from Air Force and Army pre-commissioning programs, some National Science Foundation Cyber Corps Fellows, and some civilian college students. For 2006, the theme was "Cybercraft", described as a non-kinetic weapon platform that seeks dominance in cyberspace, corresponding to the new mission of the Air Force to 'fly and fight in air, space, and cyberspace', according to program director Dr. Kamal Jabbour. Students study legal and policy issues, cryptography, computer network defense and attack, steganography, and analysis of malicious code. ACE students also spend an average of three days per week in internships at the Air Force Research Laboratory, or with local industry partners, and participate in officer development activities. The faculty for ACE is drawn from Syracuse University, West Point, and Norwich University.

DHS and the National Science Foundation (NSF) have recognized the ACE program as an official internship program for Federal Cyber Service Scholarship for Service (SFS) program. The SFS program seeks to increase the number of skilled students entering the fields of information assurance and cyber security by funding universities to award 2-year scholarships in cyber security. Graduates are then required to work for a federal agency for two years. Recent ACE graduates are now working at the Air Force Office of Special Investigations, the AFRL, and the NSA.

Also, as a result of ACE summer program success with college students, in September 2006, Syracuse University developed a special cyber security course to be offered in 12 high schools in New Your State. Currently, Syracuse University offers 29 introductory cyber security courses in 148 high schools throughout New York, New Jersey, Maine, Massachusetts, and Michigan. High school students who successfully complete the cyber security courses can receive Syracuse college credits in computer science and engineering.

POLICY ISSUES

Potential oversight issues for Congress may include the following areas.
Could provocative actions, for example, intelligence gathering by the U.S. military that involves using intrusive cyber or electronic warfare tools to monitor enemy system activity, or copy important data files, be challenged by other nations as a violation of the law of Armed Conflict? Exploratory intrusions by U.S. military computers to gather intelligence may provoke other strong or unexpected

responses from some countries or extremist groups that are targeted for monitoring by DOD.

Several questions also may arise when conducting a retaliatory cyber or electronic warfare counterstrike: (1) if the attacker is a civilian, should the attack be considered a law enforcement problem rather than a military matter?; (2) if a U.S. military cyberattack against a foreign government also disables civilian infrastructure, can it be legally justified?; (3) how can the military be certain that a targeted foreign computer system has not been innocently set up to appear as an attacker by another third party attacker?

Some observers have stated that success in future conflicts will depend less on the will of governments, and more on the perceptions of populations, and that perception control will be achieved and opinions shaped by the warring group that best exploits the global media[4605]. As a result of the increasingly sophisticated use of networks by terrorist groups and the potentially strong influence of messages carried by the global media, does DOD now view the Internet and the mainstream media as a possible threat to the success of U.S. military missions? How strongly will U.S. military PSYOP be used to manipulate public opinion, or reduce opposition to unpopular decisions in the future?

Another emerging issue may be whether DOD is legislatively authorized to engage in PSYOP that may also affect domestic audiences.[4606] DOD Joint Publication 3-13, released February 2006, provides current doctrine for U.S. military Information Operations, and explains the importance of achieving information superiority.[4607] However, the DOD Information Operations Roadmap, published October 2003, states that PSYOP messages intended for foreign audiences increasingly are consumed by the U.S. domestic audience, usually because they can be re-broadcast through the global media. The Roadmap document states that, "...the distinction between foreign and domestic audiences becomes more a question of USG (U.S. Government) intent rather than information dissemination practices (by DOD)."[4608]

[4605] Maj. Gen. Robert Scales (Ret), Clausewitz and World War IV, Armed Forces Journal, July 2006, p.19.

[4606] Psychological Operations are authorized for the military under Title 10, USC, Subtitle A, Part I, Chapter 6, Section 167.

[4607] DOD Joint Publication 3-13, Information Operations, Feb 13, 2006, [http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf].

[4608] DOD Information Operations Roadmap, October 30, 2003, p.26. [http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB177/info_ops_roadmap.pdf].

This may be interpreted to mean that DOD has no control over who consumes PSYOP messages once they are re-transmitted by commercial media.

CURRENT LEGISLATION

Currently, there are no outstanding bills in the 110th Congress linked to Information Operations or Cyberwarfare.

Network Centric Operations: Background and Oversight Issues for Congress, RL32411 (March 15, 2007).

CLAY WILSON, CONGRESSIONAL RESEARCH SERV., NETWORK CENTRIC OPERATIONS: BACKGROUND AND OVERSIGHT ISSUES FOR CONGRESS (2007), *available at* http://www.intelligencelaw.com/library/secondary/crs/pdf/RL32411_3-15-2007.pdf.

Order Code RL32411

Updated March 15, 2007

Clay Wilson
Specialist in Technology and National Security
Foreign Affairs, Defense, and Trade Division

Summary

Network Centric Operations (also known as Network Centric Warfare) is a key component of DOD planning for transformation of the military. Network Centric Operations (NCO) relies on computer equipment and networked communications technology to provide a shared awareness of the battle space for U.S. forces. Proponents say that a shared awareness increases synergy for command and control, resulting in superior decision-making, and the ability to coordinate complex military operations over long distances for an overwhelming war-fighting advantage. NCO technology saw limited deployment in Afghanistan and, more recently, increased deployment in Operation Iraqi Freedom (OIF). Several DOD key programs are now underway for deployment throughout all services.

Congress may be concerned with oversight of the DOD organization and the individual services as they transform through NCO programs that are intended to promote a management style and culture with joint objectives. Oversight may involve a review of service efforts to improve interoperability of computer and communications systems, and may also involve questions from some observers about whether DOD has given adequate attention to possible unintended outcomes resulting from over-reliance on high technology. Updates may also be required on emerging threats that may be directed against increasingly complex military equipment.

This report describes technologies that support NCO, and includes (1) questions about possible vulnerabilities associated with NCO; (2) a description of electronic weapons, and other technologies that could be used as asymmetric countermeasures against NCO systems; (3) descriptions of several key military

programs for implementing NCO; (4) a list of other nations with NCO capabilities; and, (5) a description of experiences using NCO systems in recent operations involving joint and coalition forces. The final section raises policy issues for NCO that involve planning, network interoperability, acquisition strategies, offshore outsourcing, technology transfer, asymmetric threats, coalition operations, and U.S. military doctrine.

Appendices to this report give more information about the global network conversion to Internet Protocol version 6 (IPv6), views on Metcalfe's Law of Networks, and possible perverse consequences of data-dependent systems.

This report will be updated to accommodate significant changes.

Introduction

This report provides background information and discusses possible oversight issues for Congress regarding DOD's strategy for implementing a network centric approach to warfare, otherwise known as Network Centric Operations (NCO). NCO forms a central part of the Administration's plans for defense transformation.

Proponents argue that a Network Centric approach may improve both the efficiency and effectiveness of U.S. combat operations. However, when NCO was originally envisioned, the U.S. military was structured to counter conventional threats, including possibly, two regional war scenarios involving national armies.[4609] Now, partlyfrom recognition that U.S. forces were inadequately prepared for the insurgency in Iraq and the wider hunt for terrorists worldwide, DOD reportedly may be considering new policy that places less emphasis on waging conventional warfare and more on dealing with counterinsurgency, terrorist networks, and other non-traditional threats.[4610]

Some observers now question the effectiveness of Network Centric Operations, and its relevance to different types of conflict, including close urban combat. Others argue that technology may be dictating military strategy, and point out that the military's extreme reliance on high technology may also present a new

---

[4609] Vice Adm. A. Cebrowski, John Gartska, Net-Centric Warfare: Its Origin and Future, Proceedings, U.S. Naval Institute, January 1998, [http://www.usni.org/Proceedings/Articles98/PROcebrowski.htm]. Ivan Eland, Bush Versus the Defense Establishment, Issues Online, National Academy of Sciences, Summer 2001, [http://www.issues.org/17.4/eland.htm]. U.S. Defense Policy, GlobalSecurity.Org, [http://www.globalsecurity.org/military/intro/intro.htm].

[4610] Bradley Graham, Pentagon Prepares to Rethink Focus on Conventional Warfare, Washington Post, Jan. 26, 2005, A2.

vulnerability that adversaries may exploit.[4611] Still others pose questions about (1) the interoperability of information systems for joint and coalition forces, (2) a shortage of available bandwidth to support Net Centric Operations, and (3) possible unexpected outcomes when organizations rely on data-dependent systems.

Background

Defense Transformation

NCO is recognized as the cornerstone of military transformation that is occurring in many countries around the world. Defense transformation for the U.S. military involves large-scale and possibly disruptive changes in military weapon systems, organization, and concepts of operations. These changes are the result of technology advances, or the emergence of new international security challenges.[4612] Many observers believe that a U.S. military transformation is necessary to ensure U.S. forces continue to operate from a position of overwhelming military advantage in support of national objectives.[4613] The Administration has stated that DOD must transform to achieve a fundamentally joint, network centric, distributed force structure capable of rapid decision superiority. To meet this goal, DOD is building doctrine, training, and procurement practices to create a culture of continual transformation that involves people, processes, and systems.

Past experimentation to stimulate wider innovation for military operations and NCO has been coordinated by the DOD Office of Force Transformation (OFT). However, DOD plans to shift many ongoing technology initiatives formerly managed by the OFT into the DOD Research and Engineering Directorate. In addition, a reorganization of the office of the DOD Undersecretary for Policy will lead to establishment of a new Office of Strategic Futures, which will examine technology issues that may affect U.S. defense policies. The reorganization is reportedly planned for early 2007, and will require congressional approval for a new assistant secretary position.[4614]

[4611] Military technology emulates commercial technology in the hope that adapting the latest commercial innovation to war may bring to national security the same benefits that accrued to commercial enterprises. Alfred Kaufman, Caught in the Network: How the Doctrine of Network-Centric Warfare Allows Technology to Dictate Military Strategy, Armed Forces Journal, Feb. 5, 2005, p.20-22.

[4612] For more information, see CRS Report RL32238, Defense Transformation: Background and Oversight Issues for Congress, by Ronald O'Rourke.

[4613] U.S. Department of Defense, Transformation Planning Guidance, Apr. 2003.

[4614] Gopol Ratnam, Pentagon to dissolve transformation office, AirForceTimes, Aug. 29, 2006, [http://www.airforcetimes.com/story.php?f=1-292925-2066882.php].

Definition of Network Centric Operations

NCO is a theory which proposes that the application of information age concepts to speed communications and increase situational awareness through networking improves both the efficiency and effectiveness of military operations. Proponents advocate that this allows combat units to be smaller in size, operate more independently and effectively, and undertake a different range of missions than nonnetworked forces.[4615] Networked sensors are sources of data, and data is processed into information. NCO is intended to increase collaboration through enabling the free flow of information across the battlespace so that acquired data is shared, processed into information, and then provided quickly to the person or system that needs it.[4616]

Proponents argue that a strong and flexible network linking military forces will speed up the pace of warfare, prevent or reduce fratricide, and also provide the means for getting more combat power out of a smaller force.[4617] These proponents also argue that theory and practice have merged through achieving proof of concept in the major operations phase of Operation Iraqi Freedom, and that NCO is now an accepted and enduring part of current and future combat.[4618] Procurement policy to support joint NCO efforts is also intended to improve economic efficiency by eliminating stovepipe systems, parochial interests, redundant and non-interoperable systems, and by optimizing capital planning investments for present and future information technology systems.

Command and control objectives of NCO include the following:

[4615] The Office of Force Transformation (OFT) and the Command and Control Research Program (CCRP) of the Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD/C3I) have been collaborating to develop metrics to support experiments, studies, and analyses related to Military Transformation and Net Centric Operations. To date the effort has been led by RAND, with support from Evidence Based Research, Inc. (EBR), and participation of the government sponsors. The NCO theory posits that the application of information technologies has a positive impact on military effectiveness. Independent variables include networking, information sharing, collaboration, etc. Dependent variables include speed of command and force effectiveness. Dr. Kimberly Holloman, Evidence Based Research, Inc., "The Network Centric Operations Conceptual Framework," Presentation at the Network Centric Warfare 2004 Conference, Washington, D.C., Jan. 20, 2004, [http://www.oft.osd.mil/library/library.cfm?libcol=2].

[4616] Ted McKenna, Developers of Net-Centric Warfare Battle Complexity, Journal of Electronic Defense, July 2005, No.7, p.23.

[4617] John Tirpak, The Network Way of War, Air Force Magazine, March 2005, p.31.

[4618] Dan Gonzales, et.al., Assessing the Value of Information Superiority for Ground Forces – Proof of Concept, National Defense Research Institute, 2001, RAND, Sant Monica, California. Dennis Murphy, Network Enabled Operations in Operation Iraqi Freedom: Initial Impressions, Center for Strategic Leadership, U.S. Army War College, March 2005, vol. 06-05, p. CSL-4.

(1) Self-synchronization, or doing what needs to be done without traditional orders.
(2) Improved understanding of higher command's intent.
(3) Improved understanding of the operational situation at all levels of command.
(4) Increased ability to tap into the collective knowledge of all U.S. (and coalition) forces to reduce the "fog and friction" commonly referred to in descriptions of fighting.[4619]

Some argue that as new concepts and technologies are proven over time, NCO may also become a stabilizing deterrence against extended conflict. For example, if adversary targets are neutralized by NCO systems before they can engage in fighting with U.S. forces, then the battle can be finished before it has really begun.[4620] Others argue that wealthy countries now only have a temporary advantage which may be reduced as NCO technology becomes less expensive and as technical knowledge spreads to other nations, and also to terrorist groups.[4621] Hence, to maintain its advantage, the United States must continue to refine the uses of technology to increase adaptability for both joint and coalition NCO operations.

Other observers have wondered whether proponents of NCO are making claims that create unrealistic expectations. They wonder if the DOD model for network centric operations may underestimate an enemy's ability to deceive high technology sensors, or block the information necessary for NCO to be effective. A possible vulnerability cited by observers may be the fact that DOD has openly published its plans for using NCO technologies in future warfare, thus giving an enemy time to create strategies to avoid strengths and attack weaknesses.[4622]

Advantages of the Net Centric Approach

National security in the "Information Age" involves a complex environment, where U.S. forces are confronted by instantaneous media coverage, insurgencies, terrorist cells, regional instability, and adversaries using commercially available state-of-the-art high technology devices. Therefore, military operations are now

---

[4619] "Fog" is the term that describes the uncertainty about what is going on during a battle, while "Friction" is the term that describes the difficulty translating a commander's intent into battlefield actions.

[4620] Dr. Kimberly Holloman, Evidence Based Research, Inc., The Network Centric Operations Conceptual Framework, Presentation at the Network Centric Warfare 2004 Conference, Washington, DC, Jan. 20, 2004, [http://www.oft.osd.mil/library/library.cfm?libcol=2].

[4621] Scott Renner, C2 Information Manager, MITRE Corporation, Building Information Systems for NCW, 4th Annual Multinational C4ISR Conference, McLean, Virginia, May 6, 2004.

[4622] Alfred Kaufman, "Be Careful What You Wish For: The Dangers of Fighting with a Network Centric Military," Journal of Battlefield Technology, vol 5, no.2. July 2002, and "Networking in an Uncertain World," Journal of Battlefield Technology, vol 5, no.3, Nov. 2002.

characterized by greater complexity. Events involving greater complexity are less effectively controlled through traditional industrial-age methods that de-construct problems into a manageable series of predictable pieces.[4623] However, the command and control objectives of NCO seem to align closely with many of the key properties of complexity – nonlinear interaction, decentralization, and self-organization.

Proponents of NCO support the theory that power is increasingly derived from information sharing, information access, and speed. This view is reportedly also supported by results of recent military operational experiences[4624] showing that when forces are truly joint, with comprehensively integrated capabilities and operating according to the principles of NCO, they can fully exploit the highly path-dependent[4625] nature of information age warfare. Some resulting military advantages that are expected from applying NCO systems to military operations include the following:

(1) Networked forces can consist of smaller-size units that can travel lighter and faster, meaning fewer troops with fewer platforms and carrying fewer supplies may be able to perform a mission effectively, or differently, at a lower cost.
(2) Networked forces can fight using new tactics. During OIF, U.S. Army forces utilized movement that was described by some as "swarm tactics." Because networking allows soldiers to keep track of each other when they are out of one another's sight, forces in Iraq could move forward spread out in smaller independent units, avoiding the need to maintain a tight formation. Using "swarm tactics," unit movements are conducted quickly, without securing the rear. Network technologies enable all units to know each other's location. If one unit gets into trouble, other independent units nearby can quickly come to their aid, by "swarming" to attack the enemy from all directions at once. Benefits may include the following: (1) it is harder for an enemy to effectively attack a widely dispersed formation; (2) combat units can cover much more ground, because they do not have to maintain a formation; (3) knowing the location of all friendly units reduces fratricide during combat operations; and (4) swarming can allow

[4623] Murray Gell-Mann, "What is Complexity?" Complexity, John Wiley and Sons, 1995, Vol. 1, No.1.

[4624] John Garstka, "Network-Centric Warfare Offers Warfighting Advantage," Signal Forum, Signal Magazine, May 2003.

[4625] Path-dependence means that small changes in the initial conditions will result in enormous changes in outcomes. Therefore, a military force must define initial conditions that are favorable to their interests, with the goal of developing high rates of change that an adversary cannot outpace. Dan Caterinicia and Matthew French, "Network-Centric Warfare: Not There Yet," Federal Computer Week, June 9, 2003, [http://www.fcw.com/fcw/articles/2003/0609/cov-netcentric-06-09-03.asp].

an attack to be directed straight into the heart of an enemy command structure, undermining support by operating from the inside, rather than battling only on the periphery.

(3) The way individual soldiers are expected to think and act on the battlefield is also changing. When a unit encounters a difficult problem in the field, they can radio the Tactical Operations Center, which types the problem into an online chat room, using Microsoft Chat commercial software. The problem is then "swarmed" by experts who may be located as far away as the Pentagon.[4626]

(4) The sensor-to-shooter time is reduced. Using NCO systems, soldiers in the field may have the capability to conduct an "on site analysis" of raw intelligence from sensor displays, rather than waiting for "return analysis" reports to arrive back from the continental United States.[4627]

This has led some to question the investment in NCO.

Questions About the Net Centric Approach

DOD officials have stated that it is irregular and unconventional conflicts, rather than confrontations with standing armies, that will dominate U.S. military operations for the foreseeable future.[4628] Accordingly, some observers question the utility of NCO in urban combat operations and for counterinsurgency operations, and ask whether the U. S. military currently places too much emphasis on high-technology. In operations in Afghanistan and in urban warfare in Iraq, NCO has reportedly reduced fratricide among friendly forces.[4629] However, in Afghanistan and Iraq, the insurgents mixin with the population, and are able to get very close to U.S. forces. This tactic alone reportedly may negate

---

[4626] Joshua Davis, "If We Run Out of Batteries, This War is Screwed," Wired Magazine, June 2003, [http://www.wired.com/wired/archive/11.06/battlefield.html].

[4627] For example, one UAV equipped with multiple sensors can survey the same area as ten human sentries, or one could monitor areas contaminated with radiological, chemical or biological agents without risk to human life. Today, DOD has in excess of 90 UAVs in the field; by 2010, this inventory is programmed to quadruple. U.S. Department of Defense, Office of the Secretary, Unmanned Aerial Vehicles Roadmap, 2002-2007, Dec. 2002.

[4628] Donna Miles, Army Experts: Unconventional Conflicts to Dominate Future Operations, American Forces Information Service News Articles, Oct. 12, 2006. John Doyle, Conuterinsurgency Forces Need to Control Cyberspace, Aviation Week and Space Technology, Oct. 23, 2006, p.64.

[4629] Rodney Pringle, NCW Changing Urban Warfare, Official Says, AviationWeek NetDefense, February 3, 2005, [http://www.aviationow.com/avnow/news/channel_netdefense_story.jsp?view=story&id=news/NCW02035.xml].

much of the technological and military advantage of superior coalition forces.[4630] Others question whether information itself may be overrated as a useful military asset (See Appendix C, Perverse Consequences of Data-Dependent Systems).

NCO Theory Remains Scientifically Untested

Proponents say that a growing body of evidence highlights a very strong relationship between information advantage, cognitive advantage, and increased lethality and survivability at the tactical level.[4631] DOD has conducted several exercises to demonstrate the effectiveness of network centric strategies to improve success in combat scenarios.[4632] However, some researchers warn that thorough testing of NCO concepts is vital before systems are deployed[4633], and others argue that NCO theory may manifest important and pervasive flaws.[4634] These researchers state that "...the theory of network-centric warfare...cannot substantiate a claim to scientific status, despite its mesmerizing transformational luster". They also state that "...the [NCO] thesis simultaneously overstates the promise of information and communications technology, while being incapable of adequately realizing the great potential the technology does offer."[4635]

Their argument is that NCO theory has several paradoxes, including: (1) no proper definition of NCO yet exists, but proponents claim that experimentation supports the NCO hypothesis, (2) experimental evidence equally supports multiple alternative explanations for potentially improved performance with

---

[4630] Jim Garamone, No Silver Bullet to Counter Explosive Devices, Head of Anti-IED Office Says, American Forces Information Services DefenseLink, September 7, 2006, [http://www.defenselink.mil/News/NewsArticle.aspx?ID=743].

[4631] John Garstka, Network-Centric Warfare Offers Warfighting Advantage, Signal Magazine, May, 2003. Walter Perry, et.al., Exploring Information Superiority: A Methodology for Measuring the Quality of Information and Its Impact on Shared Awareness, National Defense Research Institute, 2004, RAND, Santa Monica, California.

[4632] Guy Norris, Major Exercise to Prove Net Warfare, Flight International, December 2004, p.5.

[4633] Walter Perry, James Moffat, Information Sharing Among Military Headquarters, [http://www.rand.org/pubs/monographs/MG226/].

[4634] Metcalfe's Law observes that the potential value of a communications network increases (or scales) as a function of the square of the number of nodes that are connected by the network. Critics of NCO argue that Metcalfe's Law breaks down at a sufficiently large number of nodes. The military symptoms are chronic bandwidth deficiency, information overload, and increasing costs for information management solutions, such as "data fusion" centers. Ralph Griffin and Darryn Reid, A Woven Web of Guesses, Proceedings of the 8th International Command and Control Research and Technology Symposium, Washington D.C., June 17-19, 2003. For more information on Metcalfe's Law, see Appendix B.

[4635] Darryn Reid et. al., All that Glitters: Is Network-Centric Warfare Really Scientific?, Defense and Security Analysis, vol.21, No.4, p. 359 and p.360.

networking, and (3) the conclusions of proponents are based on an invalid notion of knowledge development, known as "inductivisim". These researchers maintain that a close examination of the structure of repeated NCO experiments shows that the only hypothesis that has actually been tested is a refutation of the theory that networks cannot yield improvements.

Finally, these researchers have asked how it can be possible for faults to remain unrecognized despite troubling results found through critical review and testing. They warn that contemporary military theory may be encouraging NCO proponents to seek confirmation and ignore refutation of their ideas.

Overconfidence about the Effectiveness of NCO

Proponents of NCO say that shared situational awareness enables collaboration and self-synchronization and enhances speed of command, which increasing mission effectiveness. Critics, however, are concerned that dangerous assumptions are being made by military planners about how future forces will benefit from "information dominance" to such a degree that fewer soldiers will be needed, or that U.S. forces will not require as much protection because they will be able to act ahead of enemy action. They believe that the doctrine of "see first, act first", that underlies NCO, may be flawed because the tempo of operations may outpace the ability of U.S. forces to assess and respond.[4636]

While a network may provide better access to information, usually about the activities of one's own side, that information may not be complete and may not necessarily enable an accurate understanding of the situation. They have indicated that sensor-based situational awareness may not reflect an accurate picture of operational reality.[4637]

Other observers say that the military leadership's commitment to NCO may stifle useful criticism from operational commanders. These observers question whether the U.S. military is constructing it forces to prepare to fight the type of wars they want to fight, and rather than the wars they are likely to fight. For example, if NCO is intended to make wars short in duration, then inferior adversaries may likely try to draw U.S. forces into a protracted conflict of lower intensity, and will seek to win merely by avoiding defeat, while U.S. political will dissolves as

---

[4636] Proponents of NCO say that Information Age technology makes time and distance less relevant, thus increasing the pace of events and the operational tempo of warfare. David Alberts, John Garstka, Frederick Stein, Network Centric Warfare, DOD Command and Control Research Program, Oct. 2003, p. 21. Ted McKenna, Promises, Promises, Journal of Electronic Defense, November 2005, vol. 28, No.11, p. 10.

[4637] Giles Ebbutt, Flaws in the system: modern operations test the theory of network centricity, Jane's International Defence Review, July 2006, Vol 39, p.67.

expenses mount. The inferior opponent may avoid superior U.S. firepower by simply denying a target for our complex and sophisticated weapons.[4638]

Reduced Effectiveness for Urban Counter-Insurgency Operations

Some military researchers say that opponents using guerilla tactics can significantly reduce the value of high-technology security measures, and that the utility of NCO can be less certain in urban counter-insurgency operations.[4639] When NCO is employed against conventional forces, a sensor detects a target, passes information to a decision-making process, the most effective weapon available is selected, and the target is engaged. However, when opponents hide behind walls, in sewers, or inside buildings, they may be difficult for NCO sensors to detect. If the enemy is better at concealment than U.S. forces are at finding them, then our forces may also become more vulnerable.[4640]

Some observers report that during Operation Iraqi Freedom (OIF), in order to understand the enemy, U.S. forces had to "go out and meet them on the ground", meaning that effective reconnaissance often required engaging the enemy in close combat. These observers say that interviews with OIF warfighters suggested that modern surveillance technology did not alter that condition, and in some instances did not "...provide forces in Iraq in Spring 2003 and onwards with very much insight on the opposing forces."[4641] This suggests that DOD should perhaps reexamine several of its basic assumptions about NCO and the power of technology for surveillance and information dominance.

Underestimating our Adversaries

NCO relies heavily on deployment of a network of sensors to detect movement and position of both friendly and enemy forces. However, a study by the Rand Corporation in 2002 concluded that, "...as remote assets become more capable, it is likely that a future [enemy] force will develop counter technologies and become

---

[4638] J. Bailey, "Over by Christmas: Campaigning, Delusions and Force Requirements, AUSA Land Warfare Institute, The Land Warfare Papers, No. 51, September 2005, [http://www.ausa.org/pdfdocs/LWP_51WBailey.pdf].

[4639] Brian Jackson, Breaching the Fortress Wall: Understanding Terrorist Efforts to Overcome Defensive Technologies, presentation by RAND corporation at the Rayburn House Office Building, October 24, 2006. J.A. Bailey, Over by Christmas: Campaigning, Delusions and Force Requirements, The Institute of Land Warfare, Association of the United States Army, Land Warfare Papers, No. 51, September, 2005.

[4640] Giles Ebbutt, Flaws in the system: modern operations test the theory of network centricity, Jane's International Defence Review, July 2006, Vol 39, p.57.

[4641] Curtis Taylor, Trading the Saber for Stealth: Can Surveillance Technology Replace Traditional Aggressive Reconnaissance?, AUSA Land Warfare Institute, The Land Warfare Papers, No. 53, September 2005, [http://www.ausa.org/pdfdocs/LWP_53.pdf].

more sophisticated at cover, concealment, deception, and electronic warfare. Taking all of these into consideration, the net effect may actually be a decrease of knowledge and ultimately of situational awareness on the battlefield."[4642]

Our adversaries in Iraq and Afghanistan have taken actions to directly bypass U.S. NCO sensors, and to negate the usefulness of U.S. high technology NCO weapons. Examples include (1) use of suicide bombings and Improvised Explosive Devices (IEDs); (2) hostile forces intermingling with civilians used as shields; or (3) irregular fighters and close-range snipers that swarm to attack, and then disperse quickly.[4643]

Other possible uses of technology by adversaries of the United States to attack NCO capabilities may include use of (1) powerful directed energy devices to disrupt commercial satellite signals;[4644] (2) smaller directed energy devices to burn out computer circuits at a distance,[4645] and (3) malicious computer code to subvert controls for complex weapon systems.

Overreliance on Information

Some observers state that huge information resources may be overrated as an asset for creating effective military operations, and that important military decisions may not always lend themselves to information based rational analysis.[4646] They argue that discussions of military transformation have been overwhelmingly focused on the rewards of information, and that the military services, national security establishment, and intelligence community have not

---

[4642] John Matsumura, et. al., Preparing for Future Warfare with Advanced Technologies, Rand, Arroyo Center, 2002, p.11.

[4643] For more information, see CRS Report RS22330, Improvised Explosive Devices in Iraq: Effects and Countermeasures, by Clay Wilson.

[4644] A group of Iranians last summer reportedly jammed a U.S.-built commercial satellite broadcasting pro-rebel information into that Middle Eastern country. The specific transponder that was carrying the broadcast was disrupted for about two weeks by Iranians operating at a teleport in Cuba, according to industry sources. Amy Butler, "Heavy DoD Reliance On Commercial SATCOM Prompts Questions of Protection," Defense Daily, Apr. 13, 2004.

[4645] Directed energy weapons could include a High-Energy Microwave device (HPM), activated by a chemical explosion. Such a bomb-driven device, the size of a suitcase and using a specially-shaped antenna, could theoretically direct a narrow-beam energy pulse that could damage a computer within a distance of 1 kilometer. Prof. Robert Harney, Naval Postgraduate School, personal communications, Apr. 12, 2004.

[4646] Martin Burke, Information Superiority Is Insufficient To Win In Network Centric Warfare, Joint Systems Branch, Defense Science and Technology Organization, 2001, [http://www.dodccrp.org/events/2000/5th_ICCRTS/cd/papers/Track4/024.pdf].

thoroughly studied the risks associated with data-dependent military doctrine.[4647] Some issues raised by these observers include:

(1) Reliance on sophisticated information systems may lead to management overconfidence.[4648]
(2) Quantitative changes in information and analysis often lead to qualitative changes in individual and organizational behavior that are sometimes counterproductive; e.g., as information technology reveals more targets, ammunition may be expended faster, leading to greater dependence on logistics support.[4649]
(3) An information-rich, opportunity-rich environment may shift the value of the information, redefine the mission objectives, and possibly increase the chances for perverse consequences. (See Appendix C, Perverse Consequences of Data-Dependent Systems.)

Management of Information Overload

The proliferation of sensors in the battlefield has created what some would call "data overload", where large inflows of real-time data could overwhelm users, and jeopardize the decision-making process. DOD is examining using new "data fusion" centers, which would use special software to filter out battlefield data that is unneeded by warfighters. Also, to make sure that radio frequencies in use don't encounter interference, the US Air Force Electronic Systems Center is working to design a universal tool called the Joint Interface Control Officer (JICO) Support System, which is intended to manage all radio communications traffic in tactical situations.[4650]

Increasing Complexity of Military Systems

Military systems and software are becoming increasingly complex. Software is used to process sensor data, identify friend and foe, set targets, issue alerts,

---

[4647] Michael Schrage, Perfect Information and Perverse Incentives: Costs and Consequences of Transformation and Transparency, Security Studies Program Working Paper, Massachusetts Institute of Technology, E38-600, May 2003, p.15.

[4648] Michael Schrage, Perfect Information and Perverse Incentives: Costs and Consequences of Transformation and Transparency, Security Studies Program Working Paper Massachusetts Institute of Technology, E38-600, May 2003, p.4.

[4649] Dr. Kimberly Holloman, Evidence Based Research, Inc., "The Network Centric Operations Conceptual Framework," Presentation at the Network Centric Warfare 2004 Conference, Washington, D.C., Jan. 20, 2004, [http://www.oft.osd.mil/library/library. cfm?libcol=2].

[4650] Staff, U.S. Forces in Iraq Face Obstacles in Getting Intelligence They Need, Inside the Pentagon, May 5, 2005, Vol. 21, No.18, p.10. Ted McKenna, Orchestrating Tactical Communications, Journal of Electronic Defense, August 2005, No 8, P. 22.

coordinate actions, and guide decisions for manned and unmanned combat vehicles on land, sea, and in the air. For example, observers estimate that at least 31 million lines of computer code will be required to operate the Army Future Combat System.[4651] Also, many military combat systems which now operate as stand-alone equipment will eventually be tied into network systems.[4652] However, as complexity grows, components of networked systems may sometimes process information received from other systems whose capabilities, intentions, and trustworthiness are not always known.[4653]

A recent article published by the Carnegie Mellon Software Engineering Institute about the growing complexity of military computerized systems argues the following:

> *With modern complex systems of systems, most systems are described as "unbounded" because they involve an unknown number of participants or otherwise require individual participants to act and interact in the absence of needed information.*
>
> *For the complex systems of systems being constructed today and defined for the future, it is no longer possible for any human or automated component to have full knowledge of the system. Each component must depend on information received from other systems whose capabilities, intentions, and trustworthiness are unknown.*
>
> *Unbounded systems of systems are fast becoming the norm in many of the most demanding military and commercial applications. These include command-and-control systems, air traffic control systems, the electric power grid, the Internet, individual aircraft, enterprise database systems, and modern PC operating systems. For example, in net-centric warfare as applied by U.S. troops at the beginning of the current war in Iraq, agility and rapid progress were achieved by direct interactions among ground troops, helicopters, artillery, and bombers using equipment whose designs did not anticipate such usage and the accompanying mission changes.*

[4651] David Talbot, How Technology Failed in Iraq, Technology Review, November 2004, p.1.

[4652] Goodrich Engine Control Systems, [http://www.enginecontrols.goodrich.com/ small/products/ecu.shtml]..

[4653] David Fisher, Dennis Smith, Emergent Issues in Interoperability, Carnegie Mellon Software Engineering Institute, No.3, 2004, [http://www.sei.cmu.edu/news-at-sei/columns/eye-on-integration/2004/3/ eye-on-integration-2004-3.htm].

Most systems of systems use their component systems in ways that were neither intended nor anticipated. Assumptions that were reasonable and appropriate for individual component systems become sources of errors and malfunction within systems of systems. As a result, the individual systems – and the system of systems as a whole -- acquire vulnerabilities that can be triggered accidentally by normal actions of users and automated components, or exploited consciously by intelligent adversaries.

Often when problems of interoperability arise in complex systems, there is a tendency to try to gain greater visibility, to extend central control, and to impose stronger standards. Not only are these actions ineffective in complex systems, they also increase the likelihood of certain kinds of accidents, user errors, and other failures. What are called normal accidents are inherent and occur naturally in complex systems. The frequency of normal accidents increases with the degree of coupling in systems. Coupling is increased by central control, overly restrictive specifications, and broadly imposed interface standards. Developers of systems of systems should strive for loose coupling.[4654]

Vulnerabilities of Military Software and Data

Military computers are continuously threatened by attack from hackers, or others with malicious intent. One example of a hacker attack is the British programmer, Gary McKinnon, who reportedly used commercially-available off-the-shelf software in several attacks through the Internet to successfully penetrate hundreds of military computers, causing measurable damage,[4655] and forcing

[4654] David Fisher and Dennis Smith, Emergent Issues in Interoperability, News@ SEI, 2004, No.3, [http://www.sei.cmu.edu/news-at-sei/columns/eye-on-integration/2004/3/ eye-on-integration-2004-3.htm].

[4655] Gary McKinnon has been indicted for breaking into approximately 100 military networks between 2001 and 2002. He is charged with installing Trojan Horses and back doors, stealing military passwords, and disabling networks at Fort Meyers, Fort McNair, the Pentagon, and other locations belonging to the Army, Navy, and Air Force. However, DOD officials claim that no classified data was taken. In May 2006, the U.S. prosecutors secured his extradition from Britain to the United States, where he could face 70 years in prison, plus fines. Larry Greenmeier, To Catch A Hacker, Information Week, May 15, 2006, p. 31. Maija Palmer, "Hacker Cites Easy Access to U.S. Data", Los Angeles Times, May 8, 2006. Brooke Masters, "Briton Indicted as Hacker," Washington Post, Nov. 13, 2003, p. A11, [http://www.washingtonpost.com/wp-dyn/articles/A45963-2002Nov12.html]. MARADMIN, "Marine Corps Announcement of Website Breach," Inside Defense, Oct. 15, 2003, [http://www.insidedefense.com].

portions of several military network to shut down temporarily.[4656] Also, in Afghanistan, stolen military portable computer drives, some containing classified data and software, were recently discovered for sale in the streets, in public markets, and in local shops.[4657]

There is growing controversy about whether the U.S. military should rely on general purpose "open-source" commercial computer software for the command, control, and communications functions in advanced defense systems for tanks, aircraft and other complex equipment. An example of open-source code is the popular computer operating system known as Linux, which has been developed by a worldwide community of programmers who continuously add new software features by building on each others' openly-shared source code. Subscriptions can be purchased from different commercial vendors who will provide technical support for specific versions of the Linux open-source software. In contrast, proprietary code created by other commercial vendors is called "closed-source", and includes software products such as Microsoft Windows. Both open-source and closed-source products which are supported by commercial software vendors are commonly referred to as commercial-off-the-shelf (COTS). However, open-source software appears much less expensive than proprietary software, and the reputation it has earned for general soundness and reliability is helping open-source software gain acceptance by different government organizations and the global business community.

NSA has researched a secure version of Linux, but it is not clear that all military computer systems that use Linux are restricted by the results of that research.[4658] Some experts believe that open-source software violates many security principles, and may be subverted by adversaries who could secretly insert malicious code to cause complex defense systems to malfunction. Other computer experts disagree, stating that precisely because Linux is openly reviewed by a worldwide community of contributing programmers, it has security that cannot easily be

---

[4656] U.S. Attorney's Office, District of New Jersey, Public Affairs Office, Nov. 11, 2002, [http://www.usdoj.gov/usao/nj/publicaffairs/NJ_Press/files/mc1112_r.htm].

[4657] Stolen portable hard drives from military computers, some containing sensitive and classified military information, were found for sale at a local bazaar in Afghanistan. The drives may have come from the main U.S. air base in Bagram, Afghanistan. In addition to launching an investigation, military officials reportedly coped with the problem by sending staff to buy up all the portable computer drives at the local bazaar. Paul Watson, U.S. Military Secrets for Sale at Afghan Bazaar, Los Angeles Times, April 10, 2006, p.A1. Carlotta Gall, At Afghan Bazaar, Military Offers Dollars for Stolen Data, The New York Times, Asia Pacific, April 15, 2006, [http://www.nytimes.com/
2006/04/15/world/asia/15afghanistan.html?ex=1145332800&en=e12bbb6b87a5b3fb&ei
=5087%0A].

[4658] See NSA Security Enhanced Linux, [http://www.nsa.gov/selinux/index.cfm].

compromised by a foreign agency. The open review by many contributors acts as a safeguard against insertion of malicious code.

A recent study by the Defense Information Systems Agency (DISA) states that DOD currently uses a significant variety of open-source computer software programs, and concluded that open-source software is vital to DOD information security. This is partly because many information security tools used by DOD are built using open-source code, and effective counterparts are not available from proprietary COTS products. The study also states that DOD web services and DOD software development would be disrupted without continued use of open-source software. This is because many tools that are basic to web design and software development are based on open-source code.[4659]

Experts at the Naval Post Graduate School reportedly have stated that "software subversion" can only be avoided by using "high-assurance" software that has been proven to be free of any malicious code.[4660] Because of the added development rigor and intensive test procedures required to achieve such proof, high-assurance software would cost considerably more than open-source software.[4661] However, researchers at the Massachusetts Institute of Technology have reportedly found that as the complexity of a system increases, additional testing does not always reduce the number of vulnerabilities that can remain hidden in computer software.[4662]

Vulnerabilities of Military Equipment to Electronic Warfare

U.S. military forces may be vulnerable to electronic warfare attacks, such as Electromagnetic Pulse (EMP), which is an instantaneous, intense energy field that can overload or disrupt at a distance numerous electrical systems and high

---

[4659] DISA, "Use of Free and Open-Source Software (FOSS) in the U.S. Department of Defense," Mitre Report No. MP 02 W0000101, Version 1.2, Oct. 2002, p. 20, [http://unix.be.eu.org/docs-free/dodfoss.pdf].

[4660] Alexander Wolfe, "Green Hills calls Linux 'Insecure' for Defense," EETimes, Apr. 9, 2004, [http://eetimes.com/showArticle.jhtml?articleID=18900949] and Charles J. Murray, Apr. 19, 2004, "Linux: Unfit for National Security?," EETimes, [http://eetimes.com/show Article.jhtml?articleID=18901858].

[4661] Research at the Naval Postgraduate School has resulted in new security tools for protecting against unauthorized computer and network intrusions. The new technology has been licensed to Lancope Inc. of Alpharetta, Georgia, which has created a new commercial version of the intrusion detection tool, called "StealthWatch." The license was granted because the Naval Postgraduate School intended that the technology become more developed through marketing in the commercial world. William Jackson, "Hasta La Vista, Attacks," Government Computer News, vol.23, no.6, Mar. 22, 2004, p.27.

[4662] Simson Garfinkel, Battling Bugs: A Digital Quagmire, Wired News, November 9, 2005, [http://www.wired.com/news/technology/bugs/0,2924,69369,00.html].

technology microcircuits, which are especially sensitive to power surges. A single, specially designed low-yield nuclear explosion high above a local battlefield area can produce a large-scale electromagnetic pulse (EMP) effect that could result in widespread disruption of electronic equipment, without any fatalities due to blast or radiation. A similar EMP effect on a more limited scale could also be produced by using a high-power microwave device, triggered by a conventional explosive.[4663]

Commercial electronic equipment is now used extensively to support logistics to support the operation of complex U.S. weapons systems. For example, a large percentage of U.S. military communications during Operation Iraqi Freedom was carried by commercial satellites, and much military administrative information is currently routed through the civilian Internet.[4664] Many commercial communications satellites, particularly those in low earth orbit, reportedly may degrade or cease to function shortly after a high-altitude EMP attack.[4665] Special shielding could reduce this vulnerability in future commercial satellites. However, the current vulnerability of high technology equipment and communications to the effects of EMP could create a new incentive for other countries, or terrorists and extremists, to develop or acquire electronic warfare weapons.

Net Centric Technologies and Related Issues

The following is a list of key technology areas used to implement NCO for U.S. forces, and related issues.

Command, Control, Communications, Computers, and Intelligence

C4I capabilities are the nervous system of the military. DOD is seeking to move from a policy of information "push", where information is labeled and sent by data "owners" only to recipients who are deemed appropriate, to a policy of information "pull", where authenticated users within a given community of interest can request and receive all information available to solve a problem, regardless of the data owner. This shift in policy is intended to promote more widespread information sharing and collaboration.[4666]

[4663] For more on EMP, see CRS Report RL32544, High Altitude Electromagnetic Pulse (HEMP) and High Power Microwave (HPM) Devices: Threat Assessments, April 14, 2006, by Clay Wilson.

[4664] Jefferson Morris, "DISA Chief Outlines Wartime Successes," Federal Computer Week, June 6, 2003; and "GAO: DOD Needs New Approach to Buying Bandwidth," Aerospace Daily, Dec. 12, 2003.

[4665] U.S. Congress, House Armed Services Committee, Hearing on Commission to Assess the Threat to the United States from Electromagnetic Pulse Attack, July 22, 2004.

[4666] Memorandum by John Stenbit, DoD Net-Centric Data Management Strategy: Metadata Registration, April 3, 2003.

NCO relies on a high-bandwidth communications backbone consisting of fiber optics and satellites, all communicating using Internet Protocol (IP). By 2008, DOD is planning to switch all communications systems from IPV4 to the newer IPV6 to improve communications mobility, create more IP addresses, and reduce system management problems (See Appendix A for more on IPV6).[4667]

Interoperability

NCO is highly dependent on the interoperability of communications equipment, data, and software to enable networking of people, sensors, and manned and unmanned platforms. Parts of NCO technology rely on line-of-sight radio transmission for microwave or infrared signals, or laser beams. Other parts of the technology aggregate information for transmission through larger network trunks for global distribution via fiber optic cables, microwave towers, or both low-altitude and high-altitude satellites. The designs for this technology must enable rapid communications between individuals in all services, and rapid sharing of data and information between mobile platforms and sensors used by all military services.[4668] The architectures must also have the ability to dynamically self-heal and re-form the network when one or more communications nodes are interrupted. DOD officials have noted that the new military Global Information Grid (GIG) must be also designed to interoperate securely with the networks of other organizations outside of DOD, including state and local governments, multinational military commands, and the commercial and research communities.[4669]

Some observers question whether the U.S. military can achieve true network and systems interoperability among all services. DOD reportedly intends to integrate the architectures of network systems used by all branches of the military to create a network centric capability linked to the GIG (see section below). To help accomplish this integration, the DOD Joint Staff has created a new Force Capability Board (FCB) to monitor NCO programs for mismatches in funding, or mismatches in capability. When an issue is detected, the FCB reports to the Joint

---

[4667] Rodney Pringle, DOD Faces Challenges, Risks in Transition to IPV6, GAO Study Says, Aviation Week NetDefense, June 6, 2005, [http://www.aviationnow.com/avnow/news/channel_netdefense_story.jsp?view=story&id=news/IPV606095.xml].

[4668] For more information about military network interoperability issues, and the Global Information Grid, see CRS Report RS21590, Defense Program Issue: Global Information Grid, Bandwidth Expansion.

[4669] Sebastian Sprenger, GIG CONOPS Stresses Interoperability with Non-DOD Agencies, Allies, Inside the Pentagon, September 39, 2005.

Requirements Oversight Council, which then provides guidance during budget deliberations at the Pentagon.[4670]

Space Dominance

Satellites are crucial for enabling mobile communications in remote areas, as well as for providing imagery, navigation, weather information, a missile warning capability, and a capability to "reach back" to the continental United States for added support. For example, the Global Positioning System (GPS), consisting of 28 navigation satellites, helps identify the location of U.S. forces, as well as the locations of targets for guided U.S. weapons, such as cruise missiles. The United States maintains 6 orbital constellations for Intelligence, Surveillance, and Reconnaissance (ISR): one for early warning, two for imagery, and three for signals intelligence. Recently, the Army deployed the Coalition Military Network, a new satellite communications system designed to add bandwidth to support coalition forces in remote areas of Iraq.

However, despite the growing number of military satellites, the Defense Information Systems Agency (DISA) reported that up to 84 percent of the satellite communications bandwidth provided to the Operation Iraqi Freedom (OIF) theater was supplied by commercial satellites.[4671] Some drawbacks using commercial satellite services became apparent during OIF. U.S. Army officials indicated that the high volume of traffic on Iridium communications satellites at times overwhelmed that system, which also had to suspend service periodically for updates. In addition, the military reportedly was unable to get encrypted data transmission services from the Inmarsat satellite system at transmission rates of 128 kilobits per second, and instead had to settle for rates of 64 kilobits per second, which was too slow for the Army's needs.[4672]

[4670] Brigadier General Marc Rogers, Director Joint Requirements and Integration Directorate/ J8, for U.S. Joint Forces Command, in U.S. Congress, House Armed Services Subcommittee on Terrorism, Unconventional Threats and Capabilities, Hearing on Military C4I Systems, Oct. 21, 2003 [http://www.cq.com], and Rich Tuttle, "New Organization to Stress Importance of Network Programs," Aerospace Daily, Jan. 30, 2004,

[4671] DOD satellites could not satisfy the entire military demand for satellite bandwidth, and therefore DOD has become the single largest customer for commercial satellite services. DOD sometimes leases commercial satellite bandwidth through DISA, and at other times bypasses the process to buy directly from industry. Bypassing DISA may reduce interoperability and increase redundancies. Jefferson Morris, "GAO: DOD Needs New Approach to Buying Bandwidth," Aerospace Daily, Dec. 12, 2003; "DISA Chief Outlines Wartime Successes," Federal Computer Week, June 6, 2003.

[4672] Warren Ferster, Military Bandwidth Demand Energizes Market, SpaceNews, September 2, 2003, [http://www.space.com/spacenews/archive03/militaryarch_090203.html].

The Transformational Satellite Communications (TSAT) program, run by the Air Force, is part of a plan to build a satellite-based military Internet. The future TSAT program involves launching 5 military satellites in geosynchronous orbit, with laser communication links and Internet-like routers to provide high-speed, high-capacity communications to U.S. warfighters worldwide.[4673] The first TSAT satellite is scheduled to be launched in 2014, with full operational capacity scheduled for 2018.[4674]

The United States remains highly-dependent on space assets, and has enjoyed space dominance during previous Gulf conflicts largely because its adversaries simply did not exploit space, or act to negate U.S. space systems. However, the United States may not be able to rely on this same advantage in the future. For example, a non-state group could possibly take advantage of commercial space-based technology by leasing satellite bandwidth, or by purchasing high-resolution imagery from suppliers in the Soviet Union, China, or other countries that own and operate space assets. Also, less-technically advanced nations and non-state actors may employ electronic jamming techniques, or launch attacks against satellite ground facilities.[4675] News reports show that over a period of several years China has fired high-power laser weapons at U.S. military optical spy satellites as they fly over Chinese territory. Experts say this may have been testing of a new ability to blind the spacecraft. It is not clear how many times China may have tested their ground-based laser system against U.S. satellites, or whether the tests were successful.[4676]

Networked Weapons

Individual air-to-ground weapons will be integrated into network centric operations. Recent tests under the Weapons Data Link Network (WDLN) Advanced Concept Technology Demonstration have shown that various weapons can use standard methods to report their status after release from an aircraft, and provide information on their impact. When pilots and ground controllers have two-way communications with network-enabled weapons after they are in flight, new information can be continually supplied to shift the weapon as the target changes location, or to shift the attack to a different target, or to abort the attack. Networked weapons with these capabilities are projected to become operational

---

[4673] Rebecca Christie, DoD Space Program's Costs Rise as New Plan Takes Shape, Wall Street Journal, February 21, 2006.

[4674] James Canan, Timing in Battle: The T-Sat Edge, American Institute of Aeronautics and Astronautics, Inc., Aerospace America, January, 2006, p.39.

[4675] Testimony from the hearing on Army Transformation, Senate Armed Services Committee, Subcommittee on Airland, Mar. 12, 2003, CQ.com,[http://www.cq.com/aggregatedocs.do].

[4676] Vago Muradian, China Tried to Blind U.S. Sats with Laser, Defense News, September 25, 2006, p.1.

by 2010.[4677] However, if a large volume of weapons are used concurrently in a conflict, this may add considerably to the demand for network bandwidth.

Bandwidth Limitations

Bandwidth is the transmission capacity for any given channel on a network. Since 1991, there has been an explosive increase in military demand for bandwidth, largely due to efforts to speed up the delivery of digital information. Defense officials remain concerned about whether the bandwidth available through DOD communications systems will grow to keep up with increasing military demand in the future. Some observers question whether enough bandwidth will be available in the future to support DOD plans for major NCO systems, such as the Future Combat System, Warfare Information Network - Tactical, and Joint Tactical Radio System.[4678]

When the supply of bandwidth becomes inadequate during combat, military operations officers have sometimes been forced to subjectively prioritize the transmission of messages. They do this by literally pulling the plug temporarily on some radio or computer switching equipment in order to free up enough bandwidth to allow the highest-priority messages to get through. This can delay messages, or cancel other data transmissions. Latency, or delays in information updates resulting from a bandwidth shortage could leave some units attempting to fight on their computer screens with outdated information, when the enemy changes position faster than the screen image data can be updated. An example of this type of problem occurred in April 2003, when a U.S. Army battalion was surprised by a large force of Iraqi tanks and troops because intelligence systems were unable to update enemy information in databases quickly enough to keep front line units accurately informed.[4679]

By the year 2010, the Congressional Budget Office estimates that the supply of effective bandwidth in the Army is expected to fall short of peak demand by a ratio of approximately 1 to 10.[4680] According to former Assistant Secretary of

---

[4677] Rich Tittle, Promise of Networked Weapons is Shown in Eglin Demos, NetDefense, January 19, 2006, [http://www.aviationnow.com/avnow/news/channel_netdefense_story.jsp?view=story&od=news/EGLIN01196.xml].

[4678] Scott Nance, Krepinevich: FCS Revolutionary But Irrelevant?, Defense Today, March 31, 2005, p.3.

[4679] Greg Grant, "Net-Centric Warfare Experts Look to Improve Communications", C4ISR The Journal of Net-Centric Warfare , October 11, 2005, [http://www.isrjournal.com/story.php?F=1166143}.

[4680] Anticipated hardware improvements by 2010 will shift the existing bandwidth bottleneck from the brigade level to the corps level. If the Joint Tactical Radio System (JTRS) performs as the Army projects, the new radio may provide more than enough bandwidth for the lower tactical

Defense for Networks and Information Integration (ASD/NII), Paul Stenbit, the primary barrier to achieving the NCO Internet paradigm is finding new ways to meet the demand for bandwidth. Communications infrastructure must have enough bandwidth to allow, for example, several people at different locations in the battlefield to pull the same problem-solving data into their computer systems at the same time, without having to take turns sharing and using the same limited local bandwidth.[4681]

Unmanned Robotic Vehicles (UVs)

UVs, also known as Unmanned Aerial Vehicles (UAVs), Ground Vehicles (UGVs), and Underwater Vehicles (UUVs) are primarily used for surveillance. However, their mission is evolving to also include combat, under the title Unmanned Combat Vehicles (UCVs).[4682] During OIF, approximately 16 Predator and 1 Global Hawk UAVs were in operation, and all were controllable remotely via satellite link from command centers in the continental United States. UVs each require a large amount of bandwidth for control and for transmission of reconnaissance images.[4683]

Sensor Technology

Sensors are being developed to remotely detect movement and heat signatures of enemy equipment. However, some observers have warned that it is likely that future foes will develop technologies to counter U.S. weapons, and will become more sophisticated in cover and concealment, with the possible net effect that

---

levels of command, with a margin for growth of demand beyond 2010. However, at the division and corps level, the projected demand is still expected to be much greater than the likely supply. U.S. Congressional Budget Office, "The Army's Bandwidth Bottleneck," Aug. 2003, [http://www.cbo.gov].

[4681] In certain situations, some commanders had access to only one communications channel. If someone else was using it first, the commander had to wait until it was free for him to use. Matthew French, "Bandwidth in Iraq a subject of debate," Federal Computer Week, Oct. 20, 2003, p.43.

[4682] The two key programs for UAV development are the USAF's X-45 and the Navy's carrier-capable X-47. Both projects are under the Joint Unmanned Combat Air System (JUCAS) program, which is led by DARPA. DOD believes that merging these two projects will lead to greater efficiencies and reduced acquisition costs. Adam Herbert, "New Horizons for Combat UAVs," Air Force Magazine, Dec. 2003.

[4683] For more information about UVs, see CRS Report RS21294, Unmanned Vehicles for U.S. Naval Forces: Background and Issues for Congress.

U.S. situational awareness on the battlefield could decrease, depending upon the sophistication of the adversary.[4684]

Software Design

Software is an important component of all complex defense systems used for NCO. GAO has recommended that DOD follow best practices of private sector software developers to avoid the schedule delays and cost overruns that have plagued past DOD programs dependent on development of complicated software.[4685] Many observers of the software industry believe that globalization of the economy dictates a global process for software development. In keeping with the GAO recommendation, contractors for DOD often outsource software development to smaller private firms, and in some cases, programming work is done by offshore companies. This raises questions about the possibility of malicious computer code being inserted to subvert DOD computer systems. However, DOD is currently investigating ways to increase confidence in the security of both foreign and domestic software products, for example, by co-sponsoring with the Department of Homeland Security a series of software assurance forums where government, industry, and academic leaders discuss security methodologies that promote integrity and reliability in software.[4686]

Computer Semiconductors and Moore's Law

Gordon Moore's Law of Integrated Microprocessor Circuits observes that computer semiconductor chips follow an 18-month cycle of evolution where they will become twice as dense and twice as fast for about the same cost. Commercial industries have long relied on the predictability of Moore's Law as a guide for investing in future technology systems. DOD plans for NCO also rely on the predictable growth in computer processing power, but this predictability may be affected by advances in new technologies. New technology developments could be disruptive, for example by reducing circuit size to nanometer units giving rise to extreme miniaturization, or by quickly lowering costs and giving adversaries and

---

[4684] Greg Grant, "Net-Centric Warfare Experts Look to Improve Communications", C4ISR The Journal of Net-Centric Warfare, October 11, 2005, [http://www.isrjournal.com/story.php?F=116143].

[4685] U.S. General Accounting Office, "DEFENSE ACQUISITIONS: Stronger Management Practices Are Needed to Improve DOD's Software-Intensive Weapon Acquisitions," GAO-04-393, Mar. 2004.

[4686] It is virtually impossible to find unauthorized and malevolent code hidden deep within a sophisticated computer program module that may have originated from a company in one of more than a half-dozen countries commonly used for software outsourcing. Mark Willoughby, "Hidden Malware in offshore products raises concerns," Computerworld, September 15, 2003, [http://www.computerworld.com].

terrorist groups easier access to more sophisticated and powerful commercial high-technology equipment.[4687]

Technology Transfer Threat to U.S. Net Centric Advantages

Electronic technologies are critical to the operation of modern, complex systems for communications and weaponry, and much of the technology for U.S. military data networking reportedly comes from Commercial-Off-The-Shelf (COTS) products.[4688] Much of this same state-of-the-art COTS technology is readily available on the open market, and is also available to our adversaries. Some officials in DOD also say that off-shore outsourcing of critical design and manufacturing capabilities, along with other factors, has contributed to the erosion of the U.S. lead in key defense technologies.[4689] These DOD officials warn that the United States may some day no longer have the asymmetric technology advantage it once had over our existing and potential adversaries.[4690]

Weak Export Controls for High Technology

The Defense Science Board has reported that the 1996 voluntary Wassenaar Arrangement, which replaced the Cold War-era international regime that governed semiconductor exports, is not an effective tool for assuring that potential adversaries do not have access to technology for leading-edge design and fabrication equipment for integrated circuits.[4691] In addition, non-allied foreign acquisition of any U.S. company that manufactures or develops items of

---

[4687] Today's electronic transistors are reaching physical limits where electrical circuits can leak across microscopic insulators, and the manufacturing process is increasingly expensive. Photonic computers will use photons of laser light instead of electrons, will be thousands of times faster than electronic computers, and far less expensive to manufacture. However, the effort to produce the necessary inexpensive nonlinear crystals that switch light beams quickly, and at reasonable power levels, has so far not been successful enough for commercial application. The CoolScience Center, [http://www.rmrc.org/photonics/photon1.htm].

[4688] Ted McKenna, US Military Slow to Adapt to Net-Centric Warfare, Journal of Electronic Defense, August 2005, No 8, p.24.

[4689] In 2003, of the 2,027 doctorates awarded by U.S. universities for electrical engineering and computer science, 63 percent were earned by foreign nationals. Of the 15,906 master's degrees awarded in these same fields, 56% were earned by non-U.S. residents. Eric Chabrow and Marianne McGee, "Immigration and Innovation," Information Week, Feb. 23, 2004, p. 20.

[4690] OSD Memorandum accompanying the March 2006 Joint Report from the U.S. Defense Science Board, U.K. Defence Scientific Advisory Council Task Force on Defense Critical Technologies.

[4691] Defense Science Board Task Force on High Performance Microchip Supply, U.S. Department of Defense, February 2005. [http://www.acq.osd.mil/dsb/reports/2005-02-HPMS_Report_Final.pdf].

defense significance can erode the security of the defense industrial base. China, in particular, has reportedly procured advanced weapons and technology from abroad to make up for deficiencies in its domestic military sector. In doing so, China has reportedly developed an active policy of acquiring foreign industrial and manufacturing production lines, and then seeking U.S. export licenses for advanced semiconductor fabrication instruments and equipment.[4692]

Microchip Manufacturing Moves Offshore

The Defense Science Board has also identified the increasing shift of U.S. semiconductor fabrication and design technology offshore as a critical national security challenge. Past supplies of classified integrated circuits have come from government-owned facilities operated by the National Security Agency (NSA) and Sandia National Laboratory. However, technological evolution, and new methods for mass production, have reportedly raised the cost of low-production-volume custom integrated circuits used by DOD, and made government facilities obsolete. As a result, there is no longer a diverse base of U.S. integrated circuit fabricators capable of meeting DOD needs.[4693] The DSB report calls for DOD and the defense industry to develop a new economic model for profitably producing a limited number of custom circuits and equipment for U.S. military systems.

Increased Offshore Outsourcing of R&D

U.S. corporations are now sending more high-level research and development (R&D) work to off-shore partners. For example, as early as 1998, Intel Corporation, Microsoft Corporation, and other IT vendors opened new R&D facilities in Beijing and other parts of Asia. Microsoft also reportedly has 200 Ph.D. candidates and 170 researchers currently working in its Asia R&D facilities.[4694] The Gartner Group research firm has reported that corporate spending for offshore information technology (IT) services will increase from $1.8 billion in 2003 to more than $26 billion in 2007, with half of the work going to Asian countries such as India and China.[4695]

[4692] John Tkacik, China's Military Power, testimony before the House Committee on Armed Services, July 27, 2005, p.7.

[4693] Defense Science Board Task Force on High Performance Microchip Supply, U.S. Department of Defense, February 2005. [http://www.acq.osd.mil/ dsb/reports/2005-02-HPMS_Report_Final.pdf].

[4694] Patrick Theobald and Sumner Lemon, "R&D Starts to Move Offshore," Computerworld, vol. 38, no. 9, Mar. 1, 2004, p. 1.

[4695] Paul McDougall, "Optimizing Through Outsourcing," Information Week, Mar. 1, 2004, p.56. For more information, see CRS Report RL30392: Defense Outsourcing: The OMB Circular A-76 Policy.

Contracting for national defense is reportedly among the most heavily outsourced of activities in the federal government, with the ratio of private sector jobs to civil service jobs within DOD nearly five to one.[4696] However, a 2004 study by DOD concluded that utilizing foreign companies as sources for high-technology equipment does not affect long-term military readiness.[4697]

Operational Experiences

Operation Iraqi Freedom (OIF) might be more accurately characterized as a transitional rather than transformational operation because NCO technology was not fully deployed in all units during OIF, and some systems proved not to be userfriendly.[4698] Nevertheless, some observers feel that OIF proved the effectiveness and potential of network enhanced warfare,[4699] while others believe that it is hard to interpret the NCO experiences objectively, partly because the review process may sometimes be distorted by the internal military bias that favors force transformation. Still others point out that experiences using NCO technology may be misleading because recent U.S. adversaries were relatively weak militaries, including Panama (1990), Iraq (1991), Serbia (1999), and Afghanistan (2001).[4700]

A March 2005 report from the U.S. Army War College asserts that network-enabled operations achieved proof of concept in the major combat operations phase of Operation Iraqi Freedom. The report further states that net centric operations enhanced the ability of U.S. forces to conduct battles and campaigns

---

[4696] Ann Markusen, Director, Project on Regional Industrial Economics, University of Minnesota, "Statement Made to David Walker, Chairman Commercial Activities Panel, GAO, June 5, 2001 and Pender M McCarter, "500,000 U.S. IT Jobs Predicted to Move Overseas by Year-end 2004; IEEE Sees Continued Loss in U.S. Economic Competitiveness, National Security," IEEE-USA News, July 21, 2003, [http://www.ieeeusa.org/releases /2003/072103pr.html].

[4697] U.S. Department of Defense, Office of the Deputy Undersecretary of Defense for Industrial Policy, Study on Impact of Foreign Sourcing of Systems, Jan. 2004.

[4698] Some argue that OIF experiences validate Admiral Cebrowski's view that technology is not NCW, but rather only the enabler of NCW. Loren B. Thompson, CO Lexington Institute, ISR: Lessons of Iraq, Defense News ISR Integration Conference, Nov. 18, 2003. See also CRS Report RL31946: Iraq War: Defense Program Implications for Congress, by Ronald O'Rourke.

[4699] Lt. General William Wallace, Commander Combined Arms Center, in U.S. Congress, House Armed Services Subcommittee on Terrorism, Unconventional Threats and Capabilities, Hearing on Military C4I Systems, Oct. 21, 2003, [http://www.cq.com].

[4700] Some traditional virtues such as air superiority, may be under emphasized. The review process may exaggerate the role of "jointness" and special operations, according to Loren B. Thompson, Analyst at the Lexington Institute, "ISR: Lessons of Iraq, Defense News ISR Integration Conference," Nov. 18, 2003. "The Iraqis made so many mistakes it would be foolish to conclude that defeating them proved the viability of the new strategy," Dan Caterinicia and Matthew French, "Network-Centric Warfare: Not There Yet," Federal Computing Week, June 9, 2003, [http://www.fcw.com/fcw/articles/2003/0609/ cov-netcentric-06-09-03.asp].

by providing a common operating picture and situational awareness never before experienced in combat.[4701] A case study by the Office of Force Transformation concluded that the deployment of some net centric technologies during OIF improved operational effectiveness specifically for planning, command and control agility, tempo, and synchronization.[4702]

Network Communications

Increased networking during OIF reportedly allowed U.S. forces to develop a much improved capability for coordinating quick targeting. In Operation Desert Storm in 1991, coordinating efforts for targeting required an elapsed time of as much as four days. In Operation Iraqi Freedom, U.S. forces reduced that time to about 45 minutes.[4703] During April 2003, the Marine Corps Systems Command compiled comments from some soldiers about their experiences using several new communications systems during combat operations in Iraq. Comments from soldiers and other observers follow:

(1) Several communicators, operations officers, and commanders reportedly stated that they felt generally overloaded with information, and sometimes much of that information had little bearing on their missions. They stated that they received messages and images over too many different networks, requiring them to operate a large number of different models of communications equipment.[4704]
(2) Some troops stated that when on the move, or when challenged by line-of-sight constraints, they often used military email and "chat room"[4705] messages for communications (This usually required linking to a satellite).

Sensors

(1) Force XXI Battle Command, Brigade and Below (FBCB2), with Blue Force Tracker, received widespread praise from troops for helping to reduce the

---

[4701] Dennis Murphy, Network Enabled Operations in Operation Iraqi Freedom: Initial Impressions , CSL Issue Paper, March 2005, Vol. 06-05, [http://www.oft.osd.mil/initiatives/ncw/docs/csl_issue_paper_0605.pdf].

[4702] Office of Force Transformation, US/UK Coalition Combat Operations during Operation Iraqi Freedom, March 2, 2005, [http://www.oft.osd.mil/library/library_files/document_389_Final_Cleared_US_UK_Coalition_Combat_Ops_in_OIF.pdf]. Other NCO case studies can be found at [http://www.oft.osd.mil/initiatives/ncw/studies.cfm].

[4703] Dan Caterinicia and Matthew French, "Network-Centric Warfare: Not There Yet," Federal Computing Week, June 9, 2003, [http://www.fcs/com].

[4704] Matthew French, "Technology a Dependable Ally in Iraq War," Federal Computer Week, vol. 18, no.8, Mar. 29, 2004, p. 46.

[4705] John Breeden, "Bantu Sails with the Navy," Government Computer News, May 26, 2003, p. 1.

problem of fratricide. Blue Force Tracker (BFT) is a generic term for a portable computer unit carried by personnel, vehicles, or aircraft that determines its own location via the Global Positioning System, then continuously transmits that data by satellite communications. The position of each individual unit then appears as a blue icon on the display of all other Blue Force Tracker terminals, which were used by commanders on the battlefield, or viewed at remote command centers. Clicking on any blue icon would show its individual direction and speed. A double-click reportedly would enable transmission of a text message directly to that individual unit, via satellite.

(2) Objective Peach involved U.S. forces defending a captured bridge from Iraqi forces on the morning of April 3, 2003. The commander of the U.S. forces reportedly complained that he received no information from sensors to provide warning when his position was attacked by 5,000 Iraqi soldiers approaching under cover of night, backed up by 25 tanks and 70 armored personnel carriers. Subsequent investigation revealed that at division level and above, the sensor information was adequate, but among front-line Army commanders, there was inadequate support to aid situational awareness on the ground.[4706]

(3) During a blinding sandstorm lasting from March 25 to 28, 2003, a U.S. radar plane detected Iraqi forces maneuvering near U.S. troops. U.S. bombers attacked the enemy units using satellite-guided bombs that were unaffected by poor visibility. The Blue Force Tracker system ensured that friendly forces were identified and not harmed during the successful bombing attack.[4707]

Satellites

Satellite communications played a crucial role for transmitting message and imagery data during OIF operations, and also enabled U.S. forces in the field to "reach back" to the continental United States for support. However, a growing dependence on space communications may also become a critical vulnerability for NCO.

(1) Commercial satellites were used to supplement military communications, which lacked capacity despite the fact that a number of military satellites were moved to a better geostationary orbital position for both Afghanistan and Iraq.[4708] DOD satellites cannot satisfy the entire military demand for

---

[4706] David Talbot, "How Technology Failed in Iraq", MIT Technology Review, November 2004, [http://www.technologyreview.com/articles/04/11/talbot1104.asp].

[4707] Ibid.

[4708] Brigadier General Dennis Moran, U.S. Central Command/ J6, in U.S. Congress, House Armed Services Subcommittee on Terrorism, Unconventional Threats and Capabilities, Hearing on Military C4I Systems, Oct. 21, 2003, [http://www.cq.com].

satellite bandwidth, and therefore DOD has become the single largest customer for commercial or civilian satellite services. DOD sometimes leases commercial satellite bandwidth through DISA, and at other times bypasses the process to buy directly from industry. However, bypassing DISA may reduce interoperability between the services, and may increase redundancies.

(2) During the OIF conflict, communications trunk lines, including satellite transmissions, were often "saturated", with all available digital bandwidth used up. The peak rate of bandwidth consumed during OIF was approximately 3 Gigabits-per-second, which is about 30 times the peak rate consumed during Operation Desert Storm in 1991.[4709]

Bandwidth and Latency

Some problems with delayed arrival of messages during OIF may have occurred due to unresolved questions about managing and allocating bandwidth. Sometimes, when demand for bandwidth was high, NCO messages with lower priority were reportedly dropped deliberately so that other messages with a higher priority could be transmitted.[4710]

(1) The speed with which U.S. forces moved, a shortage of satellite communications, and the inability to string fiber nationwide hampered efforts to provide adequate bandwidth. At times, some commanders were required to share a single communications channel, forcing them to wait to use it whenever it became free.[4711]

(2) Brigade-level command posts could view satellite and detailed UAV images, but battalion-level commanders, and lower command levels, could not view those same images. The lower-level commands are where greater detail is critical.

(3) Although the Army has invested in military-only decision-support systems, some of the planning and collective decision-making during OIF was handled through email and chat-rooms that soldiers were familiar with, that were "user-friendly" and reliable, that were available when

---

[4709] Jefferson Morris, "GAO: DOD Needs New Approach to Buying Bandwidth," Aerospace Daily, Dec. 12, 2003 and "DISA Chief Outlines Wartime Successes," Federal Computer Week, June 6, 2003,

[4710] U.S. Congressional Budget Office, The Army's Bandwidth Bottleneck, Aug. 2003, [http://www.cbo.gov], and Lt. General William Wallace, Commander Combined Arms Center, in U.S. Congress, House Armed Services Subcommittee on Terrorism, Unconventional Threats and Capabilities, Hearing on Military C4I Systems, Oct. 21, 2003, [http://www.cq.com].

[4711] Matthew French, "Bandwidth in Iraq a Subject of Debate," Federal Computer Week, Oct. 20, 2003, [http://www.fcw.com/fcw/articles/2003/1020/tec-iraq-10-20-03.asp].

other systems experienced transmission delays, and that required little or no training.[4712]

Air Dominance

UAVs sometimes carry thermal cameras that can see through darkness or rain. These reportedly gave military planners so much confidence when orchestrating raids, they often skipped the usual time-consuming rehearsals and contingency planning.[4713] However, without early air dominance, UAVs and other Intelligence Surveillance and Reconnaissance (ISR) aircraft could not have been used to provide information needed for NCO systems. UAVs, and other support aircraft, such as refueling support tankers, are nearly defenseless and reportedly cannot operate without early air dominance.

Operations in Iraq with Coalition Forces

Using NCO technology with coalition forces resulted in reduced fratricide during OIF. However, during OIF, coalition assets reportedly operated as separate entities, and were often locked out of

U.S. planning and execution because most information was posted on systems accessible only to U.S. forces. For example, most major air missions, that used NCO technology for coalition operations, involved only U.S. aircraft.[4714] Policy for sharing of classified information requires a separate contract agreement between the United States and each coalition partner. DOD currently maintains 84 separate secure networks for NCO coalition operations: one for each coalition partner. This is because U.S. National Disclosure Policy restricts what information may be released to coalition partners.[4715] In addition, each coalition partner nation has a corresponding policy for release of its own sensitive information. As a result of these policies, operations planning information was distributed to coalition forces using a manual process, and the transfer of data fell

---

[4712] U.S. Congressional Budget Office, "The Army's Bandwidth Bottleneck," Aug. 2003, [http://www.cbo.gov].

[4713] "In Iraq, Soldiers Wage War Via Computer," Baltimore Sun/A.P., Jan. 4, 2004.

[4714] Lt. General Daniel Leaf, Vice Commander for U.S. Air Force Space Command, in U.S. Congress, House Armed Services Subcommittee on Terrorism, Unconventional Threats and Capabilities, Hearing on Military C4I Systems, Oct. 21, 2003,[http://www.cq.com].

[4715] Each coalition partner must agree to protect classified military information that the United States shares with them. DOD Directive 5230.11, June 16, 1992, implements the Oct. 1, 1988 "National Policy and Procedures for the Disclosure of Classified Military Information to Foreign governments and International Organizations," or the National Disclosure Policy, within the Department of Defense, [http://www.dtic.mil/whs/directives/corres/pdf/d523011_061692/d523011p.pdf].

behind combat operations.[4716] A secure single network is required to efficiently share information among multiple partners, with a capability to dynamically add and subtract coalition partners. DOD has initiated a program called "Network Centric Enterprise Services" (NCES, also known as "Horizontal Fusion") to make information immediately available to coalition partners, while also providing strong security through network encryption technologies and dynamic access controls.[4717] However, this technical solution may not affect the differences in the individual policies that restrict information sharing among coalition partners.

Network Capabilities of Other Nation States

Military operations today generally are generally conducted with coalition partners. A coalition member that is unable to efficiently communicate situational information and other data electronically exert an unacceptable drag on the collective operations of all coalition members. Therefore, militaries of some other countries have developed Network Enabled Capability (NEC) technologies similar to those used by joint U.S. forces.[4718]

NEC is the European equivalent of NCO, and is at the heart of defence transformation ongoing in militaries throughout Europe. NEC is defined as the coherent integration of sensors, decision-makers and weapon systems along with support capabilities to create superior decision-making. This will enable military forces to operate more effectively in the future strategic environment through the more efficient sharing and exploitation of information.[4719]

Some countries also view NEC as a way to reduce their military budgets by gaining efficiency through networking with coalition partners.[4720] Observers note

---

[4716] Meagan Scully, "Out of Touch: Policies, Technology Hindered Data-Sharing with Allies in Iraq," ISR Journal, vol. 3, no. 4, May 2004, p. 32.

[4717] Cheryl Roby, Deputy Secretary of Defense, OASD, NII, Information Sharing Challenges in Coalition Operations, presentation at the 4th Annual Multinational C4I Conference, McLean, Virginia, May 4, 2004 and Matthew French, "DOD Blazes Trail for Net-centric Strategy," FCW.com, June 9, 2003, [http://www.fcw.com/fcw/articles/2003/0609/ news-dod-06-09-03.asp].

[4718] The military organizations of Denmark, Norway and the Netherlands have also adopted the term Network Centric Warfare. Australia uses the term Network-Enabled Warfare, while the U.K. uses the term Network-Enabled Capability, and the Republic of Singapore uses the term Knowledge-Based Command and Control. John Garstka, "Network-Centric Warfare Offers Warfighting Advantage," Signal Forum, Signal Magazine, May 2003.

[4719] From the Network Enabled Capabilities Conference, December 2006, Brussels, Belgium, [http://www.marcusevans.com/events/cfeventinfo.asp?eventID=10885].

[4720] Frederick Stein, Senior Engineer, MITRE Corporation, Presentation on Network Centric Warfare Operations, 4th Annual Multinational C4ISR Conference, McLean, Virginia, May 6, 2004.

that European and other coalition partners now deploying NEC equipment are still not yet interoperable with NCO equipment operated by the U.S. military.[4721]

NATO

NATO is currently building a NEC capability for dynamic interoperability with U.S. forces in the future and is developing a framework for high-technology warfare using the combined forces of multiple nations. Called the NATO Network Enabled Capabilities (NNEC), it is similar to the U.S. military's Joint Vision 2020.[4722]

The confidential NATO 2005 Defense Requirements Review reportedly describes newer capabilities needed by allied commanders, including a description of technologies for sensors for sharing intelligence among allied warfighters.[4723] However, problems have been encountered with the U.S. National Disclosure Policy, which restricts release of classified information, and with the International Traffic in Arms rules which govern the export of unclassified technical data, and affect technology transfer (see previous section titled, Technology Transfer Threat to U.S. Net Centric Advantages).[4724]

Initially, the DOD Office of Force Transformation constructed a conceptual model to study net centric operations. However, NATO has since developed another conceptual model to test newer network centric approaches to military command and control (C2).[4725] To resolve differences, and establish open, interoperable standards for NEC and NCO, a new Network Centric Operations Industry Consortium has been created. The consortium consists of about 80 defense and information technology companies, of which 19 are European.[4726]

[4721] Brooks Tigner, Fixing a Disconnect: EU Tries to Assess Compatibility Problems, Defense News, October 31, 2005, p.11.

[4722] "NATO Network Enabled Capability (NNEC)," Times staff, Mar. 3, 2003, "NATO Starts 'Transformation' Process," NavyTimes.com, Feb. 5, 2004, [http://www.navytimes.com/].

[4723] Sebastian Sprenger, NATO to Unveil Plan for Wartime Information Sharing by Next Summer, Inside the Pentagon, December, 2005.

[4724] Rati Bisnoi, Report: Net-Centric Warfare Training Needed for NATO Response Force, Inside the Pentagon, Nov. 3, 2005.

[4725] David Alberts and Richard Hayes, Understanding Command and Control, The Future of Command and Control, CCRP Publication 2006, P.200, [http://www.dodccrp.org/publications/pdf/Alberts_UC2.pdf].

[4726] Brooks Tigner, Standards Urged To Smooth Allied Network-Centric Ops, Defense News, Jan. 2, 2006, p.10.

Australia

The Australian Defense Force is developing innovative networked sensor technologies, and testing autonomous unmanned vehicles to offset the small size of their military. They are testing network communications that will allow one operator to control a formation of unmanned aerial vehicles that can be programmed to peel off independently for surveillance, or to launch an attack.[4727]

France

The French reportedly are implementing a concept called "Guerre Infocentre", or Infocentric Warfare, which emphasizes the importance of information flows rather than the network itself. The initial program is called the Future Air Land Combat Network System, which will enable different combat platforms to contribute to cooperative engagement of targets.[4728]

Germany

Plans call for development of a future soldier system for the German Army, called "Infanterist der Zuknft", which will introduce new ways of networking between combat units and higher command levels. The system includes optical components, soldier-level computing equipment, and a tactical military internet which links voice and data systems.[4729]

United Kingdom

The UK is reportedly building its own Global Information Infrastructure, which is a single, general purpose network, with a specialized security architecture and a family of joint command battlespace management applications.[4730] The UK system design will expand to allow multinational forces, such as the United State, Canada, Australia, and New Zealand to also reach through each others' protective electronic boundaries to share a common operating picture through Voice Over IP and video teleconferencing.[4731]

[4727] David Fulghum, Cyber-Hammer, Aviation Week and Space Technology, May 29, 2006, p.48.

[4728] Giles Ebbutt, Flaws in the System: Modern Operations Test the Theory of Network Centricity, Jane's International Defence Review, July 2006, p.61.

[4729] Staff, "German Soldier Networking System Evolves", International Defense Digest, Jane's International Defense Review, July 2006, p.10.

[4730] Giles Ebbutt, Flaws in the System: Modern Operations Test the Theory of Network Centricity, Jane's International Defence Review, July 2006, p.57.

[4731] Giles Ebbutt, Flaws in the System: Modern Operations Test the Theory of Network Centricity, Jane's International Defence Review, July 2006, p.61.

Israel

During the brief 2006 conflict with Syrian- and Iranian-supported Hizballah, Israel reportedly combined tactical unmanned aerial vehicles with their new Tzayad digitized command-and-control systems to locate and destroy many of Hizballah's rocket launchers. Experts reported that Israeli brigades that were equipped with the latest digital equipment were able to apply firepower in a very effective manner.[4732]

China

China reportedly has considerable and growing capabilities for developing information technology and networks. Chinese officials have reportedly noted that future military plans call for China to focus on developing new-concept weapons, such as electromagnetic pulse (EMP) systems for jamming adversary networks, and new satellites for establishing a unique GPS network for the Chinese military.[4733] China has also reportedly networked its forces using the European "Galileo" space-based global positioning system[4734]

Recent publications from China on security and national defense policy use terms such as "informationalization" and "Integrated Network-Electronic Warfare" (INEW), while describing how warfare is becoming more information oriented. Chinese military officials have stated that the INEW concept is comparable to U.S. Net Centric Operations. However, while INEW involves acquiring both defensive and offensive information operations capabilities, there is a priority placed on developing active strategies for offensive information operations.[4735]

DOD officials acknowledge that China has been conducting research to develop ground-based laser anti-satellite weapons. Some officials claim that China in recent years may have tested the means to harm or destroy U.S. satellites. However, a recent statement byDOD did not confirm or denythis possibility. The

---

[4732] Babara Opall-Rome, Israel Wants More Active Defenses, Better Intel, DefenseNews, Aug. 14, 2006, p.8.

[4733] Mary Fitzgerald, China plans to control space and win the coming information war, Armed Forces Journal, November 2005, p.40.

[4734] David Gompert, Irving Lachow, and Justin Perkins, "Battle-Wise: Gaining Advantage in Networked Warfare", Center for Technology and National Security Policy, National Defense University, January 2005, p.13.

[4735] Timothy Thomas, Chinese and American Network Warfare, Joint Forces Quarterly, Issue 38, #rd Quarter 2005, p.76.

United States military relies on commercial satellites for up to 80 percent of DOD space-based communications, according to space officials.[4736]

DOD officials also report that hacker attacks directed against U.S. military networks increased approximately fiftypercent between 2003 and 2004. Officials also state that most of these computer intrusions were originating from within China, with one extended attack involving the theft of perhaps 10 to 20 terabytes of data from the DOD Non-Classified IP Router Network. These attacks may indicate that China, and perhaps other countries, are developing or testing skills to defeat U.S. Network Centric Operations.[4737]

Network Capabilities of Extremist Groups

Other non-state groups also watch as the United States and other countries network their forces. In many cases, these groups are able to bypass much of the R&D associated with creating and testing new networked services, and instead are able to purchase Commercial-Off-Shelf (COTS) products and equipment adequate for their purposes. These sophisticated commercial technologies may enable smaller countries, or Al Qaeda or Hamas, to project an advanced and adaptive electronic warfare threat.[4738]

Attacks by Unknown Foreign and Domestic Adversaries

In 2003 the U.S. government launched an investigation code named "Titan Rain" after detecting a series of persistent intelligence-gathering cyberattacks directed at military computer systems. The attackers demonstrated a high level of sophistication, and the investigation led many security experts to believe that the computer intrusions originated from sources in China. The targeted systems included (1) the U.S. Army Information Systems Engineering Command at Fort Huachuca, Arizona, (2) the Defense Information Systems Agency in Arlington, Virginia, (3) the Naval Ocean Systems Center in San Diego, California, (4) the U.S. Army Space and Strategic Defense installation in Huntsville, Alabama, and many other installations. In 2004, the Army base at Fort Campbell, Kentucky initiated a multimillion-dollar program to secure its computer systems after its networks were penetrated for a period of approximately two months, during a

---

[4736] Elain Grossman, Top Commander: Chinese Interference with U.S. Satellites Uncertain, Inside the Pentagon, October 12, 2006.

[4737] Peter Brookes, The Art of Cyber War, The Conservative Voice, August 29, 2005, [http://www.theconservativevoice.com/articles/article.html?id=7860].

[4738] J.R. Wilson, High-Tech Challenge: Terrorists present Electronic Warfare Threat, Too, Armed Forces Journal, February 5, 2005, pp.38-39.

sustained intelligence-gathering cyberattack.[4739] Although these attacks persisted over a long period of time, the U.S. government claims that no classified information was compromised.[4740]

Recently, China was also blamed for cyber intrusions that disabled the computer networks of the Department of Commerce Bureau of Industry and Security, which is responsible for controlling U.S. exports of software and technology for both commercial and military use. The attacks were traced to websites registered with Chinese Internet service providers.[4741]

However, other analysts caution that a sophisticated opponent, such as China, would not leave clues pointing back to itself. Instead, another sophisticated opponent could use China as a platform for third party computer attacks. China's civilian computer networks are very vulnerable to viruses. Some estimates reportedly say that up to 90% of the software used in China is pirated, lacking in the most important security patches, and especially vulnerable to being taken over by malicious code. Therefore, any attack that can be traced back to China may actually demonstrate very little about the true source. Sophisticated hacking tools are widely available on the Internet, and some hackers advertise their cybercrime skills for hire to other organizations, which could include extremists, both domestic and international.[4742]

Hizballah

After the 34-day war with Israel in 2006, Hizballah was described by some Israeli officials as a well-equipped, networked force still capable of commanding its combat units after weeks of high-intensity fighting. Hizballah's units were supported by a well-fortified terrestrial communications network supplemented by satellite telephone and broadcast services, including the Al-Manar television

---

[4739] Frank Tiboni, Army Rebuilds Networks after Hack Attack, Federal Computer Week, September 6, 2004, [http://www.fcw.com].

[4740] Tom Espiner, Security Experts Lift Lid on Chinese Hack Attacks, ZDNet, November 23, 2005, [http://www.zdnet.co.uk/print/?type=story&at=39237492-39020375t-10000025c]. Nathan Thronburgh, The Invasion of the Chinese Cyberspies (And the Man Who Tried to Stop Them), Time, August 29, 2005, [http://www.time.com/time/magazine/printout/0,8816,1098961,00.html].

[4741] Alan Sipress, Computer System Under Attack, Washington Post. October 6, 2006, A21.

[4742] James Lewis, Computer Espionage, Titan Rain and China, Center for Strategic and International Studies, December 14, 2005, [http://www.csis.org/index.php?option=com_csis_pubs&task=view&id=2576].

network. Hizballah units also reportedly had the capability to attempt eavesdropping on Israeli cellular networks.[4743]

Hamas

Hamas was reportedly inspired by the way Hizballah fought against Israel in Lebanon, and the organization continues to receive increasing support from both Iran and Hizballah in the form of weapons, funding, and training. Hizballah is also reportedly sharing with Hamas operatives many of the lessons they learned from the recent military engagement with Israel.[4744]

Al Qaeda

Al Qaeda networks, in addition to technology, often rely on dispersed cells of people that are under central direction, which allows the organization to be highly flexible, elusive, and adaptable. As Al Qaeda evolves to using newer commercially available communication systems, dispersed cells may become more coordinated and self-organizing, with increased situational awareness, with the possible future capability of conducting their own network operations, in ways similar to the network operations of current U.S. military units.[4745]

Key Military Programs

The following are key DOD programs related to NCO.

Global Information Grid (GIG)

The GIG is the communications infrastructure that supports DOD and related intelligence community missions and functions, and enables sharing of information between all military bases, mobile platforms, and deployed sites. The GIG also provides communications interfaces to coalition, allied, and non-DOD users and systems. Key service network architectures for implementing an important NCO capability through the GIG are the Air Force C2 Constellation, Navy and Marine Corps ForceNet, and Army LandWarNet.[4746] The Joint Task

---

[4743] Barbara Opall-Rome, Combating the Hizballah Network, Defense News, Oct. 9, 2006, p.6.

[4744] Alon Ben-David, Hamas Boosts its Weapons Stocks, Janes Defence Weekly, October 25, 2006, [http://www4.janes.com/subscribe/jdw/doc_view.jsp?K2DocKey=/content1/janesdata/mags/jdw/history/jdw2006/jdw30827.htm@current&Prod_Name=JDW&QueryText=].

[4745] David Compert et. al, Battle-Wise: Gaining Advantage in Networked Warfare, Center for Technology and National Security Policy, National Defense University, January 2005, p.15.

[4746] For more information about the GIG, see CRS Report RS21590, Defense Program Issue: Global Information Grid, Bandwidth Expansion (GIG-BE).

Force Global Network Operations is tasked with operation and defense of the GIG.

DOD is planning that 2008 military communications equipment will use the new Internet Protocol version 6 (IPv6) as the standard for all transmission through the Global Information Grid (GIG), and for all Defense Information System Network systems that will interoperate with the GIG.[4747] The new IPv6 protocol offers greater message security and better tracking of equipment, supplies, and personnel through use of digital tags (See Appendix A, The Transition from Internet Protocol Version 4 (IPv4) to IPv6).

It is noteworthy that in a 2006 study, the Government Accountability Office found that the GIG lacks clearly defined leadership able to cut across organizational lines. GAO warned that without adequate leadership the GIG program could exceed cost and schedule requirements, partly due to development and acquisition methods characterized as "stovepiped" and "uncoordinated". [4748]

Air Force Advanced Tactical Targeting Technology (AT3)

The AT3 system combines information collected by an airborne network of sensors to identify the precise location of enemy air defense systems. The system relies on coordination of information from different systems aboard multiple aircraft.[4749]

Air Force Link 16

Tactical Data Links (TDLs) are used in combat for machine-to-machine exchange of information messages such as radar tracks, target information, platform status, imagery, and command assignments. The purpose of this program is to insure the interoperability of Air Force TDLs. TDLs are used by weapons, platforms, and sensors of all services.

Navy Cooperative Engagement Capability (CEC)

The CEC system links Navy ships and aircraft operating in a particular area into a single, integrated air-defense network in which radar data collected by each

---

[4747] Staff, "DOD Now Preparing for Rapid Move to IPv6, Hi-Tech Chief Says," LookSmart, July 2, 2003, [http://www.findarticles.com/cf_dls/m0PJR/13_1/110307574/p1/article.jhtml].

[4748] Zachery Peterson, Report Finds DOD Management Style Hindering Development of GIG, Inside the Navy, Feb. 6, 2006.

[4749] Hampton Stephens, "USAF Will Begin Air-Defense Targeting Demonstration In FY-04," IDGA, June 27, 2003, [http://www.idga.org/iowa-robot/document.html?topic=196&document=30568].

platform is transmitted in a real-time to the other units in the network. Each unit in the CEC network fuses its own radar data with data received from the other units. As a result, units in the network share a common, composite, real-time air-defense picture. CEC will permit a ship to shoot air-defense missiles at incoming anti-ship missiles that the ship itself cannot see, using radar targeting data gathered by other units in the network. It will also permit air-defense missiles fired by one ship to be guided by other ships or aircraft.[4750]

Army Force XXI Battle Command Brigade and Below (FBCB2)

FBCB2, used with Blue Force Tracker computer equipment, is the U.S. Army's main digital system that uses the Tactical Internet for sending real-time battle data to forces on the battlefield. During Iraq operations, this system was used in some Bradley Fighting Vehicles and M1A1 Abrams tanks, and replaced paper maps and routine reporting by radio voice communication. The computer images and GPS capabilities allowed tank crews to use Blue Force Tracker to pinpoint their locations, even amid Iraqi sand storms, similar to the way pilots use instruments to fly in bad weather. Officials stationed at the Pentagon using Blue Force Tracker receivers were also able to observe the movements of U.S. forces.[4751]

Joint Tactical Radio System (JTRS)

The software-based JTRS Program is intended to bring together separate service-led programs into a joint software defined radio development effort.[4752] JTRS is a family of common, software-defined, programmable radios that are intended to interoperate with existing radio systems and provide the additional capability to access maps and other visual data by allowing the war fighter to communicate directly with battlefield sensors.[4753] DOD has determined that all future military radio systems should be developed in compliance with the architecture for JTRS. JTRS will initially be used by the Army as its primary tactical radio for mobile communications, including satellite communications. Acquisition for the JTRS program is being carried out through a series of five separate but interrelated clusters, with each cluster intended to meet a specific DOD requirement.

[4750] For more information, see CRS Report RS20557, Navy Network-Centric Warfare Concept: Key Programs and Issues for Congress, by Ronald O'Rourke.

[4751] Frank Tiboni and Matthew French, "Blue Force Tracking Gains Ground," Federal Computer Week, vol. 18, no. 7, Mar. 22, 2004, p. 49.

[4752] GAO report to the U.S. House of Representatives Committee on Appropriations, Subcommittee on Defense, Challenges and Risks Associated with the Joint Tactical Radio System Program, Aug. 2003.

[4753] Stephen Trimble, "Pentagon Adds 'Network Router' to List of JTRS Missions," Aerospace Daily, vol. 206, no 13, Apr. 17, 2003.

Army WIN-T and JNN

The Warfighter Information Network (WIN-T) is a high-capacity network system that will allow units and command centers to communicate while on the move. The Joint Network Nodes (JNN) is the bridge between the Cold War legacy 30-year-old Mobile Subscriber Equipment and the WIN-T. JNN currently gives brigade and battalion command posts a "reach-back" capability for direct contact with bases in the continental United States, or other locations. JNN provides a significant increase in capability to Army modular units by providing satellite-based high bandwidth communications down to the battalion level.[4754]

Army FCS

The Future Combat System (FCS) is intended to be the U.S. Army's multi year, multi-billion-dollar program at the heart of the Army's transformation efforts. It is to be the Army's major research, development, and acquisition program consisting of 18 manned and unmanned systems tied together by an extensive communications and information network. FCS is intended to replace such current systems as the M-1 Abrams tank and the M-2 Bradley infantry fighting vehicle with advanced, networked combat systems.[4755]

Oversight Issues for Congress

Potential oversight issues for Congress pertaining to NCO include the following.

Sufficient Information for Effective NCO Oversight

Does Congress have sufficient information on the full scope of the Administration's strategy for implementing NCO to conduct effective oversight? Are programs critical for NCO adequately identified as such in the DOD budget? Does the Administration's plan for defense transformation place too much, too little, or about the right amount of emphasis on NCO? Is the strategy for implementing NCO paced too quickly, too slowly, or at about the right speed? Does the Administration's strategy for implementing NCO programs call for too much, too little, or about the right amount of funding? How are "network centric" items identified separately in the budget line items?

[4754] Lieutenant General Steven Boutelle, U.S. Army, testimony at the Congressional hearing on Information Technology Issues and Defense Transformation, House Armed Services Subcommittee on Terrorism, Unconventional Threats and Capabilities Holds Hearing, April 6, 2006.

[4755] See CRS Report RL32888, The Army's Future Combat System (FCS): Background and Issues for Congress, by Andrew Feickert.

Sufficiently Joint NCO Planning

Is the Administration's strategy for implementing NCO sufficiently joint? Officials at DOD have recently said that when individuals responsible for program management fail to collaborate properly, program offices sometimes move forward working on requirements tailored for their specific service, rather than working on joint requirements.[4756] Is there adequate overall DOD information architecture or enterprise architecture? Do the current service network architectures — Army LandWarNet, Navy ForceNet, Air Force C2 constellation — allow systems to work together through the GIG, or do they function along service boundaries inconsistent with the joint environment?

Has DOD provided industry with sufficiently clear definitions of the architectures for its various desired NCO systems? If not, when does DOD plan to provide industry with such definitions? What are the potential risks of inadequately defined architectures?

What is the role of the Defense Information Systems Agency (DISA) in managing the DOD implementation of NCO? Does DISA have too much, not enough, or about the right amount of policy and funding authority to fulfill its role? Has DISA developed an adequate NCO roadmap to help guide investments, and if not, when does DISA plan to issue such a roadmap?

Future Combat System (FCS)

The FCS concept originally consisted of consisting of 18 manned and unmanned systems to be tied together by a network of advanced offensive, defensive, and communications/information systems, including WIN-T and the JTRS.[4757] The FCS is experiencing a number of program development issues - with some technologies advancing quicker than anticipated, others progressing along predicted lines, while still others are not meeting the Army's expectations.[4758] Is the FCS high technology concept appropriate for the types of conflicts that the U.S. will likely experience in the Global War on Terror?

[4756] John Bennett, C4ISR Programs Need Fewer Milestone Decision-Makers, Myers Says, InsideDefense, January 20, 2006, [http://www.insidedefense.com/secure/defense_docnum.asp?f=defense_2002.ask&docnum=AIRFORCE-17-3-9].

[4757] Lieutenant General Steven Boutelle, U.S. Army, testimony at the Congressional hearing on Information Technology Issues and Defense Transformation, House Armed Services Subcommittee on Terrorism, Unconventional Threats and Capabilities, Hearing, April 6, 2006.

[4758] See CRS Report RL32888, The Army's Future Combat System (FCS), Background and Issues for Congress, by Andrew Feickert.

Satellites

Some additional security features that help protect satellites from electronic attack may consume portions of bandwidth that could otherwise be used for communications. News reports note that DOD may, in some cases, be designing military satellites with reduced security features in order to free more bandwidth to support growing communications needs.[4759]

Unmanned Vehicles

Over 100 different UAVs of 10 different types were used in Operation Iraqi Freedom. Worldwide spending on UAVs will likely increase over the next decade to $4.5 billion annually, according to one defense analyst.[4760] However, officials from the Government Accountability Office recently reported that DOD lacks a "viable and strategic" plan for developing and acquiring unmanned vehicles. This problem has resulted in cost overruns, delivery delays, and duplication of effort. As a result of the Quadrennial Defense Review, the joint structure of the Joint Unmanned Combat Aerial System (J-UCAS) program was ended, and some UAV programs are now being developed separately by the Navy and Air Force.

The J-UCAS program had combined the efforts previously conducted under the DARPA/Air Force Unmanned Combat Air Vehicle (UCAV) program and the DARPA/Navy Naval UCAV (UCAV-N) program, for a common architecture to maximize interoperability. It is uncertain how many crossover benefits can be mutually provided by separate Navy and Air Force efforts because requirements are now very divergent. Other problems reportedly include issues of interoperability of UAVs with ground forces, limited availability of bandwidth, and problems with having both manned and unmanned aerial vehicles share airspace.[4761]

FBCB2 (Blue Force Tracker)

"Blue Force Tracker" describes a technical capability that has received widespread praise from troops for helping to reduce the problem of fratricide. During the 1991 Gulf War, friendly fire accounted for about 24 percent of 148 U.S. combat deaths, however, the rate declined to about 11 percent of 115 U.S.

[4759] Vago Muradian, China Tried to Blind U.S. Sats with laser, Defense News, Sept. 25, 2006, p.6.

[4760] Doub Beizer, Network Centric warfare Takes Flight, Washington Technology, July 18, 2005, [http://www.washingtontechnology.com/cgibin/udt/im.display.printable?client.id=wtonline-test&story.id=26588].

[4761] Testimony by Sharon Pickup, Hearing on FY2007 Budget: Unmanned Aerial Vehicles and Intelligence, Surveillance, and Reconnaissance Capabilities, House Armed Services Subcommittee on Tactical Air and Land Forces, April 6, 2006.

deaths during major combat in Iraq in 2003. Many top leaders credit Blue Force Tracker (BFT) technology with saving lives during combat.[4762]

The Blue Force Tracking System reportedly proved so successful in Iraq and Afghanistan that the Army is fielding it to additional units. Observers state that BFT is directly responsible for significant reduction in vehicle-to-vehicle fratricide, and, for example, allowed the Third Infantry Division to fight through darkness and sandstorms on its way to Baghdad.[4763]

Some questions remain that may affect the future development of BFT equipment and capabilities. Will the Blue Force Tracker database be designed with sufficient categories to enable tracking of different weapon types, vehicles, and individual soldiers for future joint, and coalition operations? Is training adequate for military operators to handle complex BFT capabilities? Will the military have sufficient bandwidth available for future needs? As technology evolves, will the supply of bandwidth support the deployment of miniaturized BFT communications equipment for the individual soldier? Is BFT adequately supported when operatingin urban areas and complex terrains, where structures may block radio signals?

Joint Tactical Radio System (JTRS)

The Joint Tactical Radio System (JTRS) is intended to enable faster, more streamlined communications among many different types of forces, but stalled development of this system may have created an obstacle to the full implementation of net-centric operations.[4764] Originally, the JTRS program was intended to replace DOD legacy radios operating between 2 megahertz and 2 gigahertz, and which were not designed to communicate with each other. However, requirements were modified in 2004 so that future JTRS radios would also include frequencies above 2 gigahertz, to allow communication with satellites and to support future access to the military Global Information Grid. To spur development of JTRS, DOD in November 2004, developed a policy that restricted the purchase of non-JTRS radios already on the market. However, this policy was cited by Congress as an impediment to meeting the needs of operational commanders in the field.[4765] JTRS is seen now as a program to

---

[4762] Charles Dervarics, "Broadening Blue Force Tracking," Defense News, Oct. 11, 2004.

[4763] Lieutenant General Steven Boutelle, U.S. Army, testimony at the Congressional hearing on Information Technology Issues and Defense Transformation, House Armed Services Subcommittee on Terrorism, Unconventional Threats and Capabilities, April 6, 2006.

[4764] For more information about JTRS, see CRS Report RL33161, The Joint Tactical Radio System (JTRS) and the Army's Future Combat System (FCS): Issues for Congress, by Andrew Feickert.

[4765] House of Representatives Report 108-622, July 20, 2004, p.170.

enhance, rather than replace, existing legacy radios, and JTRS systems will eventually replace legacy radios as they wear out.[4766]

Value of NCO Information

Is information overrated as an asset for NCO? How thoroughly has the administration studied the risks associated with data-dependent military doctrine? Several observers have argued that DOD plans stress only the rewards of information without including adequate analysis of the risks associated with possible over-reliance on data-driven systems. Some elite network centric corporations with state-of-the-art systems that offer "information superiority" have experienced perverse results, and sometimes even catastrophic economic losses (See Appendix C, Perverse Consequences of Data-Dependent Systems). Congress could encourage DOD to examine the economics of information in order to avoid similar perverse consequences on the battlefield that may be created by "information abundance."[4767]

Networking Classified Data with Coalition Forces

How well are coalition forces adapting to NCO? How are U.S. forces affected if coalition networks to which we must link are not as secure and robust? What are implications for future NCO operations when there is a need to share classified information with coalition forces and foreign countries? Is it possible to give Allies access to C4ISR information to improve collaboration during high-speed combat operations, while still protecting other information that is sensitive or classified? Will differences in the national disclosure policies for each coalition nation restrict sharing of necessary information among all partners during training operations, and if so, will this threaten the effectiveness of training? Will U.S. analysts or warfighters be overwhelmed by the vast increase in information that will flow if all coalition NCO networks are seamlessly linked to the U.S. NCO network? Will potential enemies probe for weaknesses in the links between the different networks operated by less sophisticated coalition forces, and thus find a way to disrupt the networks of U.S. forces?

The same issues that affect DOD operations with coalition partners may also affect coordination with U.S. first-responders during domestic attacks by terrorists. Should DOD networks also be extended to first-responders who may need support during possible widespread attacks involving nuclear bombs or biological weapons; for example, geo-spatial images from UAVs monitoring domestic areas? Should policy allow domestic first-responders to input, view, or

---

[4766] Scott Nance, "Army Sets Narrower Aims on Radio System," Defense Daily, Feb. 18, 2005, p.4.

[4767] Modern portfolio theory, Baysian analysis, and Monte Carlo simulation are quantitative tools that can be used to examine when and where the benefits of information transparency consistently outweigh the costs. Michael Schrage, Perfect Information and Perverse Incentives: Costs and Consequences of Transformation and Transparency, Security Studies Program Working Paper, Massachusetts Institute of Technology, E38-600, May 2003.

update important data during such an attack, even though some may not have appropriate security clearances?

NCO Technology Transfer

The global diffusion of technology will lead to the eventual loss of the monopoly position now enjoyed by U.S. forces using sophisticated networks and communications equipment. The United States may eventually face adversaries equipped with COTS technologies that provide many NCO capabilities. Technology transfer and offshore outsourcing may also increase the number of foreign-nationals who are experts in newer Internet technologies and software applications (See Appendix A, The Transition from IPv4 to IPv6). Does the Administration's strategy pay sufficient attention to possible national security issues related to technology transfer? What controls does DOD have in place regarding offshore subcontracting that ensure security?

Several potential adversaries reportedly have a military strategy that focuses on engaging the United States asymmetrically, rather than with conventional forces. China, for example, is reportedly tailoring its military capabilities to directly, or indirectly, undermine U.S. technological advantages.[4768] Does the Administration's strategy for implementing NCO pay sufficient attention to asymmetric threats and growth of technology skills in other countries? How is DOD working with industry to find ways to protect software against cyber threats, including those possibly related to offshore outsourcing of R&D and information technology services? Several policy options that may reduce risk to the effectiveness of NCO due to growth of technology skills in foreign countries may include (1) encourage companies to maintain critical design and manufacturing functions inside the U.S., (2) encourage highly skilled individuals to relocate to areas in the U.S. where industries are in need of technical professionals, or (3) encourage U.S. high technology workers to update and increase their set of job skills.[4769]

Speeding Acquisition for NCO Technologies

Does the Administration's strategy for implementing NCO incorporate the right technologies and strategy for acquisition? Some observers have stated there is not enough coordination between DOD and the private sector officials involved in information technology acquisition.[4770] Others have suggested that the

---

[4768] Vago Muradian, China Tried to Blind U.S. Sats with Laser, Defense News, Sept. 25, 2006, p.6.

[4769] Paul J. Kostek, Chair, American Association of Engineering Societies, Globalization vs Outsourcing and Their Impact on Competitiveness, Oct. 30, 2003, [http://www.planetee.com/Forums].

[4770] Representatives Kline and Meehan, Congressional Hearing on Information Technology Issues and Defense Transformation, Armed Services Subcommittee on Terrorism, Unconventional Threats and Capabilities, April 6, 2006.

acquisitions community must communicate more directly with the most forward areas of the military, where the business processes deliver value to the war-fighter, so that needs are more clearly understood.[4771]

DOD Directive 5000 requires that acquisition for all equipment and systems must follow a standard process which involves an examination of requirements, safety testing, developmental testing, and operational testing.[4772] However, the acquisition for an information system sometimes requires the same processes as that used for acquiring a major weapons system.

For a critically needed system, an operational needs statement (ONS) can sometimes shorten the debate about requirements, and also shorten the traditional testing process, thereby speeding acquisition and deployment of critical systems to warfighting units. Also, in some circumstances, to reduce delays in deployment of critical equipment and systems, the Secretary of Defense was given rapid acquisition authority to waive all federal acquisition regulations for acquisition of equipment.[4773] Some observers have suggested that another possibility for speeding up the process for acquisition and deployment would be to give Combatant Commanders limited acquisition authority. For example, the United States Special Operations Command (SOCOM) already has been granted acquisition authority, and reportedly they use it efficiently, and find they are able to buy off-the-shelf technologies to meet some requirements.[4774]

Future research into areas such as nanotechnology will likely lead to radically new innovations in material science, fabrication, and computer architecture. However, the basic research to develop new technologies requires high-risk investment, and increasingly involves international collaboration. Maintaining a U.S. military advantage for NCO may require stronger policies that encourage domestic education in science and high-technology, and that nurture long-term

---

[4771] Paul Brinkley, Deputy Undersecretary of Defense, Congressional Hearing on Information Technology Issues and Defense Transformation, Armed Services Subcommittee on Terrorism, Unconventional Threats and Capabilities, April 6, 2006.

[4772] DOD Directive 5000.1, The Defense Acquisition System, May 2003, [http://akss.dau.mil/dag/DoD5000.asp?view=document&doc=1].

[4773] Lieutenant General Steven Boutelle, U.S. Army, testimony at the Congressional hearing on Information Technology Issues and Defense Transformation, House Armed Services Subcommittee on Terrorism, Unconventional Threats and Capabilities Hearing, April 6, 2006.

[4774] Representative Saxton, Congressional Hearing on Information Technology Issues and Defense Transformation, House Armed Services Subcommittee on Terrorism, Unconventional Threats and Capabilities, April 6, 2006.

research that is bounded within the United States private sector, universities, and government laboratories.[4775]

(1) Technologies: Is DOD making sufficient investments for R&D in nanotechnology? Nanoscience may fundamentally alter military equipment, weapons, and operations for U.S. forces, and possibly for future U.S. adversaries. Does the Administration's plan pay sufficient attention to creating solutions to meet bandwidth requirements for implementing NCO? Latency, which is often caused by a bandwidth bottleneck, is an important complaint of warfighters. How do messages that are either dropped, lost, or delayed during transmission alter the effectiveness of Network Centric Operations?
(2) Acquisition: All DOD acquisition programs require a key performance parameter for interoperability and for successful exchange of critical information.[4776] Development of some weapons in the past has rendered them obsolete by the time they are finally produced, sometimes 15 to 20 years later. Admiral Arthur Cebrowski, former director of the DOD Office of Force Transformation reportedly proposed that program development cycles be brought in line with those of commercial industry, which are typically measured in months and years, instead of decades.[4777] How does the traditional DOD long acquisition cycle keep up with new commercial developments for high technology?[4778]

NCO Doctrine

NCO enables the military to fight with smaller units, moving rapidly using "swarming tactics". Has DOD developed adequate joint doctrine for NCO? Do training exercises involve coalition partners with complimentary NCO capabilities? How do differences in NCO capabilities of other coalition partners

---

[4775] Gerald Borsuk and Timothy Coffey, Moore's Law: A Department of Defense Perspective, Defense Horizons, Center for Technology and National Security Policy, National Defense University, No. 30, July 2003.

[4776] Lt. General Daniel Leaf, Vice Commander for U.S. Air Force Space Command, in U.S. Congress, House Armed Services Subcommittee on Terrorism, Unconventional Threats and Capabilities, hearing, Military C4I Systems, Oct. 21, 2003, [http://www.cq.com].

[4777] Keith Phucas, "The New Military: Proposing Change," Norristown, Pennsylvania Times-Herald, Nov. 28, 2003.

[4778] The Army Science Board recently completed a study of high-risk technologies that will be developed as part of the Army Future Combat System (FCS) program. The study identifies 7 major technology areas that will be emphasized throughout the FCS incremental acquisition strategy: joint interoperability, network survivability, bandwidth efficiency, smart antennas, software, transparent battle space, and systems reliability, [https://webportal.saalt.army.mil/sard-asb/ASBDownloads/FCS-Exec-Briefing.pdf].

affect U.S. warfighting capabilities? What are the potential risks of inadequately developed doctrine for joint or coalition operations using NCO?

Does doctrine for NCO also stress civilian casualty prevention and protection? What are the changing requirements for finding and recruiting personnel who are qualified to operate high-technology NCO equipment? Finally, if terrorist groups become more local and smaller in size, will law-enforcement activities, coupled with good intelligence, displace military operations as a more effective pre-emptive strategy for the future, partly because it may be seen as less controversial?

Related Legislation

No bills have yet been introduced in the current congress that are directly related to network centric operations. This report will be updated as events warrant.

Appendix A: The Transition from Internet Protocol Version 4 (IPv4) to IPv6

The Internet Protocol version 4 (IPv4) is the name of the digital signal transport protocol that has been used for global communications through the Internet since the 1970s. The U.S. military now uses several transport protocols for digital communications in addition to IPv4. However, DOD planners see a need for more network capabilities to support future NCO operations. By 2008, DOD is planning to convert digital military communications to use the newer Internet Protocol version 6 (IPv6) as the standard for all transmission through the Global Information Grid (GIG), and for all systems that are part of the Defense Information System Network (DISN) that will interoperate with the GIG.

IPv6 technology is considered the next-generation Internet transport protocol, and all commercial network communications equipment (also heavily used by the military) will eventually transition to its use, and gradually reduce support for IPv4. This is because IPv6 offers advantages in speed, capacity, and flexibility over IPv4. For example, IPv6 will enable network users to more easily set up a secure virtual private network (also known as secure tunneling through a network) than with IPv4. Using IPv6, hardware devices can be attached to a network and configured more easily, which will also provide mobile users with easier and faster access to network services.[4779]

However, because use of IPv4 is so firmly embedded in the commercial systems now used in the United States, the transition for the civilian communications infrastructure in other countries may go more smoothly and quickly. This is because new communications infrastructures now being built in other countries will use the newest equipment with IPv6 capability already built in. This may also

---

[4779] Brian Robinson, "IPv6: Built for Speed," Federal Computer Week, Aug. 30, 2004.

mean that much of the talent for managing the new IPv6 technology may eventually belong to technicians and programmers who reside in countries outside the United States. Research has shown that regional agglomeration of technical expertise increases active sharing of tacit knowledge among groups of innovators.[4780] Some of that tacit knowledge may also include sharing of information about newly-discovered vulnerabilities for the IPv6 technology.

What follows is a brief explanation of some technical differences between IPv4 and IPv6, and a discussion of possible economic and security issues related to the coming transition to the new Internet protocol.

Technical differences between IPv4 and IPv6

Information is sent through the Internet using packets (approximately 4000 digital bits per packet), and which include the address of the sender and the intended destination. Internet Protocol version 4 (IPv4) has been used globally since before 1983. However, IPv4 information packets are designed to carry an address in a 32-bit field, which means that IPv4 can only support approximately 4,000,000,000 Internet devices (computers, routers, websites, etc.). With Internet access expanding globally, and with more types of equipment now using Internet addresses (e.g., cell phones, household appliances, and PDAs) the number of Internet addresses needed for connected equipment could soon exceed the addressing capacity of the IPv4 protocol.

For example, slightly more than 3 billion of the 4 billion possible 32-bit IPv4 addresses are now allocated to U.S.-operated ISPs. In contrast, China and South Korea, with a combined population of more than 1.3 billion, are allocated 38.5 million and 23.6 million respectively. Therefore, Asian counties are especially interested in the possibilities that come with adoption of IPv6.

Internet Protocol version 6 (IPv6) quadruples the size of the address field from 32 bits to 128 bits (IPv1-IPv3, and IPv5 reportedly never emerged from testing in the laboratory). IPv6 could theoretically provide each person on the planet with as many as 60 thousand trillion-trillion unique Internet addresses. Theoretically, by switching to IPv6, humanity will never run out of Internet addresses. IPv6 is also believed to be more secure than IPv4 because it offers a feature for encryption at the IP-level.

[4780] Geographic concentration of information technology employment increases labor productivity among IT workers. Research indicates that geographic proximity matters most where tacit knowledge plays an important role in the generation of innovative activity, and tacit knowledge does play an very important role during the early life cycle of an information technology system. Christian Le Bas and Frederic Miribel, "Is the Death of Distance Argument Relevant: The Agglomeration Economies Associated with Information Technology Activities," [http://www.ish-lyon.cnrs.fr/labo/walras/Objets/Membres/Miribelebas_paper.pdf], p. 20.

However, several drawbacks may slow the global adoption of the IPv6 standard. Switching to IPv6 means that software applications that now use Internet addresses need to be changed. Every Web browser, every computer, every email application, and every Web server must be upgraded to handle the 128-bit address for IPv6. The routers that operate the Internet backbone now implement IPv4 via computer hardware, and cannot route IPv6 over the same hardware. By adding software to route IPv6 packets, the routers will operate more slowly, which may cripple the Internet. Alternatively, upgrading and replacing the hardware for millions of Internet routers would be very costly.

IPv4 also uses a technology feature called Natural Address Translation (NAT) which effectively multiplies the number of IP address that may exist behind any single firewall. This technology trick is widely employed within the United States, and its usage also adds an extra layer of security to both commercial networks and home PC networks that have a router. NAT allows a home user to connect multiple PCs to their home network, so they all can share a single IPv4 address behind the router/firewall. By using NAT, it is possible, and certainly much cheaper, to put off or ignore the problem of running out of IPv4 addresses. At least temporarily, in the United States, most technologists prefer sticking with NAT rather than switching over to IPv6.

Also, despite the new feature that allows IP-level encryption, there may be new security problems associated with converting to IPv6. Whenever new code is deployed onto computers, undiscovered bugs are usually soon discovered through study and repeated experimentation by hackers. Therefore, IPv6 may well hold security surprises that the designers have simply not found through extensive testing. And because switching over to IPv6 will be a global undertaking, some of the newly

discovered security problems could possibly become critical, and even threaten the functioning of the Internet itself.

IPv6 also offers other technical advantages over IPv4. For example, IPv6 makes peer-to-peer communication between individual computers much easier than with IPv4. This will make applications like Internet telephony and next generation multimedia groupware work much more smoothly.

Technology Divide

The opportunity to leapfrog past older Internet technology may someday result in increased expertise in newer technology for technicians and engineers who reside outside the United States. For example, countries such as India, North Korea, Iran, Pakistan, and Iraq that are now building new communications infrastructures for Internet commerce, may initially adopt the latest network

switching equipment using the newer IPv6 technology, and thus leapfrog over IPv4.

Meanwhile, industries in the United States, which are already heavily invested in older IPv4 technology, may remain tied to IPv4 using the NAT technology for a longer time. This is because NAT can extend the useful life of older IPv4 applications, and can defer the cost of conversion by transferring that cost to the ISPs, who would then set up gateways to translate between all IPv4 and IPv6 Internet traffic going into and out of the United States. The U.S. could then become divided from the technology used in the rest of the world, at least for a while, by an IPv4/IPv6 difference that is similar to the U.S./metric divide we see today.[4781]

Possible Vulnerabilities

U.S. military forces, to save time and expense, sometimes connect staff at multiple locations to the DOD secure SIPRNET network by using an encryption technique known as tunneling, which lets users traverse a non-secure network to access a top-secret one. For example, Marine Corps staff recently began using tunneling through the non-classified NIPRNET to extend the DOD classified SIPRNET to 47 sites in the Marine Forces Pacific Command.[4782] However, during OIF as much as seventy percent of NIPRNET traffic reportedly was routed through the civilian communications infrastructure. This means that when there is need for a high volume of U.S. military communications, security may be partly dependent on reliability of IPv6 equipment found in the civilian infrastructure and in commercial satellites.[4783]

Countries with emerging communications infrastructures, and purchasing the latest commercial network equipment, may also be the home countries of those best able to exploit IPv6 technical vulnerabilities. If this includes countries where the United States may be involved in military activity, hostile groups with appropriate technical knowledge of IPv6 vulnerabilities may be positioned to attempt to interfere with U.S. military communications.

[4781] Simson Garfinkel, The Net Effect, Jan. 7, 2004, [http://www.simson.net/pubs.php].

[4782] Dan Caterinicciа, "Marines Tunnel to SIPRNET," FederalComputerWeek, Dec. 9, 2002, [http://www.fcw.com].

[4783] Christopher Dorobek and Diane Frank, "Dod May Pull Key Net from the Internet," InsideDefense, Dec. 26, 2002, [http://www.insidedefense.com].

Appendix B: Changing Views on Metcalfe's Law of Networks

Differing interpretations of what is known as "Metcalfe's Law" may lead to different priorities for acquisition and deployment of NCO technologies, systems, and equipment.

In the past, some observers have stated that according to Metcalfe's Law, "the 'power' of a network is proportional to the square of the number of nodes in the network".[4784] Proponents of NCO in the past have also stated that network centric computing is governed by Metcalfe's Law, which asserts that the "power" or "payoff" of network-centric computing comes from information-intensive interactions between very large numbers of heterogeneous computational nodes on the network.[4785]

However, Metcalfe's Law observes that the potential value of a communications network increases (or scales) as a function of the square of the number of nodes that are connected by the network. After some deliberation, many of the same proponents now argue differently about the applicability of Metcalfe's Law to NCO, saying that it only provides insight into the fact that the "value" of a network to its users depends mainly on the interaction between the following:[4786]

1) content, quality, and timeliness of information interactions enabled by the network;
2) network-enabled, value-creation logic; and
3) user-value functions.

These proponents further state that NCO does not focus on network-centric computing and communications, but rather on information flows and the nature and characteristics of battlespace entities. However, it is also noteworthy that other military observers now propose a corollary to Metcalfe's Law: the complexity of a system is proportional to the cube of the number of nodes, and the reliability of a system is inversely proportional to its complexity.[4787]

[4784] Col. T.X. Hammes, War Isn't A Rational Business, Proceedings, U.S. Naval Institute, July 1998, [http://www.usni.org/Proceedings/Articles98/PROhammes.htm}.

[4785] Vice Admiral Arthur Cebrowski, John Garstka, Network-Centric Warfare: Its Origin and Future, Proceedings U.S. Naval Institute, January 1998, [http://www.usni.org/Proceedings/Articles98/PROcebrowski.htm].

[4786] David Alberts, John Garstka, Frederick Stein, Network Centric Warfare: Developing and Leveraging Information Superiority, 2nd edition, February 2000, pp. 103, 252, 265.

[4787] Col. T.X. Hammes, War Isn't A Rational Business, Proceedings, U.S. Naval Institute, July 1998, [http://www.usni.org/Proceedings/Articles98/PROhammes.htm].

In line with this corollary, some observers propose that different types of networks could have indirect limitations that may begin to appear as those networks reach very large numbers of nodes. Briscoe et. al. (2006) use observations of the rise and fall of Internet companies to propose that use of Metcalfe's Law to predict organizational success can sometimes result in organizational damage, if expectations are set too high.[4788] Other observers agree, stating that, with very large networks, other negative factors begin to emerge. For example, the number of messages increases beyond the capacity of the reader to handle. Many network users may then see a strong need to operate within a "less-noisey" network by using editors, moderators, or automatic filters to limit the number of messages.[4789] These observers agree that more research is need in the area of indirect limitations of networks.

Appendix C: Perverse Consequences of Data-Dependent Systems

The Office of Force Transformation [http://www.oft.osd.mil/] has indicated that DOD must continue to refine the rules and theory of network centric operations through simulation, testing, and experimentation. This section notes that although some experiences have shown that networking may increase certain advantages in warfare, other experiences may also indicate that relying on information systems can sometimes lead to unexpected results.

Information-Age warfare is increasingly path-dependent, meaning that small changes in the initial conditions will result in enormous changes in outcomes. Speed is an important characteristic for NCO because it enables a military force to define initial conditions favorable to their interests, and then pursue a goal of developing high rates of change that an adversary cannot outpace.[4790] To this end, whenever data-links are employed between military units and platforms, digital information can be shared and processed instantaneously, which produces a significant advantage over other military units that must rely on voice-only communications.

Examples that illustrate this advantage are found in several training exercises conducted in the 1990's between Royal Air Force jets equipped with data-links, referred to as Link-16, and U.S. Air Force jets with voice-only communications. A

[4788] Bob Briscoe, Andrew Odiyzko, Benjamin Tilly, Metcalfe's Law is Wrong; Communications Networks Increase in Value as they Add Members – but by How Much? The Devil is in the Details, IEEE Spectrum, July 1, 2006, vol.43, no. 7.

[4789] Brad Templeton, The Opposite of Metcalfe's Law, Comments on IEEE article by Briscoe, Andrew, and Tilly, July 2006, [http://www.templetons.com/brad/metcalfe.html].

[4790] Dan Caterinicia and Matthew French, "Network-centric Warfare: Not There Yet," Federal Computer Week, June 9, 2003, [http://www.fcw.com/fcw/articles/2003/0609/ cov-netcentric-06-09-03.asp].

series of air-to-air engagements showed that the RAF jets were able to increase their kill ratio over the U.S. jets by approximately 4-to-1. Other training engagements, involving more than 12,000 sorties using 2-versus-2, or 8-versus-16, aircraft showed that jets equipped with Link-16 increased their kill ratio by 150 percent over those aircraft having voice-only communications. Similar results were seen in training exercises involving Navy and Army units equipped with new networking technology.[4791]

However, some observers believe that important military decisions may not always lend themselves to information-based rational analysis.[4792] They argue that the military services, national security establishment, and intelligence community have not thoroughly studied the risks associated with a data-dependent military doctrine.

Issues raised by these observers include the following:

(1) Information flows may be governed by a diminishing marginal utility for added effectiveness. Quantitative changes in information and analysis may lead to qualitative changes in individual and organizational behavior that are sometimes counter-productive.
(2) An information-rich, opportunity-rich environment may shift the value of the information, redefine the mission objectives, and possibly increase the chances for perverse consequences.

In 1999, large-scale army experimentation with better visualization of the battlefield resulted in surprises such as requests for up to five times the normally-expected amounts of ammunition. Instead of concentrating on only critical targets, the experimental army units were overwhelmed with the vast array of potential targets they could now see. The unprecedented requests for larger quantities of ammunition caused logistical failures. More information did not assure better decision-making, but rather it exposed doctrinal flaws.[4793]

A similar effect was observed in later experiments conducted as part of the Network Centric Operations Conceptual Framework. Ammunition was expended at a faster rate, possibly because more information creates a target-rich

---

[4791] John Garstka, "Network-Centric Warfare Offers Warfighting Advantage," Signal Forum, Signal Magazine, May 2003.

[4792] Martin Burke, Information Superiority Is Insufficient To Win In Network Centric Warfare, Joint Systems Branch, Defence Science and Technology Organisation, 2001, [http://www.dodccrp.org/events/2000/5th_ICCRTS/cd/papers/Track4/024.pdf].

[4793] Robert R. Leonhard, "Principles of War for the Information Age," (Novato, CA: Presidio Press, 2000) p. 156, and p.224.

environment. These observations imply a possibly greater demand for logistics support.[4794]

Issues raise by other observers of data-driven systems are:

(3) Reliance on sophisticated information systems may lead to management overconfidence.
(4) Different analytical interpretations of data may lead to disagreements among commanders about who is best situated to interpret events and act on them.

The past economic under-performance of many hedge fund organizations and other technology firms that have employed very sophisticated network centric management techniques may serve as examples to caution DOD against over-reliance on data-driven military information systems. For example, Long-Term Capital Management (LTCM), a highly-leveraged multi-billion dollar hedge fund, and Cisco Systems, a well-respected high-tech firm, both used sophisticated systems to track market conditions and expand their data-driven "situational awareness" to gain and maintain competitive advantage. However, in 1998 a U.S. government-led consortium of banks bailed out LTCM after its trading losses put the entire world's financial system at risk of meltdown. Also, in 2001 Cisco was forced to take a $2.25 billion inventory write-down. While there is yet no professional consensus explaining these poor performance problems, many analysts agree that the presumed excellence of information systems may have invited managerial over-reliance, and that overreliance led to overconfidence. Executives may have ignored unambiguous external signals in favor of their own networked data.[4795]

Finally, some believe that more information imposes a higher degree of accountability on actions. Failure to minimize casualties or protect civilians may be digitally reviewed and used to politicize flawed military decisions.

These observers suggest that modern portfolio theory, Bayesian analysis, and Monte Carlo simulation are three quantitative tools that military decision makers should explore if they want the benefits of information transparency to consistently outweigh its costs. These tools could answer questions, such as: (a) if information were to be managed as a portfolio of investment risks much as asset classes like equities, fixed income, and commodities, how would commanders

---

[4794] Dr. Kimberly Holloman, Evidence Based Research, Inc., "The Network Centric Operations Conceptual Framework," Presentation at the Network Centric Warfare 2004 Conference, Washington, DC, Jan. 20, 2004, [http://www.oft.osd.mil/library/library.cfm?libcol=2].

[4795] Michael Schrage, Perfect Information and Perverse Incentives: Costs and Consequences of Transformation and Transparency, Security Studies Program Working Paper, Massachusetts Institute of Technology, E38-600, May 2003, p.4.

diversify to maximize their returns; (b) what information asset classes would they deem most volatile; (c) what information would they see as most reliable; and (d) which information classes would be co-variant, and which would be auto-correlated?[4796]

[4796] Ibid, 15.

Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, RL32114 (January 29, 2008).

CLAY WILSON, CONGRESSIONAL RESEARCH SERV., BOTNETS, CYBERCRIME, AND CYBERTERRORISM: VULNERABILITIES AND POLICY ISSUES FOR CONGRESS (2008), *available at* http://www.intelligencelaw.com/library/secondary/crs/pdf/RL32114_1-29-2008.pdf.

Order Code RL32114
Updated January 29, 2008

Clay Wilson
Specialist in Technology and National Security
Foreign Affairs, Defense, and Trade Division

Summary

Cybercrime is becoming more organized and established as a transnational business. High technology online skills are now available for rent to a variety of customers, possibly including nation states, or individuals and groups that could secretly represent terrorist groups. The increased use of automated attack tools by cybercriminals has overwhelmed some current methodologies used for tracking Internet cyberattacks, and vulnerabilities of the U.S. critical infrastructure, which are acknowledged openly in publications, could possibly attract cyberattacks to extort money, or damage the U.S. economy to affect national security.

In April and May 2007, NATO and the United States sent computer security experts to Estonia to help that nation recover from cyberattacks directed against government computer systems, and to analyze the methods used and determine the source of the attacks.[4797] Some security experts suspect that political protestors may have rented the services of cybercriminals, possibly a large network of infected PCs, called a "botnet," to help disrupt the computer systems of the Estonian government. DOD officials have also indicated that similar

[4797] Larry Greenemeier, "Estonian Attacks Raise Concern Over Cyber 'Nuclear Winter,'" Information Week, May 24, 2007, at [http://www.informationweek.com/news/showArticle.jhtml?articleID=199701774].

cyberattacks from individuals and countries targeting economic, political, and military organizations may increase in the future.[4798]

Cybercriminals have reportedly made alliances with drug traffickers in Afghanistan, the Middle East, and elsewhere where profitable illegal activities are used to support terrorist groups. In addition, designs for cybercrime botnets are becoming more sophisticated, and future botnet architectures may be more resistant to computer security countermeasures.[4799]

This report discusses options now open to nation states, extremists, or terrorist groups for obtaining malicious technical services from cybercriminals to meet political or military objectives, and describes the possible effects of a coordinated cyberattack against the U.S. critical infrastructure. This report will be updated as events warrant.

Introduction

The U.S. military is supported partly by civilian high technology services and products, most often in the form of communications systems and computer software.[4800] In future conflicts that involve cyberwarfare between nations, the distinction between U.S. military and civilian targets may be blurred and civilian computer systems may increasingly be seen as viable targets vulnerable to attack by adversaries.[4801] Computer networking technology has also blurred the boundaries between cyberwarfare, cybercrime, and cyberterrorism. Officials in government and industry now say that cybercrime and cyberattack services available for hire from criminal organizations are a growing threat to national

---

[4798] Jeanne Meserve, "Official: International Hackers Going After U.S. Networks," CNN.com, October 19, 2007, [http://www.cnn.com/2007/US/10/19/cyber.threats/index.html]. Sebastian Sprenger, "Maj. Gen. Lord Is a Groundbreaker," Federal Computer Week, October 15, 2007, vol. 21, no. 34, p. 44.

[4799] Tom Espiner, "Security Expert: Storm Botnet 'Services' Could Be Sold," CnetNews.com, October 16, 2007, [http://www.news.com/Security-expert-Storm-botnet-services-could-besold/2100-7349_3-6213781.html]. Dan Sullivan, "P2P Botnets Increasingly Sophisticated, Realtime-Websecurity," April 18, 2007, [http://www.realtime-websecurity.com/articles_and_analysis/2007/04/p2p_botnets_increasingly_sophi.html].

[4800] Dan Kuehl, professor at the National Defense University School of Information Warfare and Strategy, has pointed out that a high percentage of U.S. military messages flow through commercial communications channels, and this reliance creates a vulnerability during conflict. Eric Naef, "Wanja," Infocon Magazine, October 2003, [http://www.iwar.org.uk/ infocon/io-kuehl.htm].

[4801] Sebastian Sprenger, "Maj. Gen. Lord Is a Groundbreaker," Federal Computer Week, October 15, 2007, vol. 21, no. 34, p. 44.

security as well as to the U.S. economy.[4802] New and sophisticated cybercrime tools could operate to allow a nation state or terrorist group to remain unidentified while they direct cyberattacks through the Internet.[4803] Many experts point out that past incidents of conventional terrorism have already been linked with cybercrime, and that computer vulnerabilities may make government and civilian critical infrastructure systems seem attractive as targets for cyberattack.[4804] Some experts argue that the government of Estonia may have already experienced this type of cyberattack directed against their systems and websites in April, 2007.

This report explores the possible connections between cybercriminals and terrorist groups that want to damage the U.S. economy or national security interests. The report also examines the effects of a coordinated cyberattack against the U.S. critical infrastructure, including use of cybercrime tools that could possibly take advantage of openly-publicized cyber vulnerabilities. Trends in cybercrime are described, showing how malicious Internet websites, and other cybercrimes such as identity theft are linked to conventional terrorist activity.

Congress may wish to explore the possible effects on the U.S. economy and on the U.S. military that could result from a coordinated attack against civilian and military computers and communications systems, whether due to cybercrime or cyberterrorism. Congress may also wish to explore the difficulties associated with establishing doctrine for selecting an appropriate military or law enforcement response after such an attack.

Background

It is clear that terrorist groups are using computers and the Internet to further goals associated with spreading terrorism. This can be seen in the way that extremists are creating and using numerous Internet websites for recruitment and fund raising activities, and for Jihad training purposes. Several criminals who have recently been convicted of cybercrimes used their technical skills to acquire stolen credit card information in order to finance other conventional

---

[4802] James Lewis, testimony before the House Committee on Homeland Security, Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, April 15, 2007.

[4803] Tim Greene, "Storm Worm Strikes Back at Security Pros," NetworkWorld.com, October 24, 2007, at [http://www.networkworld.com/news/2007/102407-storm-worm-security.html?nlhtsec=1022securityalert4&&nladname=102507securityal].

[4804] Brian Krebs, "Three Worked the Web to Help Terrorists," The Washington Post, July 6, 2007, p. D01. Walsh, Terrorism on the Cheap. Rollie Lal, "Terrorists and Organized Crime Join Forces," International Herald Tribune, May 25, 2005, at [http://www.iht.com/articles/2005/05/23/opinion/edlal.php]. Barbara Porter, "Forum Links Organized Crime and Terrorism," By George!, summer 2004, at [http://www2.gwu.edu/~bygeorge/060804/crimeterrorism.html].

terrorist activities.[4805] It is possible that as criminals and terrorist groups explore more ways to work together, a new type of threat may emerge where extremists gain access to the powerful network tools now used by cybercriminals to steal personal information, or to disrupt computer systems that support services through the Internet.

Three Basic Methods for Disrupting Computer Systems

There are several effective methods for disrupting computer systems. This report focuses on the method known as cyberattack, or computer network attack (CNA), which uses malicious computer code to disrupt computer processing, or steal data. A brief description of three different methods are shown here. However, as technology changes, future distinctions between these methods may begin to blur.

An attack against computers may (1) disrupt equipment and hardware reliability, (2) change processing logic, or (3) steal or corrupt data.[4806] The methods discussed here are chosen based on the technology asset against which each attack mode is directed, and the effects each method can produce. The assets affected or effects produced can sometimes overlap for different attack methods.

- Conventional kinetic weapons can be directed against computer equipment, a computer facility, or transmission lines to create a physical attack that disrupts the reliability of equipment.
- The power of electromagnetic energy, most commonly in the form of an electromagnetic pulse (EMP), can be used to create an electronic attack (EA) directed against computer equipment or data transmissions. By overheating circuitry or jamming communications, EA disrupts the reliability of equipment and the integrity of data.[4807]
- Malicious code can be used to create a cyberattack, or computer network attack (CNA), directed against computer processing code, instruction logic, or data. The code can generate a stream of malicious network packets that can disrupt data or logic through exploiting a vulnerability in computer software, or a weakness in the computer security practices of an organization. This type of cyberattack can disrupt the reliability of equipment, the integrity of data, and the confidentiality of communications.

[4805] Gregory Crabb, "U.S. Postal Service Global Investigations," and Yuval Ben-Itzhak, "CTO Finjan," Presentation at the Gartner IT Security Summit 2007, Washington, DC, June 4, 2007.

[4806] All methods of computer attack are within the current capabilities of several nations. See CRS Report RL31787, Information Operations and Cyberwar: Capabilities and Related Policy Issues, by Clay Wilson.

[4807] For more on electromagnetic weapons, see CRS Report RL32544, High Altitude Electromagnetic Pulse (HEMP) and High Power Microwave (HPM) Devices: Threat Assessments, by Clay Wilson.

Cyberattack, Cybercrime, and Cyberterrorism

Labeling a "cyberattack" as "cybercrime" or "cyberterrorism" is problematic because of the difficulty determining with certainty the identity, intent, or the political motivations of an attacker.[4808] "Cybercrime" can be very broad in scope, and may sometimes involve more factors than just a computer hack. "Cyberterrorism" is often equated with the use of malicious code. However, a "cyberterrorism" event may also sometimes depend on the presence of other factors beyond just a "cyberattack."

Definitions for Cyberterrorism

Various definitions exist for the term "cyberterrorism", just as various definitions exist for the term "terrorism."[4809] Security expert Dorothy Denning defines cyberterrorism as "... politically motivated hacking operations intended to cause grave harm such as loss of life or severe economic damage."[4810] The Federal Emergency Management Agency (FEMA) defines cyberterrorism as "unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives."[4811]

Others indicate that a physical attack that destroys computerized nodes for critical infrastructures, such as the Internet, telecommunications, or the electric power grid, without ever touching a keyboard, can also contribute to, or be labeled as cyberterrorism.[4812] Thus, it is possible that if a computer facility were deliberately attacked for political purposes, all three methods described above (physical attack, EA, and cyberattack) might contribute to, or be labeled as "cyberterrorism."

[4808] Serge Krasavin, What is Cyberterrorism? Computer Crime Research Center, April 23, 2004, [http://www.crime-research.org/analytics/Krasavin/].

[4809] Under 22 USC, Section 2656, "terrorism" is defined as premeditated, politically motivated violence perpetrated against noncombatant targets by sub national groups or clandestine agents, usually intended to influence an audience. The United States has employed this definition of terrorism for statistical and analytical purposes since 1983. U.S. Department of State, 2002, Patterns of Global Terrorism, 2003, [http://www.state.gov/s/ct/rls/pgtrpt/2001/html/10220.htm].

[4810] Dorothy Denning, "Activism, Hactivism, and Cyberterrorism: The Internet as a tool for Influencing Foreign Policy," in John Arquilla and David Ronfeldt, eds., Networks and Netwars, (Rand 2001), p. 241. Dorothy Denning, Is Cyber War Next? Social Science Research Council, November 2001, at [http://www.ssrc.org/sept11/essays/denning.htm].

[4811] [http://www.fema.gov/pdf/onp/toolkit_app_d.pdf].

[4812] Dan Verton, "A Definition of Cyber-terrorism", Computerworld, August 11, 2003, [http://www.computerworld.com/securitytopics/security/story/0,10801,83843,00.html].

Definitions for Cybercrime

Cybercrime is crime that is enabled by, or that targets computers. Some argue there is no agreed-upon definition for "cybercrime" because "cyberspace" is just a new specific instrument used to help commit crimes that are not new at all. Cybercrime can involve theft of intellectual property, a violation of patent, trade secret, or copyright laws. However, cybercrime also includes attacks against computers to deliberately disrupt processing, or may include espionage to make unauthorized copies of classified data. If a terrorist group were to launch a cyberattack to cause harm, such an act also fits within the definition of a cybercrime. The primary difference between a cyberattack to commit a crime or to commit terror is found in the intent of the attacker, and it is possible for actions under both labels to overlap.

Botnets

Botnets are becoming a major tool for cybercrime, partly because they can be designed to very effectively disrupt targeted computer systems in different ways, and because a malicious user, without possessing strong technical skills, can initiate these disruptive effects in cyberspace by simply renting botnet services from a cybercriminal.[4813] Botnets, or "Bot Networks," are made up of vast numbers of compromised computers that have been infected with malicious code, and can be remotely-controlled through commands sent via the Internet. Hundreds or thousands of these infected computers can operate in concert to disrupt or block Internet traffic for targeted victims, harvest information, or to distribute spam, viruses, or other malicious code. Botnets have been described as the "Swiss Army knives of the underground economy" because they are so versatile.

Botnet designers, or "botmasters", can reportedly make large sums of money by marketing their technical services. For example, Jeanson Ancheta, a 21-year-old hacker and member of a group called the "Botmaster Underground", reportedly made more than $100,000 from different Internet Advertising companies who paid him to download specially-designed malicious adware code onto more than 400,000 vulnerable PCs he had secretly infected and taken over. He also made tens of thousands more dollars renting his 400,000-unit "botnet herd" to other companies that used them to send out spam, viruses, and other malicious code on the Internet. In 2006, Ancheta was sentenced to five years in prison.[4814]

[4813] Jeanne Meserve, "Official: International Hackers Going After U.S. Networks," CNN.com, October 19, 2007, [http://www.cnn.com/2007/US/10/19/cyber.threats/index.html]. Sebastian Sprenger, "Maj. Gen. Lord Is a Groundbreaker," Federal Computer Week, October 15, 2007, vol. 21, no. 34, p. 44.

[4814] Bob Keefe, "PC Security Still More of a Wish than a Promise," The Atlanta Journal, February 3, 2007, p. 1A.

Botnet code was originally distributed as infected email attachments, but as users have grown more cautious, cybercriminals have turned to other methods. When users click to view a spam message, botnet code can be secretly installed on the users' PC. A website may be unknowingly infected with malicious code in the form of an ordinary-looking advertisement banner, or may include a link to an infected website. Clicking on any of these may install botnet code. Or, botnet code can be silently uploaded, even if the user takes no action while viewing the website, merely through some un-patched vulnerability that may exist in the browser. Firewalls and antivirus software do not necessarily inspect all data that is downloaded through browsers. Some bot software can even disable antivirus security before infecting the PC. Once a PC has been infected, the malicious software establishes a secret communications link to a remote "botmaster" in preparation to receive new commands to attack a specific target. Meanwhile, the malicious code may also automatically probe the infected PC for personal data, or may log keystrokes, and transmit the information to the botmaster.

The Shadowserver Foundation is an organization that monitors the number of command and control servers on the Internet, which indicates the number of bot networks that are being controlled online at a given time. From November 2006 through May 2007, approximately 1,400 command and control servers were found to be active on the Internet. The number of individual infected drones that are controlled by these 1,400 servers reportedly grew from half a million to more than 3 million from March to May 2007. Symantec, another security organization, reported that it detected 6 million bot-infected computers in the second half of 2006.[4815]

Some botnet owners reportedly rent their huge networks for US$200 to $300 an hour, and botnets are becoming the weapon of choice for fraud and extortion.[4816] Newer methods are evolving for distributing "bot" software that may make it even more difficult in the future for law enforcement to identify and locate the originating "botmaster." Some studies show that authors of software for botnets are increasingly using modern, open-source techniques for software development, including the collaboration of multiple authors for the initial design, new releases to fix bugs in the malicious code, and development of software modules that make portions of the code reusable for newer versions of malicious software designed for different purposes. This increase in collaboration among hackers mirrors the professional code development techniques now used to create commercial software products, and is expected to make future botnets

---

[4815] Julie Bort, "Attack of the Killer Bots," Network World, Jul 2/9, 2007, p. 29.

[4816] Susan MacLean, "Report warns of Organized Cyber Crime," ItWorldCanada, August 26, 2005, [http://www.itworldcanada.com/a/IT-Focus/39c78aa4-df47-4231-a083-ddd1ab8985 fb.html].

even more robust and reliable. This, in turn, is expected to help increase the demand for malware services in future years.[4817]

Traditionally, botnets organize themselves in an hierarchical manner, with a central command and control location (sometimes dynamic) for the botmaster. This central command location is useful to security professionals because it offers a possible central point of failure for the botnet. However, in the near future, security experts believe that attackers may use new botnet architectures that are more sophisticated, and more difficult to detect and trace. One class of botnet architecture that is beginning to emerge uses peer-to-peer protocol,[4818] which, because of its decentralized control design, is expected to be more resistant to strategies for countering its disruptive effects.[4819] For example, some experts reportedly argue that a well-designed peer-to-peer botnet may be nearly impossible to shut down as a whole because it may provide anonymity to the controller, who can appear as just another node in the bot network.[4820]

Estonia, 2007

In the Spring of 2007, government computer systems in Estonia experienced a sustained cyberattack that has been labeled by various observers as cyberwarfare, or cyberterror, or cybercrime. On April 27, officials in Estonia moved a Soviet-era war memorial commemorating an unknown Russian who died fighting the Nazis. The move stirred emotions, and led to rioting by ethnic Russians, and the blockading of the Estonian Embassy in Moscow. The event also marked the beginning of a series of large and sustained Distributed Denial-Of-Service

---

[4817] McAfee Virtual Criminology Report: Organized Crime and the Internet, December 2006, [http://www.sigma.com.pl/pliki/albums/userpics/10007/Virtual_Criminology_Report_ 2006.pdf].

[4818] Gnutella emerged as the first fully decentralized peer-to-peer protocol in 2000, and was used on the Internet to share and swap music files in MP3 compression format. The music industry was often frustrated in their efforts to counter this peer-to-peer technology because it could not identify a main controlling source. Since then, several other peer-to-peer protocols have been developed.

[4819] Symantec, Trojan.Peacomm: Building a Peer-to-Peer Botnet, 2007, [http://www.symantec.com/enterprise/security_response/weblog/2007/01/trojanpeacomm_ building_a_peert.html]. Matthew Broersma, Peer-to-Peer Botnets a New and Growing Threat, CSO Online, April 17, 2007, [http://www2.csoonline.com/blog_view.html?CID= 32852]. Julian B. Grizzard et. al., Peer-to-Peer Botnets: Overview and Case Study, 2007, [http://www.usenix.org/events/hotbots07/tech/full_papers/grizzard/grizzard_html/]. Reinier Schoof and Ralph Koning, Detecting Peer-to-Peer Botnets, February 4, 2007, [http://staff.science.uva.nl/~delaat/sne-2006-2007/p17/report.pdf].

[4820] Tom Espiner, "Security Expert: Storm Botnet 'services' Could Be Sold," CnetNews.com, October 16, 2007, [http://www.news.com/Security-expert-Storm-botnet-services-could-besold/2100-7349_3-6213781.html]. Robert Lemos, Bot software looks to improve peerage, The Register, May 4, 2006, [http://www.theregister.co.uk/2006/05/04/nugache_p2p_ botnet/].

(DDOS) attacks launched against several Estonian national websites, including government ministries and the prime minister's Reform Party.[4821]

In the early days of the cyberattack, government websites that normally receive around 1,000 visits a day reportedly were receiving 2,000 visits every second. This caused the repeated shut down of some websites for several hours at a time or longer, according to Estonian officials.[4822] The attacks, which flooded computers and servers and blocked legitimate users, were described as crippling, owing to Estonia's high dependence on information technology, but limited resources for managing their infrastructure. Security experts say that the cyberattacks against Estonia were unusual because the rate of the packet attack was very high, and the series of attacks lasted weeks, rather than hour or days, which is more commonly seen for a denial of service attack.[4823] Eventually, NATO and the United States sent computer security experts to Estonia to help recover from the attacks, and to analyze the methods used and attempt to determine the source of the attacks.

This event can serve to illustrate how computer network technology has blurred the boundaries between crime, warfare, and terrorism. A persistent problem during and after any cyberattack is accurate identification of the attacker, by finding out whether it was sponsored by a nation, or was the independent work of a few unconnected individuals, or was initiated by a group to instill frustration and fear by damaging the computerized infrastructure and economy. The uncertainty of not knowing the initiator also affects the decision about whom should ultimately become a target for retaliation, and whether the response should come from law enforcement or the military.

Initially, the Russian government was blamed by Estonian officials for the cyberattacks, and there were charges of cyberwarfare. Other observers argued that the cyberattack involved collusion between the Russian government and transnational cybercriminals who made their large botnets available for short-term rent, either to individuals or to larger groups. They argue that as the rented time expired, the intensity of the persistent cyberattacks against Estonia also began to fall off.[4824] However, not all security experts agree, and it remains

---

[4821] Robert Vamosi, "Cyberattack in Estonia — What It Really Means," CnetNews.com, May 29, 2007, at [http://news.com.com/Cyberattack+in+Estonia-what+it+really+means/ 2008-7349_3-6186751.html].

[4822] Christopher Rhoads, "Cyber Attack Vexes Estonia, Poses Debate," The Wall Street Journal, May 18, 2007, p. A6.

[4823] Carolyn Marsan, "Examining the Reality of Cyberwar in Wake of Estonian Attacks," Network World, August 27, 2007, vol. 24, no. 33, p. 24.

[4824] Iain Thomson, "Russia 'Hired Botnets' for Estonia Cyber-War," Computing, [http://www.computing.co.uk/vnunet/news/2191082/claims-russia-hired-botnets].

unclear at this time whether the cyberattacks were sanctioned or initiated by the Russian government, or if a criminal botnet was actually involved.

After some investigation, network analysts later concluded that the cyberattacks targeting Estonia were not a concerted attack, but instead were the product of spontaneous anger from a loose federation of separate attackers. Technical data showed that sources of the attack were worldwide rather than concentrated in a few locations. The computer code that caused the DDOS attack was posted and shared in many Russian language chat rooms, where the moving of the war memorial was a very emotional topic for discussion. These analysts state that although access to various Estonian government agencies was blocked by the malicious code, there was no apparent attempt to target national critical infrastructure other than internet resources, and no extortion demands were made. Their analysis thus far concluded that there was no Russian government connection to the attacks against Estonia.[4825] However, investigation into the incident continues, and officials from the United States view some aspects of the event as a possible model for future cyberwarfare or cyberterrorism directed against a nation state.

In January 2008, a court in Estonia convicted and fined a local man for bringing down a government website, as part of the extended cyberattack in 2007. The 20year-old, who is apparently an ethnic Russian Estonian, used his home PC to carry out the attack. The investigation continues, and so far, he is the only person convicted for participating in the cyberattack against Estonia.[4826]

Other Trends in Cybercrime Methods

Cybercrime is usually conducted through a connection to the Internet, but can also involve unauthorized removal of data on small, portable flash drive storage devices. Cybercrime, usually in the form of network hacking, has involved persons with strong technical skills, often motivated by the desire to gain popularity among their technology peers. However, the growing trend is now to profit from these network cyberattacks by targeting specific systems, often through collaboration among criminals and technical experts. The motives that drive these cybercriminal groups now may differ from those of their paying customers, who may possess little or no technical skills.

New technologies continue to outpace policy for law enforcement. Problems of coordination among agencies of different countries, along with conflicting national policies about crime in cyberspace, work to the advantage of

---

[4825] Heise Security, Estonian DDoS — a final analysis, [http://www.heise-security.co.uk/news/print/90461].

[4826] Mike Sachoff, Man Convicted In Estonia Cyber Attack, WebProNews, January 24, 2008, [http://www.webpronews.com/topnews/2008/01/24/man-convicted-in-estonia-cyber-attack].

cybercriminals who can choose to operate from geographic locations where penalties for some forms of cybercrime may not yet exist. Sophisticated tools for cyberattack can now be found for sale or for rent on the Internet, where highly-organized underground cybercrime businesses host websites that advertise a variety of disruptive software products and malicious technical services. High-end cybercrime groups use standard software business development techniques to keep their products updated with the latest anti-security features, and seek to recruit new and talented software engineering students into their organizations.

Where illicit profits are potentially very large, some high-end criminal groups have reportedly adopted standard IT business practices to systematically develop more efficient and effective computer code for cybercrime. Studies also show that organized crime groups now actively recruit college engineering graduates and technical expert members of computer societies, and sponsor them to attend more information technology (IT) courses to further their technical expertise. However, in some cases, targeted students may not realize that a criminal organization is behind the recruitment offer.[4827]

Cyberattacks are increasingly designed to silently steal information without leaving behind any damage that would be noticed by a user. These types of attacks attempt to escape detection in order to remain on host systems for longer periods of time. It is also expected that as mobile communication devices are incorporated more into everyday life, they will be increasingly targeted in the future for attack by cybercriminals.[4828]

Malicious Code Hosted on Websites

Malicious code, such as viruses or Trojan Horses, are used to infect a computer to make it available for takeover and remote control. Malicious code can infect a computer if the user opens an email attachment, or clicks an innocent-looking link on a website. For example, users who visited the popular MySpace and YouTube websites in 2005, and who lacked important software security patches, reportedly may have had their PCs infected if they clicked on a banner advertisement which silently installed malicious code on their computers to log keystrokes or capture sensitive data. During the first half of 2006, the Microsoft Security Team reported that it had removed 10 million pieces of malicious

---

[4827] McAfee Virtual Criminology Report: Organized Crime and the Internet, December 2006, [http://www.sigma.com.pl/pliki/albums/userpics/10007/Virtual_Criminology_Report_2006.pdf].

[4828] A web crawler (also known as a Web spider or Web robot) is a program or automated script that browses the World Wide Web in a methodical, automated manner. Web crawlers are mainly used to create a copy of all the visited pages for later processing by a search engine that will index the downloaded pages to provide fast searches. Wikipedia, [http://en.wikipedia.org/wiki/Web_crawler].

software from nearly 4 million computers and web servers.[4829] Recently, analysts at Google tested several million web pages for the presence of malicious software, and determined that 4.5 million of the web pages examined were suspicious in nature. After further testing of the 4.5 million web pages, over 1 million were found to launch downloads of malicious software, and more than two thirds of those programs were "bot" software that, among other things, collected data on banking transactions and then emailed the information to a temporary email account.[4830]

Researchers at the San Jose, Calif.-based security firm, Finjan Inc., after reviewing security data from the first quarter of 2007, found that more malware is hosted on servers in countries such as the U.S. and U.K., than in other countries with less developed e-crime law enforcement policies. Findings from the Finjan 2007 Web Security Trends Report are based on an analysis of more than 10 million unique websites from Internet traffic recorded in the UK, and include the following:

- Attacks that involve the use of code obfuscation through diverse randomization techniques are growing more numerous and complex, making them virtually invisible to pattern-matching/signature-based methods in use by traditional antivirus products.
- Criminals are displaying an increasing level of sophistication when embedding malicious code within legitimate content with less dependence on outlaw servers in unregulated countries.

Finjan found that 90% of the websites examined containing malware resided on servers located in the U.S. or U.K. "The results of this study shatter the myth that malicious code is primarily being hosted in countries where e-crime laws are less developed," Finjan CTO Yuval Ben-Itzhak reportedly stated.[4831]

Identity Theft

Botnets and other examples of malicious code can operate to assist cybercriminals with identity theft. Current FBI estimates are that identity theft costs American businesses and consumers $50 billion a year. Individual users are often lured into clicking on tempting links that are found in email or when

---

[4829] Elise Ackerman, "Hackers' Infections Slither Onto Web Sites," The Mercury News, January 3, 2007, p. 1.

[4830] Jeff Hecht, "Web Browsers Are New Frontline in Internet War," NewScientistTech, May 5, 2007, [http://www.newscientisttech.com/article.ns?id=mg19426026.000&print=true]. Niels Provos et. al., The Ghost in the Browser: Analysis of Web-based Malware, Google, Inc., [http://www.usenix.org/events/hotbots07/tech/full_papers/provos/provos.pdf].

[4831] Finjan, Inc., Web Security Trends Report, Q2 2007, [http://www.finjan.com/Content.aspx?id=827].

visiting websites. Clicking on titles such as "Buy Rolex watches cheap," or "Check out my new Photos," can take advantage of web browser vulnerabilities to place malicious software onto a users system which allows a cybercriminal to gather personal information from the user's computer.

Malicious code can scan a victim's computer for sensitive information, such as name, address, place and date of birth, social security number, mother's maiden name, and telephone number. Full identities obtained this way are bought and sold in online markets. False identity documents can then be created from this information using home equipment such as a digital camera, color printer, and laminating device, to make official-looking driver's licences, birth certificates, reference letters, and bank statements.[4832]

Identity theft involving thousands of victims is also enabled by inadequate computer security practices within organizations.[4833] MasterCard International reported that in 2005 more than 40 million credit card numbers belonging to U.S. consumers were accessed by computer hackers.[4834] Some of these account numbers were reportedly being sold on a Russian website, and some consumers have reported fraudulent charges on their statements. Officials at the UFJ bank in Japan reportedly stated that some of that bank's customers may also have become victims of fraud related to theft of the MasterCard information.[4835] In June 2006, officials from the U.S. Department of Energy acknowledged that names and personal information belonging to more than 1,500 employees of the National Nuclear Security Administration (NNSA) had been stolen in a network

---

[4832] Lou Bobson, "Identity Theft Ruining Lives," The Sunday Mail, May 20, 2007, p. 62.

[4833] On April 12, 2005, personal information, such as Social Security Numbers for 310,000 U.S. citizens, may have been stolen in a data security breach that involved 59 instances of unauthorized access into its corporate databases using stolen passwords. Boston College reported in March 2005 that a hacker had gained unauthorized access to computer database records with personal information for up to 106,000 alumni, and in the same month, Chico State University of California, reported that its databases had been breached containing the names and Social Security numbers for as many as 59,000 current and former students. David Bank and Christopher Conkey, "New Safeguards for Your Privacy," The Wall Street Journal, March 24, 2005, p. D1.

[4834] Jonathan Krim and Michael Barbaro, "40 Million Credit Card Numbers Hacked," Washington Post, June 18, 2005, p. A01. See also the report by the U.S. House of Representatives Homeland Security Committee, July 1, 2005, raising concerns about potential ties between identity theft victims and terrorism. Caitlin Harrington, "Terrorists Can Exploit Identity Theft, Report From House Democrats Says," CQ Homeland Security, July 1, 2005.

[4835] BBC News, "Japan Cardholders 'Hit' by Theft," June 21, 2005, at [http://news.bbc.co.uk/1/hi/business/4114252.stm].

intrusion that apparently took place starting in 2004. The NNSA did not discover the security breach until one year after it had occurred.[4836]

Some sources report that stolen credit card numbers and bank account information are traded online in a highly structured arrangement, involving buyers, sellers, intermediaries, and service industries. Services include offering to conveniently change the billing address of a theft victim, through manipulation of stolen PINs or passwords. Observers estimated that in 2005 such services for each stolen MasterCard number cost between $42 and $72.[4837] Other news articles report that, in 2007, a stolen credit card number sells online for only $1, and a complete identity, including a U.S. bank account number, credit-card number, date of birth, and a government-issued ID number now sells for just $14 to $18.[4838]

As of January 2007, 35 states have enacted data security laws requiring businesses that have experienced an intrusion involving possible identity theft to notify persons affected, and to improve security for protection of restricted data. However, existing federal and state laws that impose obligations on information owners, may require harmonization to provide protections that are more uniform.[4839]

Cyber Espionage

Cyber espionage involves the unauthorized probing to test a target computer's configuration or evaluate its system defenses, or the unauthorized viewing and copying of data files. However, should a terrorist group, nation, or other organization use computer hacking techniques for political or economic motives, their deliberate intrusions may also qualify them, additionally, as cybercriminals. If there is disagreement about this, it is likely because technology has outpaced policy for labeling actions in cyberspace. In fact, industrial cyber espionage may now be considered a necessary part of global economic competition, and secretly

---

[4836] Dawn Onley and Patience Wait, "DOD's Efforts to Stave off Nation-State Cyberattacks Begin with China," Government Computer News, August 21, 2006.

[4837] CCRC staff, Russia, Biggest Ever Credit Card Scam, Computer Crime Research Center, July 8, 2005, at [http://www.crime-research.org/news/08.07.2005/1349/].

[4838] David Hayes, "A Dollar goes a Long Way in Swiping Private Data," The Kansas City Star, March 20, 2007, p. 1.

[4839] For more information about laws related to identity theft, see CRS Report RL34120, Information Security and Data Breach Notification Safeguards, by Gina Marie Stevens.

monitoring the computerized functions and capabilities of potential adversary countries may also be considered essential for national defense.[4840]

U.S. counterintelligence officials reportedly have stated that about 140 different foreign intelligence organizations regularly attempt to hack into the computer systems of U.S. government agencies and U.S. companies. Cyber espionage, which enables the exfiltration of massive amounts of information electronically, has now transformed the nature of counterintelligence, by enabling a reduced reliance on conventional spying operations.[4841] The Internet, including satellite links and wireless local networks, now offers new, low cost and low risk opportunities for espionage. In 2001, a Special Committee of Inquiry established by the European parliament accused the United States of using its Echelon electronic spy network to engage in industrial espionage against European businesses. Echelon was reportedly set up in 1971 as an electronic monitoring system during the Cold War. European-Union member Britain helps operate the system, which includes listening posts in Canada, Australia, and New Zealand. Echelon is described as a global spy system reportedly capable of intercepting wireless phone calls, e-mail, and fax messages made from almost any location around the world.[4842]

Figure 1. Diagram of Purported Echelon Spy System

Source: BBC News, July 6, 2000, at [http://news.bbc.co.uk/1/hi/world/europe/820758.stm].

The European parliament Special Committee reported that information gathered on Echelon may have helped the United States beat the European Airbus Consortium in selling aircraft to Saudi Arabia in 1994.[4843] In 1995, France expelled five American diplomats and other officials, reportedly including the

---

[4840] U.S. intelligence officials, speaking on background, explained that they have routinely penetrated potential enemies' computer networks. These officials claim that thousands of attacks have taken place and sensitive information was stolen. John Stanton, "Rules of Cyber War Baffle U.S. Government Agencies," National Defense, February 2000, [http://www.nationaldefensemagazine.org/issues/2000/Feb/Rules.htm].

[4841] Jeanne Meserve, "Official: International Hackers Going after U.S. Netoworks," CNN.com, October 19, 2007, [http://www.cnn.com/2007/US/10/19/cyber.threats/index. html].

[4842] Martin Asser, "Echelon: Big brother without a cause?" BBC News, July 6, 2000, [http://news.bbc.co.uk/1/hi/world/europe/820758.stm].

[4843] Ron Pemstein, "Europe Spy System," GlobalSecurity.org, March 30, 2000, [http://www.globalsecurity.org/intell/library/news/2000/03/000330-echelon1.htm]. Paul Meller, "European Parliament Adopts 'Echelon' Report," CNN.com, September 7, 2001, [http://archives.cnn.com/2001/TECH/internet/09/07/echelon.report.idg/].

Paris station chief for the CIA, because of suspected industrial espionage activities linked to Echelon.[4844]

The State Department denied that the U.S. government was engaged in industrial espionage. However, former director of the U.S. Central Intelligence Agency, James Woolsey, has reportedly justified the possibility of industrial espionage by the United States on the basis of the use of bribery by European companies. Officials of the European parliament reportedly expressed outrage about the justification, while not denying that bribery is sometimes used to make sales.[4845]

Some government officials warn that criminals now sell or rent malicious code tools for cyber espionage, and the risk for damage to U.S. national security due to cyber espionage conducted by other countries is great. One industry official, arguing for stronger government agency computer security practices, stated that, "If gangs of foreigners broke into the State or Commerce Departments and carried off dozens of file cabinets, there would be a crisis. When the same thing happens in cyberspace, we shrug it off as another of those annoying computer glitches we must live with."[4846]

In 2003, a series of cyberattacks designed to copy sensitive data files was launched against DOD systems, and the computers belonging to DOD contractors. The cyber espionage attack apparently went undetected for many months. This series of cyberattacks was labeled "Titan Rain," and was suspected by DOD investigators to have originated in China. The attacks were directed against the U.S. Defense Information Systems Agency (DISA), the U.S. Redstone Arsenal, the Army Space and Strategic Defense Installation, and several computer systems critical to military logistics. Although no classified systems reportedly were breached, many files were copied containing information that is sensitive and subject to U.S. export-control laws.

[4844] Chris Marsden, "European Union to Investigate US-Run Satellite Spy Network," World Socialist Website, July 10, 2000, [http://www.wsws.org/articles/ 2000/jul2000/eche-j10.shtml].

[4845] European Parliament resolution on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) (2001/2098(INI)), European Parliament approved on September 5, 2001, by 367 votes for, 159 against, and 39 abstentions, [http://www.cyber-rights.org/interception/echelon/ European_parliament_resolution.htm]. Gerhard SCHMID Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system), Doc.: A5-0264/2001, May 9, 2001, [http://www.statewatch.org/ news/2001/sep/02echelon.htm]. James Woolsey, Intelligence Gathering and Democracies: The Issue of Economic and Industrial Espionage, Federation of American Scientists, March 7, 2000, [http://ftp.fas.org/irp/news/2000/03/wool0300.htm].

[4846] James Lewis, testimony before the House Committee on Homeland Security, Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, April 15, 2007.

In 2006, an extended cyberattack against the U.S. Naval War College in Newport, Rhode Island, prompted officials to disconnect the entire campus from the Internet.[4847] A similar attack against the Pentagon in 2007 led officials to temporarily disconnect part of the unclassified network from the Internet. DOD officials acknowledge that the Global Information Grid, which is the main network for the U.S. military, experiences more than three million daily scans by unknown potential intruders.[4848]

Accurate attribution is important when considering whether to retaliate using military force or police action. Some DOD officials have indicated that the majority of cyber attacks against DOD and U.S. civilian agency systems are suspected to originate in China, and these attacks are consistently more numerous and sophisticated than cyberattacks from other malicious actors. The motives appear to be primarily cyber espionage against civilian agencies, DOD contractors, and DOD systems. The espionage involves unauthorized access to files containing sensitive industrial technology, and unauthorized research into DOD operations. Some attacks included attempts to implant malicious code into computer systems for future use by intruders.[4849]

Security experts warn that all U.S. federal agencies should now be aware that in cyberspace some malicious actors consider that no boundaries exist between military and civilian targets. According to an August 2005 computer security report by IBM, more than 237 million overall security attacks were reported globally during the first half of that year.[4850] Government agencies were targeted the most, reporting more than 54 million attacks, while manufacturing ranked second with 36 million attacks, financial services ranked third with approximately 34 million, and healthcare received more than 17 million attacks. The most frequent targets for these attacks, all occurring in the first half of 2005, were government agencies and industries in the United States (12 million), followed by New Zealand (1.2 million), and China (1 million). These figures likely represent an underestimation, given that most security analysts agree that the

---

[4847] Chris Johnson, Naval War College Network, "Web Site Back Up Following Intrusion," Inside the Navy, December 18, 2006.

[4848] Some estimates say that up to 90% of computer software used in China is pirated, and thus open to hijack through computer viruses. James Lewis, Computer Espionage, Titan Rain and China, Center for Strategic and International Studies, December 14, 2005.

[4849] Josh Rogin, "Cyber officials: Chinese hackers attack 'anything and everything,'" FCW.com, Febrary 13, 2007, [http://www.fcw.com/article97658-02-13-07-Web&print Layout].

[4850] The Global Business Security Index reports worldwide trends in computer security from incidents that are collected and analyzed by IBM and other security organizations. IBM press release, IBM Report: Government, Financial Services and Manufacturing Sectors Top Targets of Security Attacks in First Half of 2005, IBM, August 2, 2005.

number of incidents reported are only a small fraction of the total number of attacks that actually occur.

Terrorism Linked to Cybercrime

The proportion of cybercrime that can be directly or indirectly attributed to terrorists is difficult to determine. However, linkages do exist between terrorist groups and criminals that allow terror networks to expand internationally through leveraging the computer resources, money laundering activities, or transit routes operated by criminals. For example, the 2005 U.K. subway and bus bombings, and the attempted car bombings in 2007, also in the U.K., provide evidence that groups of terrorists are already secretly active within countries with large communication networks and computerized infrastructures, plus a large, highly skilled IT workforce. London police officials reportedly believe that terrorists obtained high-quality explosives used for the 2005 U.K. bombings through criminal groups based in Eastern Europe.[4851]

A recent trial in the U.K. revealed a significant link between Islamic terrorist groups and cybercrime. In June 2007, three British residents, Tariq al-Daour, Waseem Mughal, and Younes Tsouli, pled guilty, and were sentenced for using the Internet to incite murder. The men had used stolen credit card information at online web stores to purchase items to assist fellow jihadists in the field — items such as night vision goggles, tents, global positioning satellite devices, and hundreds of prepaid cell phones, and more than 250 airline tickets, through using 110 different stolen credit cards. Another 72 stolen credit cards were used to register over 180 Internet web domains at 95 different web hosting companies. The group also laundered money charged to more than 130 stolen credit cards through online gambling websites. In all, the trio made fraudulent charges totaling more than $3.5 million from a database containing 37,000 stolen credit card numbers, including account holders' names and addresses, dates of birth, credit balances, and credit limits.[4852]

Cybercriminals have made alliances with drug traffickers in Afghanistan, the Middle East, and elsewhere where illegal drug funds or other profitable activities such as credit card theft, are used to support terrorist groups.[4853] Drug traffickers

---

[4851] Walsh, Terrorism on the Cheap. Rollie Lal, "Terrorists and Organized Crime Join Forces," International Herald Tribune, May 25, 2005, at [http://www.iht.com/articles/2005/05/23/opinion/edlal.php]. Barbara Porter, "Forum Links Organized Crime and Terrorism," By George! summer 2004 [http://www2.gwu.edu/~bygeorge/060804/crimeterrorism.html].

[4852] Brian Krebs, "Three Worked the Web to Help Terrorists," The Washington Post, July 6, 2007, p. D01.

[4853] Peter Bergen, "The Taliban, Regrouped and Rearmed," The Washington Post, September 10, 2006, p. B1. Helen Cooper, "NATO Chief Says More Troops Are Needed in Afghanistan," The New York Times, September 22, 2006, p. 10.

are reportedly among the most widespread users of encryption for Internet messaging, and are able to hire high-level computer specialists to help evade law enforcement, coordinate shipments of drugs, and launder money. Regions with major narcotics markets, such as Western Europe and North America, also possess optimal technology infrastructure and open commercial nodes that increasingly serve the transnational trafficking needs of both criminal and terrorist groups.[4854] Officials of the U.S. Drug Enforcement Agency (DEA), reported in 2003 that 14 of the 36 groups found on the U.S. State Department's list of foreign terrorist organizations were also involved in drug trafficking. A 2002 report by the Federal Research Division at the Library of Congress, revealed a "growing involvement of Islamic terrorist and extremists groups in drug trafficking", and limited evidence of cooperation between different terrorist groups involving both drug trafficking and trafficking in arms.[4855] Consequently, DEA officials reportedly argued that the war on drugs and the war against terrorism are and should be linked.[4856]

State Department officials, at a Senate hearing in March 2002, also indicated that some terrorist groups may be using drug trafficking as a way to gain financing while simultaneously weakening their enemies in the West through exploiting their desire for addictive drugs.[4857] The poppy crop in Afghanistan reportedly supplies resin to produce over 90 percent of the world's heroin, supporting a drug trade estimated at $3.1 billion. Reports indicate that money from drug trafficking in Afghanistan is used to help fund terrorist and insurgent groups that operate in that country. Subsequently, U.S. intelligence reports in 2007 have stated that "al Qaeda in Afghanistan" has been revitalized and restored to its pre-September 11,

---

[4854] Glenn Curtis and Tara Karacan, The Nexus Among Terrorists, Narcotics Traffickers, Weapons Proliferators, and Organized Crime Networks in Western Europe, a study prepared by the Federal Research Division, Library of Congress, December 2002, p. 22, at [http://www.loc.gov/rr/frd/pdf-files/WestEurope_NEXUS.pdf].

[4855] L. Berry, G.E. Curtis, R.A. Hudson, and N. A. Kollars, A Global Overview of Narcotics-Funded Terrorist and Other Extremist Groups, Federal Research Division, Library of Congress, Washington, DC, May 2002.

[4856] Authorization for coordinating the federal war on drugs expired on September 30, 2003. For more information, see CRS Report RL32352, War on Drugs: Reauthorization of the Office of National Drug Control Policy, by Mark Eddy. Also, see D.C. Préfontaine, QC and Yvon Dandurand, Terrorism and Organized Crime Reflections on an Illusive Link and its Implication for Criminal Law Reform, International Society for Criminal Law Reform Annual Meeting — Montreal, August 8 — 12, Workshop D-3 Security Measures and Links to Organized Crime, August 11, 2004, at [http://www.icclr.law.ubc.ca/Publications/Reports/International%20Society%20Paper%20of%20Terrorism.pdf].

[4857] Rand Beers and Francis X. Taylor, U.S. State Department, Narco-Terror: The Worldwide Connection Between Drugs and Terror, testimony before the U.S. Senate Judiciary Committee, Subcommittee on Technology, Terrorism, and Government Information, March 13, 2002.

2001 operation levels, and may now be in a better position to strike Western countries.[4858]

Drug traffickers have the financial clout to hire computer specialists with skills for using technologies which make Internet messages hard or impossible to decipher, and which allow terrorist organizations to transcend borders and operate internationally with less chance of detection. Many highly trained technical specialists that make themselves available for hire originally come from the countries of the former Soviet Union and the Indian subcontinent. Some of these technical specialists reportedly will not work for criminal or terrorist organizations willingly, but may be misled or unaware of their employers' political objectives. Still, others will agree to provide assistance because other well-paid legitimate employment is scarce in their region.[4859]

Terrorist Groups Linked to Hackers

Links between computer hackers and terrorists, or terrorist-sponsoring nations may be difficult to confirm. Membership in the most highly-skilled computer hacker groups is sometimes very exclusive and limited to individuals who develop, demonstrate, and share only with each other, their most closely-guarded set of sophisticated hacker tools. These exclusive hacker groups do not seek attention because maintaining secrecy allows them to operate more effectively. Some hacker groups may also have political interests that are supra-national, or based on religion, or other socio-political ideologies, while other hacker groups may be motivated by profit, or linked to organized crime, and may be willing to sell their computer services, regardless of the political interests involved.

Information about computer vulnerabilities is now for sale online in a hackers' "black market". For example, a list of 5,000 addresses of computers that have already been infected with spyware and which are waiting to be remotely controlled as part of an automated "bot network" reportedly can be obtained for about $150 to $500. Prices for information about computer vulnerabilities for which no software patch yet exists reportedly range from $1,000 to $5,000.

[4858] Matthew Lee and Katherine Shrader, Al-Qaida has rebuilt, U.S. intel warns, Associated Press, July 12, 2007, [http://news.yahoo.com/s/ap/20070712/ap_on_go_pr_wh/us_terror_threat_32;_ylt=AuURr2eP8AhBrfHyTOdw714Gw_IE]. Associated Press, "Afghanistan's poppy crop could yield more than 2006's record haul, UN says," International Herald Tribune, June 25, 2007, [http://www.iht.com/articles/ap/2007/06/25/asia/AS-GEN-AfghanDrugs.php].

[4859] Louise Shelly, Organized Crime, Cybercrime and Terrorism, Computer Crime Research Center, September 27, 2004, [http://www.crime-research.org/articles/Terro rism_Cybercrime/].

Purchasers of this information are often organized crime groups, various foreign governments, and companies that deal in spam.[4860]

Terrorist Capabilities for Cyberattack

Some experts estimate that advanced or structured cyberattacks against multiple systems and networks, including target surveillance and testing of sophisticated new hacker tools, might require from two to four years of preparation, while a complex coordinated cyberattack, causing mass disruption against integrated, heterogeneous systems may require 6 to 10 years of preparation.[4861] This characteristic, where hackers devote much time to detailed and extensive planning before launching a cyberattack, has also been described as a "hallmark" of previous physical terrorist attacks and bombings launched by Al Qaeda.

It is difficult to determine the level of interest, or the capabilities of international terrorist groups to launch an effective cyberattack. A 1999 report by The Center for the Study of Terrorism and Irregular Warfare at the Naval Postgraduate School concluded that it is likely that any severe cyberattacks experienced in the near future by industrialized nations will be used by terrorist groups simply to supplement the more traditional physical terrorist attacks.[4862]

Some observers have stated that Al Qaeda does not see cyberattack as important for achieving its goals, preferring attacks which inflict human casualties.[4863] Other observers believe that the groups most likely to consider and employ cyberattack and cyberterrorism are the terrorist groups operating in post-industrial societies (such as Europe and the United States), rather than international terrorist groups that operate in developing regions where there is limited access to high technology.

However, other sources report that Al Qaeda has taken steps to improve organizational secrecy through more active and sophisticated use of technology,

---

[4860] Hackers sell their information anonymously through secretive websites. Bob Francis, "Know Thy Hacker," Infoworld, January 28, 2005 at [http://www.infoworld.com/article/05/01/28/05OPsecadvise_1.html].

[4861] Dorothy Denning, "Levels of Cyberterror Capability: Terrorists and the Internet," [http://www.cs.georgetown.edu/~denning/infosec/Denning-Cyberterror-SRI.ppt], presentation, and Zack Phillips, "Homeland Tech Shop Wants to Jump-Start Cybersecurity Ideas," CQ Homeland Security, September 14, 2004 at [http://homeland.cq.com/hs/display.do?docid=1330150&sourcetype=31&binderName=news-all].

[4862] Report was published in 1999, available at [http://www.nps.navy.mil/ctiw/reports/].

[4863] The Ashland Institute for Strategic Studies has observed that Al Qaeda is more fixated on physical threats than electronic ones. John Swartz, "Cyberterror Impact, Defense Under Scrutiny," USA Today, August 3, 2004, p. 2B.

and evidence suggests that Al Qaeda terrorists used the Internet extensively to plan their operations for September 11, 2001.[4864] In past years, Al Qaeda groups reportedly used new Internet-based telephone services to communicate with other terrorist cells overseas. Khalid Shaikh Mohammed, one of the masterminds of the attack against the World Trade Center, reportedly used special Internet chat software to communicate with at least two airline hijackers. Ramzi Yousef, who was sentenced to life imprisonment for the previous bombing of the World Trade Center, had trained as an electrical engineer, and had planned to use sophisticated electronics to detonate bombs on 12 U.S. airliners departing from Asia for the United States. He also used sophisticated encryption to protect his data and to prevent law enforcement from reading his plans should he be captured.[4865]

Tighter physical security measures now widely in place throughout the United States may encourage terrorist groups in the future to explore cyberattack as way to lower the risk of detection for their operations.[4866] However, other security observers believe that terrorist organizations might be reluctant to launch a cyberattack because it would result in less immediate drama and have a lower psychological impact than a more conventional bombing attack. These observers believe that unless a cyberattack can be made to result in actual physical damage or bloodshed, it will never be considered as serious as a nuclear, biological, or chemical terrorist attack.[4867]

Possible Effects of a Coordinated Cyberattack

In March 2007, researchers at Idaho National Laboratories (INL) conducted an experiment labeled the "Aurora Generator Test" to demonstrate the results of a simulated cyberattack on a power network. In a video released by the Department of Homeland Security, a power generator turbine, similar to many now in use throughout the United States, is forced to overheat and shut down dramatically, after receiving malicious commands from a hacker. The researchers at INL were investigating results of a possible cyberattack directed against a vulnerability that, reportedly, has since been fixed.[4868] The video, however, implied that other

---

[4864] David Kaplan, "Playing Offense: The Inside Story of How U.S. Terrorist Hunters Are Going after Al Qaeda," U.S. News & World Report, June 2, 2003, pp. 19-29.

[4865] Robert Windrem, "9/11 Detainee: Attack Scaled Back," September 21, 2003, [http://www.msnbc.com/news/969759.asp].

[4866] "Terrorism: An Introduction," April 4, 2003 at [http://www.terrorismanswers.com/terrorism].

[4867] James Lewis, "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats," December 2002 at [http://www.csis.org/tech/0211_lewis.pdf].

[4868] Robert Lemos, DHS Video Shows Potential Impact of Cyberattack, SecurityFocus.com, September 27, 2007, [http://www.securityfocus.com/brief/597].

multiple power generators sharing similar cyber vulnerabilities could potentially be disabled the same way.

In July 2002, the U.S. Naval War College hosted a war game called "Digital Pearl Harbor" to develop a scenario for a coordinated cyberterrorism event, where mock attacks by computer security experts against critical infrastructure systems simulated state-sponsored cyberwarfare. The simulated cyberattacks determined that the most vulnerable infrastructure computer systems were the Internet itself, and the computer systems that are part of the financial infrastructure.[4869] It was also determined that attempts to cripple the U.S. telecommunications infrastructure would be unsuccessful because built-in system redundancy would prevent damage from becoming too widespread. The conclusion of the exercise was that a "Digital Pearl Harbor" in the United States was only a slight possibility.[4870]

However, in 2002, a major vulnerability was discovered in switching equipment software that threatened the infrastructure for major portions of the Internet. A flaw in the Simple Network Management Protocol (SNMP) would have enabled attackers to take over Internet routers and cripple network telecommunications equipment globally. Network and equipment vendors worldwide raced quickly to fix their products before the problem could be exploited by hackers, with possible worldwide consequences. U.S. government officials also reportedly made efforts to keep information about this major vulnerability quiet until after the needed repairs were implemented on vulnerable Internet systems.[4871] According to an

---

[4869] At the annual conference of the Center for Conflict Studies, Phil Williams, Director of the Program on Terrorism and Trans-National Crime and the University of Pittsburgh, said an attack on the global financial system would likely focus on key nodes in the U.S. financial infrastructure: Fedwire and Fednet. Fedwire is the financial funds transfer system that exchanges money among U.S. banks, while Fednet is the electronic network that handles the transactions. The system has one primary installation and three backups. "You can find out on the Internet where the backups are. If those could be taken out by a mix of cyber and physical activities, the U.S. economy would basically come to a halt," Williams said. "If the takedown were to include the international funds transfer networks CHIPS and SWIFT then the entire global economy could be thrown into chaos." George Butters, "Expect Terrorist Attacks on Global Financial System," October 10, 2003 at [http://www.theregister. co.uk/content/55/33269.html].

[4870] The simulation involved more than 100 participants. Gartner, Inc., "Cyberattacks: The Results of the Gartner/U.S. Naval War College Simulation," July 2002, at [http://www3.gartner.com/2_events/audioconferences/dph/dph.html.] War game participants were divided into cells, and devised attacks against the electrical power grid, telecommunications infrastructure, the Internet and the financial services sector. It was determined that "peer-to-peer networking," a special method of communicating where every PC used commonly available software to act as both a server and a client, posed a potentially critical threat to the Internet itself. William Jackson, "War College Calls Digital Pearl Harbor Doable," Government Computer News, August 23, 2002, at [http://www.gcn.com/vol1_no1/daily-updates/19792-1.html].

[4871] The vulnerability was found in Abstract Syntax Notation One (ASN.1) encoding, and was extremely widespread. Ellen Messmer, "President's Advisor Predicts Cyber-catastrophes Unless

assessment reportedly written by the FBI, the security flaw could have been exploited to cause many serious problems, such as bringing down widespread telephone networks and also halting control information exchanged between ground and aircraft flight control systems.[4872]

Security experts agree that a coordinated cyberattack could be used to amplify the effects of a conventional terrorist attack, including a nuclear, biological, or chemical (NBC) attack. However, many of these same experts disagree about the damaging effects that might result from an attack directed against control computers that operate the U.S. critical infrastructure. Some observers have stated that because of U.S. dependency on computer technology, such attacks may have the potential to create economic damage on a large scale, while other observers have stated that U.S. infrastructure systems are resilient and would possibly recover easily, thus avoiding any severe or catastrophic effects.

While describing possible offensive tactics for military cyber operations, DOD officials reportedly stated that the U.S. could confuse enemies by using cyberattack to open floodgates, control traffic lights, or scramble the banking systems in other countries.[4873] Likewise, some of China's military journals speculate that cyberattacks could disable American financial markets. China, however, is almost as dependent on these U.S. markets as the United States, and might possibly suffer even more from such a disruption to finances. As to using cyberattack against other U.S. critical infrastructures, the amount of potential damage that could be inflicted might be relatively trivial compared to the costs of discovery, if engaged in by a nation state. However, this constraint does not apply to non-state actors like Al Qaeda, thus making cyberattack a potentially useful tool for those groups who reject the global market economy.[4874]

SCADA Vulnerabilities

Supervisory Control And Data Acquisition (SCADA) systems are the computers that monitor and regulate the operations of most critical infrastructure industries (such as the companies that manage the power grid). These SCADA computers automatically monitor and adjust switching, manufacturing, and other process control activities, based on digitized feedback data gathered by sensors. These

---

Security Improves," Network World Fusion, July 9, 2002 at [http://www.nwfusion.com/news/2002/0709schmidt.html].

[4872] Barton Gellman, "Cyber-Attacks by Al Qaeda Feared," Washington Post, June 27, 2002, p. A01.

[4873] Sebastian Sprenger, "Maj.Gen. Lord Is a Groundbreaker," Federal Computer Week, October 15, 2007, vol. 21, no. 34, pp. 44-45.

[4874] James Lewis, "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats," December 2002, at [http://www.csis.org/tech/0211_lewis.pdf].

control systems are often placed in remote locations, are frequently unmanned, and are accessed only periodically by engineers or technical staff via telecommunications links. However, for more efficiency, these communication links are increasingly connected to corporate administrative local area networks, or directly to the Internet.

Some experts believe that the importance of SCADA systems for controlling the critical infrastructure may make them an attractive target for terrorists.[4875] Many SCADA systems also now operate using Commercial-Off-The-Shelf (COTS) software, which some observers believe are inadequately protected against a cyberattack. These SCADA systems are thought to remain persistently vulnerable to cyberattack because many organizations that operate them have not paid proper attention to these systems' unique computer security needs.[4876]

The following example may serve to illustrate the possible vulnerability of control systems and highlight cybersecurity issues that could arise for infrastructure computers when SCADA controls are interconnected with office networks. In August 2003, the "Slammer"Internet computer worm was able to corrupt for five hours the computer control systems at the Davis-Besse nuclear power plant located in Ohio (fortunately, the power plant was closed and off-line when the cyberattack occurred). The computer worm was able to successfully penetrate systems in the Davis-Besse power plant control room largely because the business network for its corporate offices was found to have multiple connections to the Internet that bypassed the control room firewall.[4877]

[4875] Proprietary systems are unique, custom built software products intended for installation on a few (or a single) computers, and their uniqueness makes them a less attractive target for hackers. They are less attractive because finding a security vulnerability takes time, and a hacker may usually not consider it worth their while to invest the pre-operative surveillance and research needed to attack a proprietary system on a single computer. Widely used Commercial-Off-The-Shelf (COTS) software products, on the other hand, are more attractive to hackers because a single security vulnerability, once discovered in a COTS product, may be embedded in numerous computers that have the same COTS software product installed.

[4876] Industrial computers sometimes have operating requirements that differ from business or office computers. For example, monitoring a chemical process, or a telephone microwave tower may require 24-hour continuous availability for a critical industrial computer. Even though industrial systems may operate using COTS software (see above), it may be economically difficult to justify suspending the operation of an industrial SCADA computer on a regular basis to take time to install every new security software patch. See interview with Michael Vatis, director of the Institute for Security Technology Studies related to counterterrorism and cybersecurity. Sharon Gaudin, "Security Experts: U.S. Companies Unprepared for Cyber Terror," Datamation, July 19, 2002 at [http://itmanagement. earthweb.com/secu/article.php/1429851]. Also, Government Accountability Office, Information Security: Further Efforts Needed to Fully Implement Statutory Requirements in DOD, GAO-03-1037T, July 24, 2003, p. 8.

[4877] Kevin Poulsen, "Slammer Worm Crashed Ohio Nuke Plant Network," Security Focus, August 19, 2003, at [http://www.securityfocus.com/news/6767].

Other observers, however, suggest that SCADA systems and the critical infrastructure are more robust and resilient than early theorists of cyberterror have stated, and that the infrastructure would likely recover rapidly from a cyberterrorism attack. They cite, for example, that water system failures, power outages, air traffic disruptions, and other scenarios resembling possible cyberterrorism often occur as routine events, and rarely affect national security, even marginally. System failures due to storms routinely occur at the regional level, where service may often be denied to customers for hours or days. Technical experts who understand the systems would work to restore functions as quickly as possible. Cyberterrorists would need to attack multiple targets simultaneously for long periods of time to gradually create terror, achieve strategic goals, or to have any noticeable effects on national security.[4878]

For more information about SCADA systems, see CRS Report RL31534, Critical Infrastructure: Control Systems and the Terrorist Threat, by Dana A. Shea.

Unpredictable Interactions Between Infrastructures

An important area that is not fully understood concerns the unpredictable interactions between computer systems that operate the different U.S. infrastructures. The concern is that numerous interdependencies (where downstream systems may rely on receiving good data through stable links with upstream computers) could possibly build to a cascade of effects that are unpredictable in how they might affect national security.[4879] For example, while the "Blaster" worm was disrupting Internet computers over several days in August 2003, some security experts suggest that slowness of communication links, caused by Blaster worm network congestion, may have contributed to the Eastern United States power blackout that occurred simultaneously on August 14. The computer worm could have degraded the performance of several communications links between data centers normally used to send warnings to other utility managers downstream on the power grid.[4880]

[4878] Scott Nance, "Debunking Fears: Exercise Finds 'Digital Pearl Harbor' Risk Small," Defense Week, April 7, 2003 at [http://www.kingpublishing.com/publications/dw/].

[4879] The most expensive natural disaster in U.S. history, Hurricane Andrew, is reported to have caused $25 billion in damage, while the Love Bug virus is estimated to have cost computer users around the world somewhere between $3 billion and $15 billion. However, the Love Bug virus was created and launched by a single university student in the Philippines, relying on inexpensive computer equipment. Christopher Miller, GAO Review of Weapon Systems Software, March 3, 2003, e-mail communication, MillerC@gao.gov.

[4880] Network congestion caused by the Blaster worm reportedly delayed the exchange of critical power grid control data across the public telecommunications network, which could have hampered the operators' ability to prevent the cascading effect of the blackout. Dan Verton, "Blaster Worm Linked to Severity of Blackout," Computerworld, August 29, 2003, [http://www.computerworld.com/printthis/2003/0,4814,84510,00.html.].

Civilian Technology that Supports DOD

DOD uses Commercial-Off-The-Shelf (COTS) hardware and software products in core information technology administrative functions, and also in the combat systems of all services, as for example, in the integrated warfare systems for nuclear aircraft carriers.[4881] DOD favors the use of COTS products in order to take advantage of technological innovation, product flexibility and standardization, and resulting contract cost-effectiveness. Nevertheless, DOD officials and others have stated that COTS products are lacking in security, and that strengthening the security of those products to meet military requirements may be too difficult and costly for most COTS vendors. To improve security, DOD Information Assurance practices require deploying several layers of additional protective measures around COTS military systems to make them more difficult for enemy cyberattackers to penetrate.[4882]

However, on two separate occasions in 2004, viruses reportedly infiltrated two top-secret computer systems at the Army Space and Missile Defense Command. It is not clear how the viruses penetrated the military systems, or what the effects were. Also, contrary to security policy requirements, the compromised computers reportedly lacked basic anti virus software protection.[4883] Security experts have noted that no matter how much protection is given to computers, hackers are always creating new ways to defeat those protective measures.[4884]

Why Cyberattacks Are Successful

Networked computers with exposed vulnerabilities may be disrupted or taken over by a hacker, or by automated malicious code. Botnets opportunistically scan the Internet to find and infect computer systems that are poorly configured, or lack current software security patches. Compromised computers are taken over to become slaves in a "botnet", which can include thousands of compromised

---

[4881] Some ships of the U.S. Navy use Windows software. Bill Murray, "Navy Carrier to Run Win 2000," GCN.com, September 11, 2000, [http://www.gcn.com/vol19_no27/ dod/2868-1.html]. Major U.K. naval systems defense contractor, BAE Systems, also took the decision to standardize future development on Microsoft Windows. John Lettice, "OSS Torpedoed: Royal Navy Will Run on Windows for Warships," Register, September 6, 2004 at [http://www.theregister.co.uk/2004/09/06/ams_goes_windows_for_warships/].

[4882] Patience Wait, "Defense IT Security Can't Rest on COTS," GCN.com, September 27, 2004, at [http://www.gcn.com/23_29/news/27422-1.html].

[4883] Dawn Onley, "Army Urged to Step Up IT Security Focus," GCN.com, September 2, 2004, at [http://www.gcn.com/vol1_no1/daily-updates/27138-1.html].

[4884] Patience Wait, "Defense IT Security Can't Rest on COTS," GCN.com, September27, 2004, at [http://www.gcn.com/23_29/news/27422-1.html].

computers that are remotely controlled to collect sensitive information from each victim's PC, or to collectively attack as a swarm against other targeted computers.

Even computers that have updated software and the newest security patches may still be vulnerable to a type of cyberattack known as a "Zero-Day exploit." This may occur if a computer hacker discovers a new software vulnerability and launches a malicious attack to infect computers before a security patch can be created by the software vendor and distributed to protect users. Zero-day vulnerabilities in increasingly complex software are regularly discovered by computer hackers. Recent news articles report that zero-day vulnerabilities are now available at online auctions, where buyers and sellers negotiate with timed bidding periods and minimum starting prices. This allows newly-discovered computer security vulnerabilities to be sold quickly to the highest bidder. Computer security expert Terri Forslof, of Tipping Point, has reportedly said that such practices will "...increase the perceived value of vulnerabilities, and the good guys already have trouble competing with the money you can get on the black market."[4885]

The Insider Threat

A major threat for organizations is the ease with which data can now be copied and carried outside using a variety of portable storage devices, such as small flash drives. Newer high-density memory stick technology reportedly allows installed computer applications to be run entirely from the flash drive. This means that the entire contents of a PC could possibly be copied to and stored on a small, easily portable, and easily concealed media device.[4886]

Employees with access to sensitive information systems can initiate threats in the form of malicious code inserted into software that is being developed either locally, or under offshore contracting arrangements. For example, in January 2003, 20 employees of subcontractors working in the United States at the Sikorsky Aircraft Corporation were arrested for possession of false identification used to obtain security access to facilities containing restricted and sensitive military technology. All of the defendants pleaded guilty and have been sentenced, except for one individual who was convicted at trial on April 19, 2004.[4887]

[4885] Tim Green, Web Site auctions software vulnerabilities to highest bidder, Network World, August 8, 2007.

[4886] McAfee Virtual Criminology Report: Organized Crime and the Internet, December 2006, [http://www.sigma.com.pl/pliki/albums/userpics/10007/Virtual_Criminology_Report_ 2006.pdf].

[4887] U.S. Attorneys Office, District of Connecticut, at [http://www.usdoj.gov/usao/ct/attf. html].

Persistence of Computer System Vulnerabilities

Vulnerabilities in software and computer system configurations provide entry points for a cyberattack. Vulnerabilities persist largely as a result of poor security practices and procedures, inadequate training in computer security, or technical errors in software products.[4888] Inadequate resources devoted to staffing the security function may also contribute to poor security practices. Home PC users often have little or no training in best practices for effectively securing home networks and equipment.

Errors in New Software Products

Vendors for Commercial-Off-The-Shelf software (COTS) are often criticized for releasing new products with errors that create the computer system vulnerabilities.[4889] Richard Clarke, former White House cyberspace advisor until 2003, has reportedly said that many commercial software products have poorly written, or poorly configured security features.[4890] In response to such criticism, the software industry reportedly has made new efforts to design products with architectures that are more secure. For example, Microsoft has created a special Security Response Center and now works with DOD and with industry and government leaders to improve security features in its new products. However, many software industry representatives reportedly agree that no matter what investment is made to improve software security, there will continue to be

[4888] The SANS Institute, in cooperation with the National Infrastructure Protection Center (NIPC), publishes an annual list of the 10 most commonly exploited vulnerabilities for Windows systems and for Unix systems. The SANS/FBI Twenty Most Critical Internet Security Vulnerabilities, 2003, SANS, April 15, 2003 at [http://www.sans.org/top20/].

[4889] In September 2003, Microsoft Corporation announced three new critical flaws in its latest Windows operating systems software. Security experts predicted that computer hackers may possibly exploit these new vulnerabilities by releasing more attack programs, such as the "Blaster worm" that recently targeted other Windows vulnerabilities causing widespread disruption on the Internet. Jaikumar Vijayan, "Attacks on New Windows Flaws Expected Soon," Computerworld, September 15, 2003, vol. 37, no. 37, p. 1.

[4890] Agencies operating national security systems must purchase software products from a list of lab-tested and evaluated products in a program that requires vendors to submit software for review in an accredited lab, a process (known as certification and accreditation under the Common Criteria, a testing program run by the National Information Assurance Partnership) that often takes a year and costs several thousand dollars. The review requirement previously has been limited to military national security software, however, the administration has stated that the government will undertake a review of the program in 2003 to "possibly extend" it as a new requirement for civilian agencies. Ellen Messmer, White House issue "National Strategy to Secure Cyberspace," Network World Fusion, February 14, 2003, [http://www.nwfusion.com/news/2003/0214ntlstrategy.html].

vulnerabilities in future software because products are becoming increasingly more complex.[4891]

Inadequate Resources

Although software vendors periodically release fixes or upgrades to solve newly discovered security problems, an important software security patch might not get scheduled for installation on an organization's computers until several weeks or months after the patch is available.[4892] The job may be too time-consuming, too complex, or too low a priority for the system administration staff. With increased software complexity comes the introduction of more vulnerabilities, so system maintenance is never-ending. Sometimes the security patch itself may disrupt the computer when installed, forcing the system administrator to take additional time to adjust the computer to accept the new patch. To avoid such disruption, a security patch may first require testing on a separate isolated network before it is distributed for installation on all other regular networked computers.

Because of such delays, the computer security patches installed in many organizations may lag considerably behind the current cyberthreat situation. Whenever delays are allowed to persist in private organizations, in government agencies, or among PC users at home, computer vulnerabilities that are widely reported may remain unprotected, leaving networks open to possible attack for long periods of time.

Future Attractiveness of Critical Infrastructure Systems

There has yet been no published evidence showing a widespread focus by cybercriminals on attacking the control systems that operate the U.S. civilian critical infrastructure. Disabling infrastructure controls for communications, electrical distribution or other infrastructure systems, is often described as a likely scenario to amplify the effects of a simultaneous conventional terrorist attack involving explosives.

However, in 2006, at a security discussion in Williamsburg, Virginia, a government analyst reportedly stated that criminal extortion schemes may have already occurred, where cyberattackers have exploited control system vulnerabilities for economic gain. And, in December 2006, malicious software

---

[4891] Scott Charney, Chief Security Strategist, Microsoft, Statement before the House Committee on Armed Services, Terrorism, Unconventional Threats and Capabilities Subcommittee, Information Technology in the 21st Century Battlespace, hearing, July 24, 2003, p. 9.

[4892] A survey of 2000 PC users found that 42% had not downloaded the vendor patch to ward off the recent Blaster worm attack, 23% said they do not regularly download software updates, 21% do not update their anti-virus signatures, and 70% said they were not notified by their companies about the urgent threat due to the Blaster worm. Jaikumar Vijayan, "IT Managers Say They Are Being Worn Down by Wave of Attacks," Computerworld, August 25, 2003, vol. 37, no. 34, p. 1.

that automatically scans for control system vulnerabilities reportedly was made available on the Internet for use by cybercriminals. This scanner software reportedly can enable individuals with little knowledge about infrastructure control systems to locate a SCADA computer connected to the Internet, and quickly identify its security vulnerabilities.

The Idaho National Laboratory is tasked to study and report on technology risks associated with infrastructure control systems. Past studies have shown that many, if not most, automated control systems are connected to the Internet, or connected to corporate administrative systems that are connected to the Internet, and are currently vulnerable to a cyberattack. And, because many of these infrastructure SCADA systems were not originally designed with security as a priority, in many cases, new security controls cannot now be easily implemented to reduce the known security vulnerabilities.[4893] Following past trends, where hackers and cybercriminals have taken advantage of easy vulnerabilities, some analysts now predict that we may gradually see new instances where cybercriminals exploit vulnerabilities in critical infrastructure control systems.[4894]

Measuring Cybercrime

New, automated attack methods have outpaced current methods for tracking the number and severity of cyberattacks and cybercrime intrusions. For example, according to a study by the Cooperative Association for Internet Data Analysis (CAIDA), on January 25, 2003, the SQL Slammer worm (also known as "Sapphire") automatically spread to infect more than 90% of vulnerable computers worldwide within 10 minutes of its release on the Internet, making it the fastest-spreading computer worm in history. As the study reports, the Slammer worm doubled in size every 8.5 seconds and achieved its full scanning rate (55 million scans per second) after about 3 minutes. It caused considerable harm through network outages which led to numerous canceled airline flights and automated teller machine (ATM) failures.[4895]

The use of automated tools for cybercrime has had a dramatic affect on the Computer Emergency Response Team/ Coordinating Center (CERT/CC). In

---

[4893] Testimony of Aaron Turner, House Committee on Homeland Security, Subcommittee on Emerging Threats, Cybersecurity and Science & Technology, Hearing on "Cyber Insecurity: Hackers are Penetrating Federal Systems and Critical Infrastructure," April 19, 2007, [http://homeland.house.gov/SiteDocuments/20070419153130-95132.pdf].

[4894] Testimony of Aaron Turner, House Committee on Homeland Security, Subcommittee on Emerging Threats, Cybersecurity and Science & Technology, Hearing on "Cyber Insecurity: Hackers are Penetrating Federal Systems and Critical Infrastructure," April 19, 2007, [http://homeland.house.gov/SiteDocuments/20070419153130-95132.pdf].

[4895] "Internet Worm Keeps Striking," January 27, 2003, CBSNews.com at [http://www.cbsnews.com/stories/2003/01/28/tech/main538200.shtml].

2004, CERT/CC announced that it had abandoned its traditional practice of producing an annual report tracking the number of cyber intrusions recorded for each year. For many years prior to 2004, CERT/CC had maintained a database of statistics about security incidents that were reported to it anonymously by businesses and individuals worldwide. The reason given for abandoning its annual tracking report was because the widespread use of new, automated cyberattack tools had escalated the number of network attacks to such a high level, that the CERT/CC organization determined that traditional methods for counting security incidents had become meaningless as a metric for assessing the scope and effects of attacks against Internet-connected systems.[4896] The CERT-CC website currently states, "Given the widespread use of automated attack tools, attacks against Internet-connected systems have become so commonplace that counts of the number of incidents reported provide little information with regard to assessing the scope and impact of attacks. Therefore, beginning in 2004, we stopped publishing the number of incidents reported."[4897]

The FBI estimates that all types of computer crime in the U.S. now costs industry about $400 billion, while officials in the Department of Trade and Industry in Britain say computer crime has risen by 50 percent from 2005 to 2006. As one example of costs associated with a recent computer security breach, TJX, the parent company of TJ Maxx, took a $12 million charge in its fiscal first quarter of 2008 due to the theft of more than 45 million credit and debit card numbers, starting in 2006. The money reportedly went to investigating and containing the intrusion, improving computer security, communicating with customers, and other fees. TJX estimates that, adding damages from future lawsuits, the breach may eventually cost $100 per lost record, or a total of $4.5 billion.[4898]

It is estimated that only five per cent of cybercriminals are ever arrested or convicted because the anonymity associated with web activity makes them hard to catch, and the trail of evidence needed to link them to a cybercrime is hard to unravel. Studies also show that cybercrime incidents are rarely reported, especially by companies that wish to avoid negative publicity leading to possible loss of confidence by its customers. However, law enforcement officials argue that "maintaining a code of silence" won't benefit a company in the long-run. Steven Martinez, deputy assistant director for the FBI's cyber division, reportedly stated at the 2006 RSI Computer Security Conference that partnerships between law

---

[4896] "CERT/CC Statistics 1988-2004" at [http://www.cert.org/stats/cert_stats.html].

[4897] CERT Coordination Center, Carnegie Mellon University, [http://www.cert.org/stats/].

[4898] Sharon Gaudin, Breach Costs Soar at TJX, Information Week, May 21, 2007, p. 19.

enforcement, the academic community, and the private sector are key to understanding and reducing cybercrime.[4899]

Each year, the Computer Security Institute (CSI), with help from the FBI, conducts a survey of thousands of security practitioners from U.S. corporations, government agencies, financial institutions, and universities. The CSI/FBI Computer Crime and Security Survey, published annually, is perhaps the most widely-used source of information about how often computer crime occurs and how expensive these crimes can be. The 2006 survey indicated that the average financial loss reported due to security breaches was $167,713, an 18% decrease from the previous year's average loss of $203,606.

However, some observers argue that the analyses reported in the CSI/FBI survey may be questionable, because the survey methodology is not statistically valid.[4900] This is because the survey is limited only to CSI members, which reduces the likelihood that respondents are a representative sample of all security practitioners, or that their employers are representative of employers in general. In addition, the 2006 CSI/FBI survey points out that most companies are continuing to sweep security incidents under the rug.

With the apparent absence of statistically valid survey results concerning the financial costs of computer crime, and with an accompanying lack of clear data about the number and types of computer security incidents reported, it appears that there may be no valid way to currently understand the real scope and intensity of cybercrime. The growing use of botnets and sophisticated malicious code also suggests that the percentage of unreported cybercrime, plus the percentage undetected, may both be going up.

Problems Tracing Cybercrime

The challenge of identifying the source of attacks is complicated by the unwillingness of commercial enterprises to report attacks, owing to potential liability concerns. CERT/CC estimates that as much as 80% of all actual computer security incidents still remain unreported.[4901] Law enforcement

---

[4899] Marcia Savage, "Companies Still Not Reporting Attacks, FBI Director Says," SearchSecurity.com, February 15, 2006, [http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1166845,00.html?bucket=NEWS&topic=299990].

[4900] Bill Brenner, "Security Blog Log: Has CSI/FBI Survey Jumped the Shark?" SearchSecurity.com, July 21, 2006, [http://searchsecurity.techtarget.com/columnItem/0,294698,sid14_gci1202328,00.html].

[4901] Many cyberattacks are unreported usually because the organization is unable to recognize that it has been attacked, or because the organization is reluctant to reveal publicly that it has experienced a cyberattack, Government Accountability Office, Information Security: Further Efforts Needed to Fully Implement Statutory Requirements in DOD, GAO-031037T, July 24, 2003, p. 6.

officials concede they are making little progress in tracing the profits and finances of cybercriminals. Online payment services, such as PayPal and E-Gold, enable criminals to launder their profits and exploit the shortcomings of international law enforcement. Recently, Intermix Media was fined $7.5 million in penalties for distribution of spyware which silently captures personal information from user's PCs. However, some adware and spyware purveyors reportedly can still make millions of dollars per year in profits. Many companies who distribute spyware are difficult to pursue legally because they typically also offer some legitimate services. In many cases, the finances that back cybercrimes are so distributed they are hard for law enforcement to figure out.[4902]

Organized Cybercrime

Some large cybercriminal groups are transnational, with names like Shadowcrew, Carderplanet, and Darkprofits. Individuals in these groups reportedly operate from locations all over the world, working together to hack into systems, steal credit card information and sell identities, in a very highly structured, organized network.[4903] Organized crime is also recruiting teenagers who indicate they feel safer doing illegal activity online than in the street. A recent report from the McAfee security organization, titled the "Virtual Criminology Report", draws on input from Europe's leading high-tech crime units and the FBI, and suggests that criminal outfits are targeting top students from leading academic institutions and helping them acquire more of the skills needed to commit high-tech crime on a massive scale.[4904]

In the future, we may see new and different modes of criminal organization evolve in cyberspace. Cyberspace frees individuals from many of the constraints that apply to activities in the physical world, and current forms of criminal organization may not transition well to online crime. Cybercrime requires less personal contact, less need for formal organization, and no need for control over a geographical territory. Therefore, some researchers argue that the classical hierarchical structures of organized crime groups may be unsuitable for organized crime on the Internet. Consequently, online criminal activity may emphasize lateral relationships and networks instead of hierarchies.[4905]

[4902] Matt Hines, "Malware Money Though to Trace," Eweek, September 18, 2006, p. 14.

[4903] Kevin Poulsen, "Feds Square off with Organized Cyber Crime," SecurityFocus, February 17, 2005, [http://www.securityfocus.com/news/10525].

[4904] Bill Brenner, "Criminals Find Safety in Cyberspace," SearchSecurity.com, December 18, 2006, [http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1235455,00.html?bucket=NEWS&topic=299990].

[4905] Council of Europe Octopus Programme, Summary of the Organised Crime Situation Report 2004: Focus on the Threat of Cybercrime, Strausbourg, September 6, 2004, p. 48.

Instead of assuming stable personnel configurations that can persist for years, online criminal organization may incorporate the "swarming" model, in which individuals coalesce for a limited period of time in order to conduct a specific task, or set of tasks, and afterwards go their separate ways. The task of law enforcement could therefore become much more difficult. If cybercriminals evolve into the "Mafia of the moment" or the "cartel of the day," police will lose the advantage of identifying a permanent group of participants who engage in a set of routine illicit activities, and this will only contribute to the future success of organized cybercrime.[4906]

Federal Efforts to Protect Computers

The federal government has taken steps to improve its own computer security and to encourage the private sector to also adopt stronger computer security policies and practices to reduce infrastructure vulnerabilities. In 2002, the Federal Information Security Management Act (FISMA) was enacted, giving the Office of Management and Budget (OMB) responsibility for coordinating information security standards and guidelines developed by federal agencies.[4907] In 2003, the National Strategy to Secure Cyberspace was published by the Administration to encourage the private sector to improve computer security for the U.S. critical infrastructure through having federal agencies set an example for best security practices.[4908]

The National Cyber Security Division (NCSD), within the National Protection and Programs Directorate of the Department of Homeland Security (DHS) oversees a Cyber Security Tracking, Analysis and Response Center (CSTARC), tasked with conducting analysis of cyberspace threats and vulnerabilities, issuing alerts and warnings for cyberthreats, improving information sharing, responding to major cybersecurity incidents, and aiding in national-level recovery efforts. In addition, a new Cyber Warning and Information Network (CWIN) has begun operation in 50 locations, and serves as an early warning system for cyberattacks.[4909] The CWIN is engineered to be reliable and survivable, has no dependency on the

---

[4906] Susan Brenner, "Organized Cybercrime? How Cyberspace May Affect the Structure of Criminal Relationships," North Carolina Journal of Law and Technology, 2002, [http://www.jolt.unc.edu/Vol4_I1/Web/Brenner-V4I1.htm].

[4907] GAO has noted that many federal agencies have not implemented security requirements for most of their systems, and must meet new requirements under FISMA. See GAO Report GAO-03-852T, Information Security: Continued Efforts Needed to Fully Implement Statutory Requirements, June 24, 2003.

[4908] Tinabeth Burton, ITAA Finds Much to Praise in National Cybersecurity Plan, May 7, 2003, [http://www.findarticles.com/p/articles/mi_go1965/is_200303/ai_n7418485].

[4909] Bara Vaida, "Warning Center for Cyber Attacks is Online, Official Says," Daily Briefing, GovExec.com, June 25, 2003.

Internet or the public switched network (PSN), and reportedly will not be affected if either the Internet or PSN suffer disruptions.[4910]

In January 2004, the NCSD also created the National Cyber Alert System (NCAS), a coordinated national cybersecurity system that distributes information to subscribers to help identify, analyze, and prioritize emerging vulnerabilities and cyberthreats. NCAS is managed by the United States Computer Emergency Readiness Team (US-CERT), a partnership between NCSD and the private sector, and subscribers can sign up to receive notices from this new service by visiting the US-CERT website.[4911]

International Convention on Cybercrime

Cybercrime is also a major international challenge, even though attitudes about what comprises a criminal act of computer wrongdoing still vary from country to country. However, the Convention on Cybercrime was adopted in 2001 by the Council of Europe, a consultative assembly of 43 countries, based in Strasbourg. The Convention, effective July 2004, is the first and only international treaty to deal with breaches of law "over the internet or other information networks." The Convention requires participating countries to update and harmonize their criminal laws against hacking, infringements on copyrights, computer facilitated fraud, child pornography, and other illicit cyber activities.[4912]

Although the United States has signed and ratified the Convention, it did not sign a separate protocol that contained provisions to criminalize xenophobia and racism on the Internet, which would raise Constitutional issues in the United States.[4913] The separate protocol could be interpreted as requiring nations to imprison anyone guilty of "insulting publicly, through a computer system" certain groups of people based on characteristics such as race or ethnic origin, a requirement that could make it a crime to e-mail jokes about ethnic groups or question whether the Holocaust occurred. The Department of Justice has said that it would be unconstitutional for the United States to sign that additional

---

[4910] The Cyber Warning Information Network (CWIN) provides voice and data connectivity to government and industry participants in support of critical infrastructure protection, [http://www.publicsectorinstitute.net/ELetters/HomelandSecurityStrategies/Volume1No1/CyberWarningNetLaunch.lsp].

[4911] [http://www.us-cert.gov/cas/].

[4912] Full text for the Convention on Cyber Crime may be found at [http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&DF=18/06/04&CL=ENG].

[4913] The U.S. Senate Committee on Foreign Relations held a hearing on the Convention on June 17, 2004. CRS Report RS21208, Cybercrime: The Council of Europe Convention, by Kristin Archick. Estelle Durnout, Council of Europe Ratifies Cybercrime Treaty, ZDNet, March 22, 2004, at [http://news.zdnet.co.uk/business/legal/0,39020651,39149470,00.htm].

protocol because of the First Amendment's guarantee of freedom of expression. The Electronic Privacy Information Center, in a June 2004 letter to the Foreign Relations Committee, objected to U.S. ratification of the Convention, because it would "create invasive investigative techniques while failing to provide meaningful privacy and civil liberties safeguards."[4914]

On August 3, 2006, the U.S. Senate passed a resolution of ratification for the Convention. The United States will comply with the Convention based on existing

U.S. federal law; and no new implementing legislation is expected to be required. Legal analysts say that U.S. negotiators succeeded in scrapping most objectionable provisions, thereby ensuring that the Convention tracks closely with existing U.S. laws.[4915]

The Need to Improve Cybersecurity

Department of Defense (DOD) officials have stated that, while the threat of cyber attack is "less likely" to appear than conventional physical attack, it could actually prove more damaging because it could involve disruptive technology that might generate unpredictable consequences that give an adversary unexpected advantages.[4916] The Homeland Security Presidential Directive 7 required that the Department of Homeland Security (DHS) coordinate efforts to protect the cybersecurity for the nation's critical infrastructure. This resulted in two reports in 2005, titled "Interim National Infrastructure Protection Plan," and "The National Plan for Research and Development in Support of Critical Infrastructure Protection", where DHS provided a framework for identifying and prioritizing, and protecting each infrastructure sector.

However, some observers question why, in light of the many such reports describing an urgent need to reduce cybersecurity vulnerabilities, there is not an apparent perceived sense of national urgency to close the gap between cybersecurity and the threat of cyberattack. For example, despite Federal Information Security Management Act of 2002 (FISMA), some experts argue that security remains a low priority, or is treated almost as an afterthought at some

---

[4914] [http://www.epic.org/privacy/intl/senateletter-061704.pdf].

[4915] For more information about the Convention on Cybercrime, see CRS Report RS21208, Cybercrime: The Council of Europe Convention, by Kristin Archick.

[4916] Advantages of EA and CNA might derive from United States reliance on a computer-controlled critical infrastructure, along with unpredictable results depending on severity of the attack. Jason Sherman, "Bracing for Modern Brands of Warfare," Air Force Times, September 27, 2004, [http://www.airforcetimes.com/story.php?f=1-AIRPAPER-358727. php].

domestic federal agencies.[4917] In 2007, the Government Accountability Office issued a report, titled "Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain," which states that cybersecurity risks have actually increased for infrastructure control systems because of the persistence of interconnections with the Internet, and continued open availability of detailed information on the technology and configuration of the control systems. The report states that no overall strategy yet exists to coordinate activities to improve computer security across federal agencies and the private sector, which owns the critical infrastructure.[4918] Some observers argue that, as businesses gradually strengthen their security policies for headquarters and administrative systems, the remote systems that control critical infrastructure and manufacturing may soon be seen as easier targets of opportunity for cybercrime.

Cybercrime is obviously one of the risks of doing business in the age of the internet, but observers argue that many decision-makers may currently view it as a low-probability threat. Some researchers suggest that the numerous past reports describing the need to improve cybersecurity have not been compelling enough to make the case for dramatic and urgent action by decision-makers. Others suggest that even though relevant information is available, future possibilities are still discounted, which reduces the apparent need for present-day action. In addition, the costs of current inaction are not borne by the current decision-makers. These researchers argue that IT vendors must be willing to regard security as a product attribute that is coequal with performance and cost; IT researchers must be willing to value cybersecurity research as much as they value research for high performance or cost-effective computing; and, finally, IT purchasers must be willing to incur present-day costs in order to obtain future benefits.[4919]

Issues for Congress

Policy issues for cybercrime and cyberterrorism include a need for the following:

- increase awareness about changing threats due to the growing technical skills of extremists and terrorist groups;
- develop more accurate methods for measuring the effects of cybercrime;

[4917] Statement of James A. Lewis, Senior Fellow and Director, Technology and Public Policy Program, Center for Strategic and International Studies, Committee on House Oversight and Government Reform Subcommittee on Government Management, Organization, and Procurement, Subcommittee on Information Policy, Census, and National Archives, June 7, 2007.

[4918] GAO -08-119T, Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems are Under Way, but Challenges Remain, October 17, 2007.

[4919] Seymour Goodman and Herber Lin, editors, Toward a Safer and More Secure Cyberspace, Committee on Improving Cybersecurity Research in the United States, National Research Council, 2007, pp. 261-267, [http://books.nap.edu/openbook.php?isbn=030910 3959].

- help to determine appropriate responses by DOD to a cyberattack;
- examine the incentives for achieving the goals of the National Strategy to Secure Cyberspace;
- search for ways to improve the security of commercial software products;
- explore ways to increase security education and awareness for businesses and home PC users; and
- find ways for private industry and government to coordinate to protect against cyberattack.

Congress may also wish to consider ways to harmonize existing federal and state laws that require notice to persons when their personal information has been affected by a computer security breach, and that impose obligations on businesses and owners of that restricted information.[4920]

Growth in Technical Capabilities of Terrorists

Seized computers belonging to Al Qaeda indicate its members are becoming more familiar with hacker tools and services that are available over the Internet.[4921] Could terrorist groups find it advantageous to hire a cybercrime botnet tailored to attack specific targets, possibly including the civilian critical infrastructure of Western nations? Could cybercrime botnets, used strategically, provide a useful way for extremists to amplify the effects of a conventional terrorist attack using bombs?

As computer-literate youth increasingly join the ranks of terrorist groups, will cyberterrorism likely become increasingly more mainstream in the future? Will a computer-literate leader bring increased awareness of the advantages of an attack on information systems, or be more receptive to suggestions from other, newer computer-literate members? Once a new tactic has won widespread media attention, will it likely motivate other rival terrorist groups to follow along the new pathway?[4922]

Better Measurement of Cybercrime Trends

Experiences at CERT/CC show that statistical methods for measuring the volume and economic effects of cyberattacks may be questionable. Without sound statistical methods to accurately report the scope and effects of cybercrime,

---

[4920] For more information about laws related to identity theft, see CRS Report RL34120, Information Security and Data Breach Notification Safeguards, by Gina Marie Stevens.

[4921] Richard Clarke, "Vulnerability: What Are Al Qaeda's Capabilities?" PBS Frontline: Cyberwar, April 2003, at [http://www.pbs.org].

[4922] Jerrold M. Post, Kevin G. Ruby, and Eric D. Shaw, "From Car Bombs to Logic Bombs: The Growing Threat From Information Terrorism," Terrorism and Political Violence, summer 2000, vol. 12, no. 2, pp. 97-122.

government and legal authorities will continue to have unreliable measures of the effectiveness of their policies and enforcement actions.

Figures from several computer security reports now used for measuring annual financial losses to U.S. industry due to intrusions and cybercrime are believed by some observers to be limited in scope or possibly contain statistical bias.[4923] Is there a need for a more statistically reliable analysis of trends in computer security vulnerabilities and types of cyberattacks to more accurately show the costs and benefits for improving national cybersecurity? Congress may wish to encourage security experts to find more effective ways to collect data that will enable accurate analysis of trends for cyberattacks and cybercrime. Congress may also wish to encourage security researchers to find better ways to identify the initiators of cyberattacks.

DOD and Cyberattack Response

If a terrorist group were to use a cybercrime botnet to subvert computers in a third party country, such as China, to launch a cyberattack against the United States, the U.S. response to the cyberattack must be carefully considered, in order to avoid retaliating against the wrong entity. Would the resulting effects of cyberweapons used by the United States be difficult to limit or control? Would a cyberattack response that could be attributed to the United States possibly encourage other extremists, or rogue nations, to start launching their own cyberattacks against the United States? Would an attempt by the U.S. to increase surveillance of another entity via use of cyberespionage computer code be labeled as an unprovoked attack, even if directed against the computers belonging to a terrorist group? If a terrorist group should subsequently copy, or reverse-engineer a destructive U.S. military cyberattack program, could it be used against other countries that are U.S. allies, or even turned back to attack civilian computer systems in the United States?[4924] If the effects become widespread and severe, could the U.S. use of cyberweapons exceed the customary rules of military conflict, or violate international laws.[4925]

[4923] A well known source of information about the costs of cyberattacks is the annual computer security survey published by the Computer Security Institute (CSI), which utilizes data collected by the FBI. However, respondents to the CSI/FBI survey of computer security issues are generally limited only to CSI members, which may create statistical bias that affects the survey findings. Recently, CSI has also conceded weaknesses in its analytical approach and has suggested that its survey of computer security vulnerabilities and incidents may be more illustrative than systematic. However, the CSI/FBI survey remains useful despite its imperfect methodology. Bruce Berkowitz and Robert W. Hahn, "Cybersecurity: Who's Watching the Store?" Issues in Science and Technology, spring 2003.

[4924] See CRS Report RL31787, Information Warfare and Cyberwar: Capabilities and Related Policy Issues, by Clay Wilson.

[4925] The laws of war are international rules that have evolved to resolve practical problems relating to military conflict, such as restraints to prevent misbehavior or atrocities, and have not been

Commercial electronics and communications equipment are now used extensively to support complex U.S. weapons systems, and are possibly vulnerable to cyberattack. This situation is known to our potential adversaries.[4926] To what degree are military forces and national security threatened by computer security vulnerabilities that exist in commercial software systems, and how can the computer industry be encouraged to create new COTS products that are less vulnerable to cyberattack?

Incentives for the National Strategy to Secure Cyberspace

Does the National Strategy to Secure Cyberspace present clear incentives for achieving security objectives? Suggestions to increase incentives may include requiring that all software procured for federal agencies be certified under the "Common Criteria" testing program, which is now the requirement for the procurement of military software. However, industry observers point out that the software certification process is lengthy and may interfere with innovation and competitiveness in the global software market.[4927]

Should the National Strategy to Secure Cyberspace rely on voluntary action on the part of private firms, home users, universities, and government agencies to keep their networks secure, or is there a need for possible regulation to ensure best security practices? Has public response to improve computer security been

---

legislated by an overarching central authority. The United States is party to various limiting treaties. Sometimes the introduction of new technology tends to force changes in the understanding of the laws of war. Gary Anderson and Adam Gifford, "Order Out of Anarchy: The International Law of War," The Cato Journal, August 2004, vol. 15, no. 1, pp. 25-36.

[4926] Stanley Jakubiak and Lowell Wood, "DOD Uses Commercial Software and Equipment in Tactical Weapons," Statements before the House Military Research and Development Subcommittee, Hearing on EMP Threats to the U.S. Military and Civilian Infrastructure, October 7, 1999. House Armed Services Committee, Commission to Assess the Threat to the United States from Electromagnetic Pulse Attack, hearing, July 22, 2004.

[4927] Agencies operating national security systems are required to purchase software products from a list of lab-tested and evaluated products in a program run by the National Information Assurance Partnership (NIAP), a joint partnership between the National Security Agency and the National Institute of Standards and Technology. The NIAP is the U.S. government program that works with organizations in a dozen other countries around the world which have endorsed the international security-evaluation regimen known as the "Common Criteria." The program requires vendors to submit software for review in an accredited lab, a process that often takes a year and costs several thousand dollars. The review previously was limited to military national security software and equipment, however, the Administration has stated that the government will undertake a review of the program to "possibly extend" this software certification requirement to civilian agencies. Ellen Messmer, White House issue "National Strategy to Secure Cyberspace," Network World Fusion, February 14, 2003, at [http://www.nwfusion.com/news/2003/0214ntlstrategy.html].

slow partly because there are no regulations currently imposed?[4928] Would regulation to improve computer security interfere with innovation and possibly harm U.S. competitiveness in technology markets? Two of the former cybersecurity advisers to the president have differing views: Howard Schmidt has stated that market forces, rather than the government, should determine how product technology should evolve for better cybersecurity; however, Richard Clarke has stated that the IT industry has done little on its own to improve security of its own systems and products.[4929]

Improving Security of Commercial Software

Some security experts emphasize that if systems administrators received the necessary training for keeping their computer configurations secure, then computer security would greatly improve for the U.S. critical infrastructure. However, should software product vendors be required to create higher quality software products that are more secure and that need fewer patches? Could software vendors possibly increase the level of security for their products by rethinking the design, or by adding more test procedures during product development?

Education and Awareness of Cyberthreats

Ultimately, reducing the threat to national security from cybercrime depends on a strong commitment by government and the private sector to follow best management practices that help improve computer security. Numerous government reports already exist that describe the threat of cybercrime and make recommendations for management practices to improve cybersecurity.

A 2004 survey done by the National Cyber Security Alliance and AOL showed that most home PC users do not have adequate protection against hackers, do not

---

[4928] Business executives may be cautious about spending for large new technology projects, such as placing new emphasis on computer security. Results from a February 2003 survey of business executives indicated that 45% of respondents believed that many large Information Technology (IT) projects are often too expensive to justify. Managers in the survey pointed to the estimated $125.9 billion spent on IT projects between 1977 and 2000 in preparation for the year 2000 (Y2K) changeover, now viewed by some as a non-event. Sources reported that some board-level executives stated that the Y2K problem was overblown and over funded then, and as a result, they are now much more cautious about future spending for any new, massive IT initiatives. Gary H. Anthes and Thomas Hoffman, "Tarnished Image," Computerworld, May 12, 2003, vol. 37, no. 19, p. 37.

[4929] Howard Schmidt points out that major technology firms now promote anti-virus software and encourage better cybersecurity practices. He stresses that market forces are causing private industry to improve security of products. Martin Kady, "Cybersecurity a Weak Link in Homeland's Armor," CQ Weekly, February 14, 2005. Meanwhile, Richard Clarke, who initially opposed regulation during his tenure in the Clinton and Bush administrations, now states that the IT industry only reponds to improve security of its products when regulation is threatened. William Jackson, "To Regulate or Not to Regulate? That Is the Question," Government Computer News, February 26, 2005.

have updated antivirus software protection, and are confused about the protections they are supposed to use and how to use them.[4930] How can computer security training be made available to all computer users that will keep them aware of constantly changing computer security threats, and that will encourage them to follow proper security procedures?

Coordination Between Private Sector and Government

What can be done to improve sharing of information between federal government, local governments, and the private sector to improve computer security? Effective cybersecurity requires sharing of relevant information about threats, vulnerabilities, and exploits.[4931] How can the private sector obtain information from the government on specific threats which the government now considers classified, but which may help the private sector protect against cyberattack? And, how can the government obtain specific information from private industry about the number of successful computer intrusions, when companies resist reporting because they want to avoid publicity and guard their trade secrets?[4932] Should cybercrime information voluntarily shared with the federal government about successful intrusions be shielded from disclosure through Freedom of Information Act requests?

How can the United States better coordinate security policies and international law to gain the cooperation of other nations to better protect against a cyberattack? Pursuit of hackers may involve a trace back through networks requiring the cooperation of many Internet Service Providers located in several different nations.[4933] Pursuit is made increasingly complex if one or more of the nations involved has a legal policy or political ideology that conflicts with that of the United States.[4934]

[4930] A 2004 survey of 329 PC users revealed that most computer users think they are safe but lack basic protections against viruses, spyware, hackers, and other online threats. In addition, large majorities of home computer users have been infected with viruses and spyware and remain highly vulnerable to future infections. AOL and the National Cyber Security Alliance, "Largest In-home Study of Home Computer Users Shows Major Online Threats, Perception Gap," October 2004 at [http://www.staysafeonline.info/news/NCSAAOLIn-HomeStudyRelease.pdf].

[4931] Government Accountability Office, Homeland Security: Efforts To Improve Information Sharing Need to Be Strengthened, GAO-03-760, August 2003.

[4932] CRS Report RL30153, Critical Infrastructures: Background, Policy and Implementation, by John Moteff.

[4933] Trace back to identify a cyberattacker at the granular level remains problematic. Dorothy Denning, Information Warfare and Security (Addison-Wesley, 1999), p. 217.

[4934] In Argentina, a group calling themselves the X-Team, hacked into the website of that country's Supreme Court in April 2002. The trial judge stated that the law in his country covers crime against people, things, and animals but not websites. The group on trial was declared not guilty of breaking into the website. Paul Hillbeck, "Argentine Judge Rules in Favor of Computer

Thirty-eight countries, including the United States, participate in the Council of Europe's Convention on Cybercrime, which seeks to combat cybercrime by harmonizing national laws, improving investigative abilities, and boosting international cooperation. However, how effective will the Convention without participation of other countries where cybercriminals now operate freely? (For more on the Convention, see CRS Report RS21208, Cybercrime: The Council of Europe Convention, by Kristin Archick.)

Legislative Activity

H.R. 1525 — The Internet Spyware (I-SPY) Prevention Act of 2007, proposes penalties for unauthorized access to computers, or the use of computers to commit crimes. On May 23, 2007, this bill was received in the Senate and referred to the Committee on the Judiciary.

H.R. 1684 — The Department of Homeland Security Authorization Act for Fiscal Year 2008 establishes within the Department of Homeland Security an Office of Cybersecurity and Communications, headed by the Assistant Secretary for Cybersecurity and Communications, with responsibility for overseeing preparation, response, and reconstitution for cybersecurity and to protect communications from terrorist attacks, major disasters, and other emergencies, including large-scale disruptions.

The bill directs the Assistant Secretary to do the following:

- Establish and maintain a capability within the Department for ongoing activities to identify threats to critical information infrastructure to aid in detection of vulnerabilities and warning of potential acts of terrorism and other attacks.
- Conduct risk assessments on critical information infrastructure with respect to acts of terrorism.
- Develop a plan for the continuation of critical information operations in the event of a cyber attack.
- Define what qualifies as a cyber incident of national significance for purposes of the National Response Plan.
- Develop a national cybersecurity awareness, training, and education program that promotes cybersecurity awareness within the Federal Government and throughout the Nation.
- Consult and coordinate with the Under Secretary for Science and Technology on cybersecurity research and development to strengthen critical information infrastructure against acts of terrorism.

On May 11, 2007, this bill was referred to the Senate Committee on Homeland Security and Governmental Affairs.

Hackers," February 5, 2002, at [http://www.siliconvalley.com/mld/siliconvalley/news/editorial/3070194.htm].

H.R. 3221 — The New Direction for Energy Independence, National Security, and Consumer Protection Act proposes establishment of the Grid Modernization Commission to facilitate the adoption of Smart Grid standards, technologies, and practices across the Nation's electricity grid. The bill was passed in the House on August 4, 2007. On October 19, 2007, there was a unanimous consent request to consider H.R. 3221 in the Senate, but objection was heard.

H.R. 3237 — The Smart Grid Facilitation Act of 2007, proposes to modernize the Nation's electricity transmission and distribution system to incorporate digital information and controls technology. "Smart grid" technology functions will include the ability to detect, prevent, respond to, or recover from cyber-security threats and terrorism. The new Grid Modernization Commission is directed to undertake, and update on a biannual basis, an assessment of the progress toward modernizing the electric system including cybersecurity protection for extended grid systems. On August 24, 2007, the bill was referred to House subcommittee on Energy and Environment.

U.S. Initiatives to Promote Global Internet Freedom: Issues, Policy, and Technology, R41120 (April 5, 2010).

PATRICIA MOLONEY FIGLIOLA, CONGRESSIONAL RESEARCH SERV., U.S. INITIATIVES TO PROMOTE GLOBAL INTERNET FREEDOM: ISSUES, POLICY, AND TECHNOLOGY (2010), *available at* http://www.intelligencelaw.com/library/secondary/crs/pdf/R41120_4-5-2010.pdf.

Patricia Moloney Figliola, Coordinator
Specialist in Internet and Telecommunications Policy
pfigliola@crs.loc.gov

Kennon H. Nakamura
Analyst in Foreign Affairs
knakamura@crs.loc.gov

Casey L. Addis
Analyst in Middle Eastern Affairs
caddis@crs.loc.gov

Thomas Lum
Specialist in Asian Affairs
tlum@crs.loc.gov

April 5, 2010

Congressional Research Service

7-5700
www.crs.gov
R41120

Summary

Modern means of communications, led by the Internet, provide a relatively inexpensive, open, easy-entry means of sharing ideas, information, pictures, and text around the world. In a political and human rights context, in closed societies when the more established, formal news media is denied access to or does not report on specified news events, the Internet has become an alternative source of media, and sometimes a means to organize politically.

The openness and the freedom of expression allowed through blogs, social networks, video sharing sites, and other tools of today's communications technology has proven to be an unprecedented and often disruptive force in some closed societies. Governments that seek to maintain their authority and control

the ideas and information their citizens receive are often caught in a dilemma: they feel that they need access to the Internet to participate in commerce in the global market and for economic growth and technological development, but fear that allowing open access to the Internet potentially weakens their control over their citizens.

Legislation now under consideration in the 111th Congress would mandate that U.S. companies selling Internet technologies and services to repressive countries take actions to combat censorship and protect personally identifiable information. Some believe, however, that technology can offer a complementary and, in some cases, better and more easily implemented solution to some of those issues. They argue that hardware and Internet services, in and of themselves, are neutral elements of the Internet; it is how they are implemented by various countries that is repressive. Also, Internet services are often tailored for deployment to specific countries; however, such tailoring is done to bring the company in line with the laws of that country, not with the intention of allowing the country to repress and censor its citizenry. In many cases, that tailoring would not raise many questions about free speech and political repression.

This report provides information regarding the role of U.S. and other foreign companies in facilitating Internet censorship by repressive regimes overseas. The report is divided into several sections:

- Examination of repressive policies in China and Iran,
- Relevant U.S. laws,
- U.S. policies to promote Internet freedom,
- Private sector initiatives, and
- Congressional action.

Two appendixes describe technologies and mechanisms for censorship and circumvention of government restrictions.

Introduction

In the late 1960s and 1970s, advancements in telecommunications technologies enabled the creation of a large-scale, interconnected network called ARPANET ("Advanced Research Projects Agency Network"). ARPANET was created by the Defense Advanced Research Projects Agency as a government-funded enterprise until the mid-1990s, when it began commercialization. Today's Internet is a direct outgrowth of the technologies developed and lessons learned from ARPANET. During the late 1990s, the Internet began having a significant impact on culture and commerce, including the exponential increase of near instant communication by electronic mail (e-mail), text-based discussion forums, and the graphical World Wide Web.

Today, the Internet has evolved even further and many people are using newer tools, such as blogs, social networks, video sharing sites, and other aspects of

today's communications technology to express their political ideals, many times in conflict with the political opinions and outlook espoused by their governments. In this way, the Internet has proven to be an unprecedented and often disruptive force in some closed societies, as the governments seek to maintain their authority and control the ideas and information their citizens receive. These regimes are often caught in a dilemma: they need the Internet to participate in commerce in the global market and for economic growth and technological development, but they also seek to restrict the Internet in order to maintain the government's control. Figure 3 illustrates an assessment by Freedom House[4935] of the extent to which selected countries restrict freedom on the Internet.

In Burma during the 2007 Saffron Revolution, YouTube footage, often filmed with cell phone cameras, conveyed to the world the human rights violations against the monks and generated international awareness and reaction. Demonstrations in Tehran following the June 12, 2009, presidential elections were often organized through Twitter and text messages over cell phones.

The Iranian government's violent response to the demonstrations was spread around the world through live cell phone pictures, e-mails, and phone calls. The Voice of America (VOA) reported that during the demonstrations, Iranians sent VOA over 300 videos a day, along with thousands of still pictures, e-mails, and telephone calls to the agency.[4936]

A variety of control mechanisms are employed by regimes seeking to limit the ways the Internet is used, ranging from sophisticated surveillance and censorship to threats of retaliation (which foster self-censorship) and actual harassment and arrests of Internet users. Such regimes often require the assistance of foreign Internet companies operating in their countries. These global technology companies find themselves in a dilemma. They often must choose between following the laws and the requests of authorities of the host country, or refusing to do so and risking the loss of business licenses or the ability to sell services in that country. Human rights groups have protested that Yahoo! and Google censor and remove material deemed sensitive by host governments on country-specific search engines.[4937] Microsoft is said to censor Chinese versions of its blog

---

[4935] Freedom House is an independent watchdog organization that supports the expansion of freedom around the world. Freedom House supports democratic change, monitors freedom, and advocates for democracy and human rights. More information can be found on its website, http://www.freedomhouse.com.

[4936] Danforth Austin, Director, Voice of America, testimony before the Subcommittee on Europe, House Committee on Foreign Affairs, Washington, July 23, 2009.

[4937] Lucie Morillon, Washington Director of Reporters Without Borders, Testimony before the Tom Lantos Human Rights Commission, U.S. House of Representatives, Washington, June 18, 2009.

platforms.[4938] Human rights groups also charge that Yahoo! has provided Chinese authorities personal identifying information about users that has allowed the government to identify and arrest individuals for statements made on the Web.[4939] A representative of Google, Inc. acknowledged the problem of government involvement, noting

> *As our ... Burma experiences indicate, our products are platforms for free expression, transparency, and accountability. Because of this, we often face efforts by governments throughout the world to restrict or deny access to our products.*[4940]

The Global Online Freedom Act of 2009 (GOFA) (H.R. 2271), introduced by Representative Christopher Smith, would mandate that companies selling Internet technologies and services to repressive countries take actions to combat censorship and protect personally identifiable information. Some believe, however, that technology can offer a complementary and, in some cases, better and more easily implemented solution to prevent government censorship. Hardware and Internet services, in and of themselves, are neutral elements of the Internet; it is how they are implemented by various countries that makes Internet access "repressive."

For example, hardware, such as routers, is needed to provide Internet service everywhere. However, hardware features intended for day-to-day Internet traffic management, conducted by Internet service providers (ISPs) and governments for benign purposes, can be misused. Repressive governments are able to use these features to censor traffic and monitor use— sometimes using them to identify specific individuals for prosecution. It is not currently feasible to remove those features from the product, even when sold to countries that use those features to repress political speech.[4941]

On the other hand, Internet services, such as Google, are often tailored for deployment to specific countries. Such tailoring is done to bring the company's products and services in line with the laws of that country, and not with the end goal of allowing the country to repress and censor its citizenry. In many cases, tailoring does not raise many questions about free speech and political repression because the country is not considered to be a repressive regime. Under Canadian

---

[4938] Ibid.

[4939] Ibid.

[4940] Nicole Wong, Deputy General Counsel, Google, Inc., Testimony before the U.S. Senate Judiciary Committee's Subcommittee on Human Rights and the Law, Washington, May 20, 2008.

[4941] Testimony of Mark Chandler, Cisco Systems, before the Senate Committee on the Judiciary Subcommittee on Human Rights and the Law, May 2, 2008.

human rights law, for example, it is illegal to promote violence against protected groups; therefore, when reported, Google.ca will remove such links from search results.[4942]

Internet censorship and the prosecution of individuals who attempt to circumvent that censorship are unlikely to be eliminated in some countries. However, while some governments are continually looking for new and more thorough methods to restrict or inhibit Internet use, citizens in these countries are active in developing techniques to circumvent those efforts.

Examples of Countries Charged with Restricting Internet Freedom

The organization Reporters Without Borders has listed 15 countries where Internet freedom is restricted. These countries are China, Cuba, North Korea, Belarus, Myanmar, Egypt, Ethiopia, Iran, Saudi Arabia, Syria, Tunisia, Turkmenistan, Uzbekistan, Vietnam, and Zimbabwe.[4943] This report covers two of these countries, China and Iran, both of which have been in the news during 2009 and 2010.

China[4944]

The People's Republic of China (PRC) has the world's largest number of Internet users, estimated at 330 million people, including 70 million bloggers. It also has one of the most sophisticated and aggressive Internet censorship and control regimes in the world. According to some estimates, between 30 and 40 Chinese citizens are serving prison sentences for writing about politically sensitive topics online.[4945] In November 2009, Huang Qi, a human rights advocate, was sentenced to three years in prison for "possessing state secrets" after posting online appeals and complaints of families whose children had been killed in school buildings during the Sichuan earthquake of May 2008. Some studies show that the vast majority of Internet users in China do not view the medium as a political tool.[4946] Nonetheless, Chinese Internet users are able to access unprecedented amounts of information, despite government attempts to limit the

---

[4942] Testimony of Nicole Wong, Google, op. cit. May 2, 2008.

[4943] See Reporters Without Borders, "Handbook for Bloggers and Cyber-Dissidents," http://www.rsf.org/IMG/pdf/ guide_gb_md-2.pdf.

[4944] Prepared by Thomas Lum, Specialist in Asian Affairs, 7-7616.

[4945] U.S. Department of State, 2008 Human Rights Report: China, February 25, 2009; PEN American Center, "Failing to Deliver: An Olympic-Year Report Card on Free Expression in China," July 8, 2008.

[4946] Rebecca MacKinnon, "Bloggers and Censors: Chinese Media in the Internet Age," China Studies Center, May 18, 2007.

flow, while political activists and others continue to push back against restrictions and find ways to circumvent censorship.

PRC officials have argued that Internet controls are necessary for social stability and that new restrictions target pornography and other "harmful content."[4947] Chinese official commentary has suggested that the U.S. government has applied a double standard, regulating the Internet at home while calling for other countries to eliminate controls. The PRC government also has referred to

U.S. criticism of Internet restrictions in China as politically motivated and an interference in China's domestic affairs.[4948]

The PRC government employs a variety of methods to control online content and expression, including website blocking and keyword filtering; regulating and monitoring Internet service providers, Internet cafes, and university bulletin board systems; registering websites and blogs; and occasional arrests of high-profile "cyber dissidents" or crackdowns on Internet service providers.[4949] Some analysts argue that even though the PRC government cannot control all Internet content and use, its selective targeting creates an undercurrent of fear and promotes self-censorship. Blocked websites, social networking sites, and file sharing sites include Radio Free Asia, international human rights websites, many Taiwanese newspapers, Facebook, Twitter, and YouTube. The government reportedly has hired thousands of students to express pro-government views on websites, bulletin boards, and chat rooms.[4950] Furthermore, some analysts argue that the Internet has enhanced government propaganda and surveillance capabilities.

Nonetheless, the Internet has made it impossible for the Chinese government to restrict information as fully as before; bulletin boards, comment boards, chat rooms, blogs, and other outlets have allowed for an unprecedented amount of information and public comment on social and other issues. Although the state has the capability to block news of events or to partially shut down the Internet, as it did in Xinjiang following ethnic unrest that erupted there in July 2009, it often cannot do so before such events are publicized, if only fleetingly, online. The threat of public exposure or condemnation through the Internet reportedly

---

[4947] Kim Zetter, "China Stands Firm in Response to Google Threat," Wired, January 14, 2010.

[4948] Gillian Wong, "China Denies Involvement in Google Hackings," Associated Press, January 25, 2010.

[4949] Some experts estimate that the PRC government has employed 30,000 "Internet police." "On the Wrong Side of Great Firewall of China," New Zealand Herald, November 27, 2007.

[4950] David Bandurski, "China's Guerrilla War for the Web," Far Eastern Economic Review, Vol. 171, no. 5 (July/August 2008).

has compelled some government officials to conduct affairs more openly. For Chinese Internet users in search of censored information, circumventing government controls is often made possible by way of "proxy servers" or "virtual private networks" using special software.[4951] Furthermore, English language news sites, such as the New York Times and the Washington Post, are generally available.

U.S. Internet Companies, China, and Human Rights Issues

Some human rights activists and U.S. policy makers have expressed concern that U.S. Internet companies have sold Internet services or technologies to China that have assisted the PRC government in restricting information and communication and in monitoring and identifying Internet users. U.S. congressional committees and commissions have held hearings on the topics of global Internet freedom and the roles of U.S. Internet and technology companies in China's censorship regime. Some media watchdog groups and Members of Congress have maintained that some U.S. information technology companies, including Yahoo!, Microsoft, Google, and Cisco Systems, have provided willing, direct, sustained, or comprehensive support to PRC Internet censorship and political control efforts.[4952]

U.S. information technology companies have responded that they must abide by the laws of the countries in which they operate, and that they are not actively cooperating or collaborating with the PRC government or tailoring their products to suit PRC censorship requirements.[4953] These companies add that despite PRC censorship policies, they nonetheless are enlarging the volume of information

---

[4951] Such software is available internally and through foreign sources, including the U.S. government.

[4952] The Tom Lantos Human Rights Commission, "The State of Global Internet Freedom," June 18, 2009; U.S. Congress, Senate Committee on the Judiciary, Subcommittee on Human Rights and the Law, Global Internet Freedom: Corporate Responsibility and the Rule of Law, May 20, 2008. U.S. Congress, House Committee on International Relations, Subcommittee on Africa, Global Human Rights and International Operations and Subcommittee on Asia and the Pacific, The Internet in China: A Tool For Freedom or Suppression?, February 15, 2006.

[4953] Cisco's general counsel argued that Cisco does not customize its equipment for China; filtering technologies that are intrinsic to Cisco products cannot feasibly be eliminated; Cisco has a written code of conduct that aims to prevent the modification of its products in foreign countries in such as way as to undermine human rights; and Cisco complies with all U.S. government regulations or export controls that restrict the sale of high tech products and crime detection equipment. See Anne Broache, "Senators Weigh New Laws over China Online Censorship," news.cnet.com, May 20, 2008; Mark Chandler, Cisco Systems, Testimony before the Senate Committee on the Judiciary, Subcommittee on Human Rights and the Law, May 20, 2008; Mark Chandler, Cisco Systems, Testimony before the Subcommittee on Africa, Global Human Rights and International Operations and the Subcommittee on Asia and the Pacific of the Committee on International Relations, February 15, 2006.

available in China and other Internet-restricting countries, and can better press for freedom of expression and protection of privacy while located in these countries. They also claim that Chinese and other Asian and European competitors would fill the void in providing Internet services and technology in their absence. Furthermore, some Chinese experts have suggested that overall, the Internet, including foreign involvement, has created greater political freedom, despite the ongoing battle against growing PRC government attempts to control it.[4954]

Yahoo!

Yahoo! has been blamed for complicity in the arrests of at least four Chinese Internet users by providing their e-mail account information to PRC authorities. In the most high-profile case, in 2004, Yahoo!'s Hong Kong office was accused of having provided information about the identity of a Chinese journalist and Yahoo! e-mail account holder, Shi Tao. Shi reportedly had forwarded information about state policy regarding the 15th anniversary of the Tiananmen demonstrations via his Yahoo! e-mail account to an overseas democracy group.[4955] In March 2005, a PRC court sentenced Shi to 10 years in prison for "leaking state secrets." In August 2005, Yahoo! bought a 39% stake in China's Alibaba Group, a Chinese Internet service provider, and turned over its PRC operations to the Chinese company.

Microsoft

In 2005, Microsoft shut down the MSN Spaces site of Chinese political blogger Zhao Jing (a.k.a. Michael Anti) at the request of the PRC government, after Zhao had expressed support in his blog for a boycott of Beijing News following the firing of one of its editors. Human rights activists also criticized Microsoft for blocking words such as "democracy" from MSN Spaces. Microsoft was China's leading blog service provider at the time and remains one of the most popular. Recently, Microsoft also has been accused of cooperating with China's censorship policies in the development of its new Bing search engine.[4956]

Google

Google's activities in China have reflected an attempt by the company to comply with PRC policies while limiting the company's role in censorship. Google's

---

[4954] "Isaac Mao and Michael Anti at Hong Kong U.," April 17, 2007, http://rconversation.blogs.com/rconversation/2007/ 04/isaac_mao_and_m.html.

[4955] Peter S. Goodman, "Yahoo Says it gave China Internet Data," Washington Post, September 11, 2005.

[4956] Christine Chiao, "Microsoft Erases Anti-Blog," AsiaMedia, January 17, 2006.

Chinese search engine, Google.cn, reportedly is the second-most widely used information-gathering service in China after that of Baidu, a Chinese company, and is the least censored, according to one study.[4957] Google.cn provides a message stating that a website is unavailable due to "local laws, regulations, and policies," suggesting to the user that additional information exists, but that the government has closed access to that site. In 2006, Google reportedly moved its search records outside of the PRC in order to prevent the government from accessing the data without the company's consent, and does not host Gmail and Blogger services in China as a measure to protect the privacy of Chinese account holders.[4958]

Ever since it entered the China market in 2005, Google and the PRC government have clashed over censorship and other issues, although the company has complied with Chinese laws in principle. In June 2009, China's Foreign Ministry accused the Internet company of violating PRC law and enabling Chinese Internet users to access "vulgar content." Google's Chinese service was disrupted for a few days, which some analysts viewed as the Chinese government response to Google's apparent resistance to abide by new censorship edicts.[4959] Chinese writers accused Google of copyright infringement after the company began publishing their works in its online library, Google Books.[4960] In October 2009, the People's Daily, the state's premier newspaper, accused Google of blocking its stories of the dispute.

Cisco Systems

Cicso Systems, Juniper Networks, Nortel of Canada, and Alcatel of France reportedly were involved in upgrading China's Internet infrastructure, filtering, and surveillance systems earlier this decade. According to some reports, Cisco Systems sold several thousand routers to China, which helped to facilitate the PRC government's censorship of Internet content and monitoring of Internet

---

[4957] Google's Chinese service, with roughly 80 million customers and 30 million Gmail accounts, has captured 20%-30% of the PRC market, compared to Baidu, which has over 60%. Tom Krazit, "Google's Censorship Struggles Continue in China," news.cnet.com, June 16, 2009; Steven Mufson, "China Faces Backlash from 'Netizens' if Google Leaves," Washington Post, January 13, 2010.

[4958] Robert McMillan, "Google Moving Search Records Out of China," InfoWorld, March 1, 2006; Rory Cellan-Jones, "China and Google: What's Going On," BBC – Dot.Life, June 25, 2009; James Mulvenon, "The Rule of Law in China: Incremental Progress," The China Balance Sheet in 2007 and Beyond, Center for Strategic and International Studies, May 2007.

[4959] Claudine Beaumont, "China Accuses Google of Spreading 'Vulgar Content,'" Telegraph.co.uk, June 25, 2009.

[4960] "Google Apologizes to Chinese Writers," Agence France Presse, January 11, 2010.

users.[4961] According to other reports, Cisco sold technology to China's police force that can be used in the collection and use of data regarding personal background and imaging information, Web browsing history, and e-mail.[4962]

The Continuing Battle Between Censorship and Freedom of Information

The PRC government has displayed a growing nervousness about the Internet's influence on Chinese society and politics, but it has been reluctant to provoke the ire of China's online population or to reduce the attractiveness of China's business environment for foreign investors. In June 2009, the PRC government issued a directive requiring "Green Dam Youth Escort" software, designed to prevent children from accessing "harmful content," such as pornography, on all Chinese computers sold after July 1, 2009, including those imported from abroad. Many Chinese Internet users, international human rights activists, foreign governments, chambers of commerce, and information technology manufacturers openly opposed the policy, arguing that the software would undermine computer operability, that it could be used to expand censorship to include political content, and that it could incorporate pirated software and weaken Internet security.[4963] On June 30, 2009, the PRC government announced that mandatory installation of the software would be delayed for an indefinite period. On August 14, 2009, Minister of Industry and Information Technology Li Yizhong stated that the directive had created misunderstandings and that, "We will listen to the public's views before issuing a new directive on Green Dam."[4964]

Following the aborted launch of "Green Dam," the PRC government has continued to tighten controls over Internet content and use, but in a quieter manner. In September 2009, PRC authorities issued requirements that new users register their true identities. This regulation reportedly has not been well enforced; however, the government can still track down individuals through their IP addresses. In December 2009, new restrictions aimed at cracking down on pornography, media piracy, and threats to national security and stability resulted in the closing of hundreds of websites, many of them entertainment-oriented. Furthermore, the China Internet Network Information Center announced that individuals could no longer apply for ".cn" domain names (China's country code),

---

[4961] Jonathan Mirsky, "China's Tyranny Has the Best Hi-Tech Help Censoring the Internet," International Herald Tribune, January 16, 2006.

[4962] Steven Mufson, "China Turning to Technology to Hold onto Power," Washington Post, April 16, 2006; U.S. Congress, "The Internet in China: A Tool for Freedom or Suppression?" op. cit.

[4963] In January 2010, a U.S. software firm filed a lawsuit against the Chinese government for copyright infringement, unfair competition, and other legal violations in connection with the Green Dam program. Agence France-Presse, "U.S. Software Firm Sues Chinese Government for US$2.2 Billion," South China Morning Post, January 6, 2010.

[4964] "Green Dam Launch 'Not Handled Well'," http://www.chinaview.cn, August 14, 2009.

which it would now limit to registered business enterprises. Some observers argued that these policies could dampen the richness and vibrancy of Internet content and activity in China, as well as provoke a public backlash.[4965] On October 15, 2009 (Internet Human Rights Day), 15 Chinese intellectuals issued a Declaration of Internet Human Rights calling for freedom of opinion, speech, and publication online.[4966]

Google and Cyber Attacks

In January 2010, Google threatened to cease censoring its Chinese search engine or to pull out of China. The company asserted that, in December 2009, Chinese hackers had attacked its Gmail service and corporate network as well as the computer systems of many other large U.S. corporations in the PRC.[4967] Hackers appeared to have targeted the Gmail accounts of Chinese human rights activists; the intellectual property, including "source codes" or programming languages, of Google and other companies; and information on U.S. weapons systems. In a statement, Google's chief legal officer announced that the company would no longer censor results on Google.cn, even if that meant having to shut down the search engine, and potentially its offices in China.[4968] Yahoo!, which was also hit by Chinese hackers, expressed support for Google's actions, thereby provoking an angry response by its PRC partner, Alibaba.

Chinese discussion boards and micro-blog postings indicated that a small majority of China's online population—and perhaps a large majority of its most active Internet users—wanted Google to stay in China, with some supporting Google's challenge to the PRC government. A significant minority adopted a pro-government stance or interpreted Google's move as profit-oriented.[4969] According

---

[4965] Rebecca MacKinnon, "China Tightens Internet Controls in the Name of Fighting Porn, Piracy, and Cybercrime," Rconversation , December 14, 2009, http://rconversation.blogs.com; Sharon LaFraniere, "China Imposes New Internet Controls," New York Times, December 18, 2009.

[4966] Rconversation, October 10, 2009, http://rconversation.blogs.com/rconversation/china/index.html.

[4967] Estimates of the number of U.S. information technology, finance, defense, and other companies targeted in this attack ranged from 20 to 34.

[4968] Google representatives stated that two Gmail accounts appeared to have been accessed but that the content of e-mail communications had not been breached. "Statement from Google: A New Approach to China," Washington Post, January 12, 2010. See also "A New Approach to China," The Official Google Blog, January 12, 2010, http://googleblog.blogspot.com/2010/01/new-approach-to-china.html.

[4969] Jessica E. Vascellaro and Aaron Back, "Fallout from Cyber Attack Spreads—Google Investigates China Employees; Rift Emerges Between Yahoo! and Alibaba," Wall Street Journal, January 19, 2010; Rebecca MacKinnon, "Google Puts Its Foot Down," RConversation, http://rconversation.blogs.com/rconversation/china/index.html, January 13, 2010.

to some analysts, although China has huge potential, the company currently earns an estimated $300 million to $400 million from its China operations, a "tiny fraction" of its $22 billion in sales worldwide.[4970]

While visiting Shanghai during his state visit to China in November 2009, President Barack Obama expressed support of unrestricted Internet access and disapproval of censorship. On January 21, 2010, in a policy speech on Internet freedom, Secretary of State Hillary Clinton urged U.S. Internet companies to oppose censorship in their overseas operations and announced that the Global Internet Freedom Taskforce (GIFT) would be reinvigorated. She also called upon the PRC government to conduct a thorough investigation of the December 2009 cyberattacks upon U.S. companies in China and to make its results transparent. Beijing denied involvement in the attacks and defended its Internet policies. The Foreign Ministry stated that foreign companies, including Google, "should respect the laws and regulations, respect the public interest of Chinese people and China's culture and customs and shoulder due social responsibilities."[4971]

Iran[4972]

The Iranian government has restricted Internet usage since access spread beyond universities and government agencies to the general population in the late 1990s. Today, Iran has an estimated 23 million Internet users,[4973] and watchdog groups and Internet activists claim that Iran's filtering and monitoring of usage is among the most extensive in the world. Additional information about Iran's Internet policies is available from the U.S. Department of State in its annual report, *2008 Country Reports on Human Rights Practices*.

The Iranian government tracks online communication and content through a centralized location in the state's telecommunications monopoly, the Ministry of Communications and Information Technology (MCIT). In addition to its 23 million Internet users, the Persian blogosphere is among the world's most robust. The status of Internet sites and blogs remains contested under Iranian law, but

---

[4970] Miguel Helft, "For Google, A Threat to China with Little Revenue at Stake," New York Times, January 15, 2010.

[4971] "Clinton Urges Global Internet Freedom," VOA News.com, January 21, 2010; Gillian Wong, "China Denies Involvement in Google Hackings," Washington Post, January 25, 2010; "China Says Google 'No Exception to Law'," Embassy of the People's Republic of China in the United States, January 19, 2010.

[4972] Prepared by Casey Addis, Analyst in Middle Eastern Affairs, 7-0846.

[4973] "ITU Internet Indicators 2008," International Telecommunications Union, http://www.itu.int/ITU-D/icteye/Reporting/ShowReportFrame.aspx?ReportName=/WTI/InformationTechnologyPublic&RP_intYear=2008&RP_intLanguageID=1.

the Press Law does require that bloggers obtain licenses, and all content on websites and blogs is subject to approval of the Ministry of Culture and Islamic Guidance (MCIG). The government also regulates access to the Internet by limiting the speed of Internet access that ISPs can provide to households and public access sites (Internet cafes) to 128 kilobytes per second, making it difficult or impossible to download multimedia content. Iran reportedly is the only country to have imposed a cap on Internet access speed for households.[4974] Iran also has arrested numerous activists, bloggers, and journalists on charges of "antigovernment publicity," "propaganda against the Islamic Republic," and "jeopardizing national security."[4975]

The government has disabled the Internet altogether in the past, usually during elections, but some observers argue that improvements in monitoring and filtering technologies have made such measures unnecessary and even enabled the government to use the Internet to disseminate disinformation and pro-government content. Following the disputed 2009 presidential election, the Internet was reportedly slow but accessible. The number of detentions of Internet activists and bloggers increased during the post-election unrest, arguably demonstrating the extent of government filtering and monitoring of usage. The post-election crackdown on Internet freedom raised concerns that Iran's human rights abuses were being aided by Western technology companies. Others said the concerns were being overstated, asserting that Iran also develops its own filtering and monitoring technologies.

The Nokia Siemens Network (NSN)[4976] sold communication monitoring equipment to the Iranian government in 2008.[4977] The monitoring center, installed into the MCIT gateway, was part of a larger contract with Iran that included mobile phone network technology. The Iranian government had reportedly experimented with the monitoring equipment prior to the election, but did not use it extensively until after the election. Some experts have argued that the nature of the content inspection happening in Iran since the election goes beyond the practices of other countries, including China.[4978]

[4974] "Speed Reduced for High Speed Internet in Iran," BBC Persian, October 20, 2006.

[4975] See the U.S. State Department "2008 Human Rights Report: Iran," http://www.state.gov/g/drl/rls/hrrpt/2008/nea/ 119115.htm.

[4976] NSN is a joint venture between the Finnish cell phone maker Nokia and the German company Siemens.

[4977] Stuart Smith, "Politics of Marketing: Why Brands Continue to Surf the Recession," Marketing Week (London), August 13, 2009.

[4978] See Christopher Rhoads and Loretta Chao, "Iran's Web Spying Aided by Western Technology," Wall Street Journal, June 22, 2009.

NSN maintains that it sold the technology for the purpose of "lawful intercept" of information used to track criminals and terrorists.[4979] Critics argue that in a country like Iran, where the population is heavily reliant on Internet communication with the outside world due to censorship of other communication, this technology enables the government to intensify repression.[4980]

U.S. Law and Internet Freedom Abroad[4981]

In response to laws and regulations of foreign countries requiring censorship and disclosure of users' personal information, some U.S. technology firms engage in Internet censoring and filtering. Some examples include China and other Internet-restricting countries such as Iran. In some cases, such as in Iran, Internet censoring and filtering reportedly involve a practice often called deep packet inspection which is under a great deal of scrutiny in the United States.[4982] Doing business in a foreign country subjects the business to the jurisdiction of that country.[4983] Nonetheless, concerns have been raised that China's Internet filtering could run afoul of world trade obligations.[4984]

U.S. Policy for the Promotion of Internet Freedom Abroad[4985]

The importance of Internet freedom to the United States was declared in 2006. During an explanation of that year's State Department 2006 Country Reports on Human Rights Practices, then-Under Secretary of State for Democracy and Global Affairs Paula J. Dobriansky explained that the 2006 reports included new, additional focus on "the extent to which internet access is available to and used

---

[4979] Nokia Siemens Networks, "Provision of Lawful Intercept Capability in Iran," June 22, 2009, http://www.nokiasiemensnetworks.com/press/press-releases/provision-lawful-intercept-capability-iran.

[4980] Eli Lake, "Fed Contractor, Cell Phone Maker Sold Spy System to Iran," Washington Times, April 13, 2009.

[4981] Prepared by Gina Stevens, Legislative Attorney, 7-2581.

[4982] Deep Packet Inspection ("DPI") is a computer network packet filtering technique that involves the inspection of the contents of data packets as they are transmitted across the network.

[4983] Many foreign countries have privacy laws that may be applicable to Internet Service Providers, websites, etc. See Morrison & Foerster's Privacy Library for the text of privacy laws in other countries, in the U.S., and for multinational organizations, http://www.mofoprivacy.com/default.aspx?tabNum=2.

[4984] See Andrew Noyes, "Chinese Demands for Web Filtering Software Cause a Stir," CongressDailyAM, June 25, 2009; Tim Wu, "The World Trade Law of Censorship and Internet Filtering," Chi. J. Int'l L., vol. 7 (2006-07).

[4985] Prepared by Kennon H. Nakamura, Analyst in Foreign Affairs, 7-9514.

by citizens in each country and … whether governments inappropriately limit or block access to the internet or censor websites."[4986] This was added as an area of concern because the internet is playing a growing role in people's ability to freely express themselves and in the free flow of information. In discussing this new area of focus, then-Under Secretary Dobriansky said,

> *We will continue to defend internet freedom, including by addressing internet repression directly with the foreign governments involved and seeking to persuade foreign officials that restricting internet freedom is contrary to their own interests and that of their countries. The new information in this year's reports will make an important contribution.*[4987]

At this same time, then-Secretary of State Condoleezza Rice also established the Global Internet Freedom Task Force (GIFT) in order to provide a U.S. foreign policy response to violations of Internet freedom by repressive regimes around the world.[4988]

Secretary of State Hillary Rodham Clinton, in a January 21, 2010, speech, stated that Internet freedom is a central part of U.S. foreign policy. She stated that Internet freedom is more than a question of information freedom, it is about the nature of the world we want to inhabit. Clinton further stated: "It's about whether we live on a planet with one Internet, one global community, and a common body of knowledge that benefits and unites us all, or a fragmented planet in which access to information and opportunity is dependent on where you live and the whims of censors."[4989]

In her remarks, Secretary Clinton placed the United States on the side of a single Internet where everyone has equal access to knowledge and ideas. She noted that blogs, e-mails, social networks, and text messages are opening up a new virtual town square where citizens can go to criticize their governments and exchange ideas. U.S. responsibility to support this new "town square" is not new but can be found in the First Amendment of the U.S. Bill of Rights ensuring freedom of speech, assembly, and religion. Secretary Clinton argued that these principles

---

[4986] Under Secretary of State for Democracy and Global Affairs Paula Dobriansky, AOn-The-Record Briefing on the State Department=s 2006 Country Reports on Human Rights Practices,@ Washington, March 6, 2007, http://www.state.gov/g/ drl/rls/rm/2007/81468.htm.

[4987] Ibid.

[4988] U.S. Mission to the United Nations in Geneva, "Secretary of State Establishes New Global Internet Freedom Task Force," press release, February 14, 2006, http://geneva.usmission.gov/Press2006/02141InternetTaskForce.html.

[4989] Secretary of State Hillary Rodham Clinton, "Remarks on Internet Freedom," January 21, 2010, http://www.state.gov/ secretary/rm/2010/01/135519.htm.

were reaffirmed in President Franklin Roosevelt's "The Four Freedoms" speech,[4990] and in the work of the United States and its support of the Universal Declaration of Human Rights.

Secretary Clinton further explained that U.S. foreign policy is premised on the idea that no country stands to benefit more than the United States when there is cooperation among peoples and states. No country shoulders a heavier burden than the United States when conflict and misunderstanding make the international system unstable, and force people and countries apart. She stated that it is important that the United States seizes the opportunities that come with interconnectivity and work for a world in which access to networks and information brings people closer together and expands the definition of the global community.

Secretary Clinton continued the GIFT and its responsibilities. The Task Force is co-chaired by the Under Secretaries of State for Democracy and Global Affairs and for Economic, Business, and Agricultural Affairs and draws on the State Department's multidisciplinary expertise in its regional and functional bureaus to work on issues such as international communications, human rights, democratization, business advocacy and corporate social responsibility, and country specific concerns. The task force supports Internet freedom by[4991]

- monitoring Internet freedom and reporting in its annual Country Reports on Human Rights Practices the quality of Internet freedom in each country around the world;
- responding in both bilateral and international fora to support Internet freedom; and
- expanding access to the Internet with greater technical and financial support for increasing availability of the Internet in the developing world.

In advancing Internet freedom as an objective of U.S. foreign policy, Secretary Clinton proposed a number of key initiatives:[4992]

- Continue the work of the State Department's GIFT as it oversees U.S. efforts in more than 40 countries to help individuals circumvent politically motivated censorship by developing new tools and providing the training needed to safely access the Internet;

[4990] On January 6, 1941, President Franklin Roosevelt addressed Congress saying that "we look forward to a world founded upon four essential human freedoms." These essential freedoms, which he referred to as the "Four Freedoms" are (1) freedom or speech and expression, (2) freedom of religion, (3) freedom from want, and (4) freedom from fear.

[4991] The GIFT Strategy is available online at http://2001-2009.state.gov/g/drl/rls/78340.htm.

[4992] Hillary Rodham Clinton, "Remarks on Internet Freedom," op. cit.

- Make Internet freedom an issue at the United Nations and the U.N. Human Rights Council in order to enlist world opinion and support for Internet Freedom;
- Work with new partners in industry, academia, and non-governmental organizations to establish a standing effort to advance the power of "connection technologies" that will empower citizens and leverage U.S. traditional diplomacy;
- Provide new, competitive grants for ideas and applications that help break down communications barriers, overcome illiteracy, and connect people to servers and information they need;
- Urge and work with U.S. media companies to take a proactive role in challenging foreign governments' demands for censorship and surveillance; and
- Encourage the voluntary work of the communications-oriented, private sector-led Global Network Initiative (GNI). The GNI brings technology companies, nongovernmental organizations, academic experts, and social investment funds together to develop responses and mechanisms to government requests for censorship.

To fund U.S. efforts in support of Internet freedom, Congress in FY2008 appropriated $15 million, most of which has been spent or is obligated. Another $5 million was appropriated in FY2009. Finally, in Secretary Clinton's January 21 speech, she spoke of an additional $15 million for FY2010 that has been allocated from State Department appropriations to a range of programs that, in full or in part, support Internet freedom. Assistant Secretary for Democracy, Human Rights, and Labor Michael Posner describes these programs as "not just circumvention.... [I]t's a lot about training people.... It's some about technology. It's some about encouraging groups that are in danger. It's a lot about diplomacy, too, for us getting out there and being sure that when groups are in trouble, we provide a lifeline."[4993]

The U.S. Broadcasting Board of Governors' International Broadcasting Bureau also supports counter-censorship technologies and has committed approximately $2 million per year to help enable Internet users in repressive regimes to have access to the VOA and other U.S. governmental and non-governmental websites and to receive VOA e-mail newsletters.

Some observers have expressed concerns that there could be serious negative consequences for U.S. and foreign companies, and U.S. or foreign nationals working or living in countries with repressive regimes, if they follow the expanded U.S. policy supporting Internet freedom. These commenters point out

---

[4993] Assistant Secretary of State for Democracy, Human Rights, and Labor Michael H. Posner, "Briefing on Internet Freedom and 21st Century Statecraft," January 22, 2010, http://www.state.gov/g/drl/rls/rm/2010/134306.htm.

that repressive governments could punish or make an example of an individual or company for not following the dictates of that country. Such actions could include harassment, lifting of business licenses, confiscation of assets, or imprisonment. These observers question what powers, beyond expressing U.S. displeasure through official demarches and public statements or through negotiations, that the United States may have to respond to such actions.[4994]

Congressional Action

In 2010, Congress has taken steps to address ongoing concerns about ensuring the free and secure flow of information over the Internet:

- On March 10, 2010, the House Committee on Foreign Affairs conducted a hearing, "The Google Predicament: Transforming U.S. Cyberspace Policy to Advance Democracy, Security, and Trade," on the December 2009 Chinese cyber attacks on Google and other U.S. companies, to consider policy tools to address Internet freedom, trade, and cyber security issues;
- On March 9, 2010, Representatives David Wu and Christopher Smith announced the formation of the House Global Internet Freedom Caucus; and
- The Senate Judiciary Committee, Subcommittee on Human Rights and the Law, held a hearing on March 2, 2010, entitled "Global Internet Freedom and the Rule of Law, Part II" to examine human rights, corporate responsibility, and other issues related to Internet censorship around the world.

The Global Network Initiative: Private Sector Support of Internet Freedom[4995]

The Global Network Initiative (GNI) was formed in October 2008 to respond to criticism of Internet service providers and computer manufacturers who had sold technology or services to Internet-restricting countries.[4996] GNI was launched by a coalition of human rights organizations, academics, investors and technology leaders. GNI adopts a self-regulatory approach to protect and advance individuals' rights to free expression and privacy on the Internet. A set of principles and supporting mechanisms provide guidance to the information and communications technology (ICT) industry and its stakeholders on how to protect and advance the human rights of freedom of expression and privacy when

---

[4994] Questions following Secretary of State Hillary Clinton's Remarks on Internet Freedom, January 21, 2010, http://www.state.gov/secretary/rm/2010/01/135519.htm, and questions following Assistant Secretary of State Michael Posner's "Briefing on Internet Freedom and 21st Century Statecraft," January 22, 2010, http://it.tmcnet.com/news/2010/ 01/26/4590599.htm.

[4995] Originally prepared by Gina Stevens, Legislative Attorney, 7-2581.

[4996] See http://www.globalnetworkinitiative.org/.

faced with pressures from governments to take actions that infringe upon these rights.

Governments are not members of the GNI, but are encouraged to support the principles and encourage their adoption. Organizations participating in the GNI include Google Inc., Microsoft Corp., and Yahoo! Inc. Each initial participating company committed $100,000 per year over the two-year start-up period. Organizations not participating in the initiative who where involved in its development include Amnesty International and Reporters Without Borders. Reporters Without Borders remains skeptical about how much change GNI can effect, and pushed for standards that would require all government requests and takedown notices be made in writing.

The GNI's Principles on Freedom of Expression and Privacy ("the Principles") are based on internationally recognized laws and standards for human rights, including the Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR) and the International Covenant on Economic, Social, and Cultural Rights.

The GNI acknowledges that the rights of privacy and of freedom of expression should not be restricted by governments, except in narrowly defined circumstances based on internationally recognized laws or standards. The Implementation Guidelines ("The Guidelines") of the GNI provide guidance to ICT companies on how to implement the Principles, and describe the actions that constitute compliance.

With respect to government demands to remove or limit access to content or restrict communications, participating companies commit to encourage governments to

- be specific, transparent, and consistent in the demands issued to restrict freedom of expression online;
- encourage government demands that are consistent with international laws and standards;
- require governments to follow local legal processes, interpret government demands so as to minimize the negative effect, when required to restrict communications or remove content; and
- interpret the governmental authority's jurisdiction to minimize the negative effect.

Participating companies commit to operate in a transparent manner when required to remove content or restrict access, and must disclose to users the applicable laws and policies requiring such action, the company's policies for responding to government demands, and provide timely notice to users when access to content has been locked or communications limited due to government restrictions. With respect to privacy, participating companies commit to assess

the human rights risks associated with the collection, storage, and retention of personal information and to develop mitigation strategies.

A system of independent third-party assessment of company compliance with the Principles and Implementation Guidelines will be phased in over three stages:

- In Phase One (ends December 2010) each participating company establishes internal policies and procedures to implement the Principles, and the Board approves independence and competence criteria for the selection of independent assessors.
- In Phase Two (2011) independent assessors will conduct process assessments of each participating company to review and evaluate their internal systems for implementing the Principles.
- In Phase Three (January 2012 onwards) the Board will accredit independent assessors to review the internal systems of companies, and company responses to specific government demands implicating freedom of expression or privacy. Each participating company will submit an annual report to the Organization. The assessors will prepare reports explaining each company's responses to government demands, evaluating the effectiveness of the company's responses. Each company will be given the opportunity to respond to the assessor's draft and final report. The Board of the Organization will assess whether the company is in compliance with the Principles and its determination will be made public. The Board of the Organization will publish an annual report assessing each participating company's compliance with the Principles.

Recent Legislative Action[4997]

Public Laws

H.R. 2647, National Defense Authorization Act for Fiscal Year 2010. Introduced by Representative Skelton (by request), referred to the House Armed Services Committee. Enacted October 28, 2009, P.L. 111-84.

Title XII: Matters Relating to Foreign Nations

Subtitle D: VOICE Act -Victims of Iranian Censorship Act or VOICE Act

(Sec. 1242) Expresses the sense of the Senate in support of the universal values of freedom of speech, the press, and expression as it pertains to the people of Iran, and condemns acts of censorship, intimidation, and other restrictions on such freedom in Iran.

[4997] Legislative summaries are taken directly from the Legislative Information Service of the Library of Congress.

(Sec. 1243) States that it shall be the policy of the United States to (1) support freedom of the press, speech, expression, and assembly in Iran; (2) support the Iranian people as they seek, receive, and impart information and promote ideas in writing, print, and through other media; (3) discourage businesses from aiding efforts to interfere with the ability of the Iranian people to access or share information or otherwise infringe upon such freedoms; and (4) encourage the development of technologies that facilitate efforts of the Iranian people to share such information, exercise such freedoms, and engage in Internet-based education programs and other exchanges between U.S. citizens and Iranians.

(Sec. 1244) Authorizes appropriations for the (1) International Broadcasting Operations Fund to expand Farsi language programming and to disseminate accurate and independent information to the Iranian people through radio, television, Internet, cellular telephone, short message service, and other communications; and (2) Broadcasting Capital Improvements Fund to expand transmissions of Farsi language programs to Iran.

(Sec. 1245) Establishes in the Treasury the Iranian Electronic Education, Exchange, and Media Fund to support the development of technologies that will aid the Iranian people in exchanging information and exercising freedom of speech, expression, and assembly. Authorizes appropriations to the Fund.

(Sec. 1246) Directs the President to report annually to Congress on the use of funds authorized under this Subtitle.

(Sec. 1247) Requires the President to (1) direct the appropriate officials to examine claims that non-Iranian companies have provided hardware, software, or other forms of assistance to the government of Iran that has furthered its efforts to filter online political content, disrupt cell phone and Internet communications, and monitor the online activities of Iranian citizens; and (2) report study results to Congress.

(Sec. 1248) Authorizes appropriations to the Secretary of State to document, collect, and disseminate information about human rights in Iran, including abuses since the Iranian presidential election on June 12, 2009.

Bills and Resolutions in the House of Representatives

H.R. 2271, *Global Online Freedom Act of 2009*. Introduced by Representative Christopher Smith and referred to the House Committee on Foreign Affairs; and the House Committee on Energy and Commerce.

Makes it U.S. policy to (1) promote the freedom to seek, receive, and impart information and ideas through any media; (2) use all appropriate instruments of U.S. influence to support the free flow of information without interference or discrimination; and (3) deter U.S. businesses from cooperating with Internet-restricting countries in effecting online censorship.

Expresses the sense of Congress that (1) the President should seek international agreements to protect Internet freedom; and (2) some U.S. businesses, in assisting foreign governments to restrict online access to U.S.-supported websites and government reports and to identify individual Internet users, are working contrary to U.S. foreign policy interests.

Amends the Foreign Assistance Act of 1961 to require assessments of electronic information freedom in each foreign country.

Establishes in the Department of State the Office of Global Internet Freedom (OGIF).

Directs the Secretary of State to annually designate Internet-restricting countries. Prohibits, subject to waiver, U.S. businesses that provide to the public a commercial Internet search engine, communications services, or hosting services from locating, in such countries, any personally identifiable information used to establish or maintain an Internet services account.

Requires U.S. businesses that collect or obtain personally identifiable information through the Internet to notify the OGIF and the Attorney General before responding to a disclosure request from an Internet-restricting country. Authorizes the Attorney General to prohibit a business from complying with the request, except for legitimate foreign law enforcement purposes.

Requires U.S. businesses to report to the OGIF certain Internet censorship information involving Internet-restricting countries.

Prohibits U.S. businesses that maintain Internet content hosting services from jamming U.S.supported websites or U.S.-supported content in Internet-restricting countries.

Authorizes the President to waive provisions of this act: (1) to further the purposes of this act; (2) if a country ceases restrictive activity; or (3) if it is the national interest of the United States.

H.R. 4784,[4998] Internet Freedom Act of 2010. Introduced by Representative Wu and referred to the House Science and Technology Committee, Subcommittee on Research and Science Education.

Directs the National Science Foundation to establish the Internet Freedom Foundation governed by a board of 12 members, with equal representation from

---

[4998] This bill is a substitute for H.R. 4595.

government, academia, and the private sector. The Internet Freedom Foundation shall—

- Award competitive, merit-reviewed grants, cooperative agreements, or contracts to private industry, universities, and other research and development organizations to develop deployable technologies to defeat Internet suppression and censorship; and
- Award incentive prizes to private industry, universities, and other research and development organizations that successfully develop deployable technologies to defeat Internet suppression and censorship.

The Internet Freedom Foundation shall be funded by such sums as may be necessary.

H.Res. 590, *Expressing grave concerns about the sweeping censorship, privacy, and cybersecurity implications of China's Green Dam filtering software, and urging U.S. high-tech companies to promote the Internet as a tool for transparency, freedom of expression, and citizen empowerment around the world*. Introduced by Representative Wu and referred to the House Committee on Foreign Affairs.

Expresses (1) grave concerns about the sweeping censorship, privacy, and cybersecurity implications of China's Green Dam filtering software; and (2) support for the Chinese people in their quest for Internet freedom and free expression.

Calls on (1) the Chinese government to rescind its requirement for Green Dam to be preinstalled on all new computers; and (2) U.S. high-tech companies to promote the Internet as a tool for transparency, freedom of expression, and citizen empowerment around the world.

H.Res. 672, Calling on the Government of the Socialist Republic of Vietnam to release imprisoned bloggers and respect Internet freedom. Introduced by Representative Sanchez and referred to the House Committee on Foreign Affairs. Passed on October 21, 2009.

Supports the right of the citizens of the Socialist Republic of Vietnam to access websites of their choosing and to have the freedom to share and publish information over the Internet.

Calls on Vietnam to (1) repeal Circular 07, Article 88, and similar statutes that restrict the Internet, so as to be in line with the International Covenant on Civil and Political Rights, to which Vietnam is a signatory; (2) become a responsible member state of the international community by respecting individuals' freedom of speech, freedom of press, and freedom of political association; and (3) release all political prisoners, including but not limited to 18 named bloggers and cyber activists.

Appendix A. Technologies Used to Monitor and Censor Web Sites and Web-Based Communications[4999]

Key-Word List Blocking

This is a simple type of filtration where a government drops any Internet packets featuring certain keywords, such as "protest" or "proxy."

Domain Name System (DNS) Poisoning

DNS poisoning intentionally introduces errors into the Internet's directory service to misdirect the original request to another IP address.

IP Blocking

IP Blocking is one of the most basic methods that governments use for censorship, as it simply prevents all packets going to or from targeted IP addresses. This is an easy technology to implement, but it does not address the problem of individual communications between users. This method is used to block banned websites, including news sites and proxy servers that would allow access to banned content, from being viewed.

Bandwidth Throttling

Bandwidth throttling simply limits the amount of traffic that can be sent over the Internet. Keeping data volume low facilitates other methods of monitoring and filtering by limiting the amount of data present.

Traffic Classification

This is a much more sophisticated method of blocking traffic than IP blocking, as governments can halt any file sent through a certain type of protocol, such as FTP. Because the government knows that FTP transfers are most often sent through TCP port 21, they can simply limit the bandwidth available on that port and throttle transfers. This type of traffic-shaping practice is the most common one used by repressive governments today. It is not resource intensive and it is fairly easy to implement.

Shallow Packet Inspection (SPI)

[4999] Prepared by Patricia Moloney Figliola, Specialist in Telecommunication and Internet Policy, 7-2508. Adapted from "The State of Iranian Communication: Manipulation and Circumvention," Morgan Sennhauser, Nedanet, July 2009, http://iranarchive.openmsl.net/SoIC-1.21.pdf; and "Five Technologies Iran is Using to Censor the Web," Brad Reed, Network World, July 2009, http://www.networkworld.com/news/2009/072009-iran-censorship-tools.html.

Shallow packet inspection is a less sophisticated version of the deep packet inspection (DPI) technique (DPI is described below) that is used to block packets based on their content. Unlike DPI, which intercepts packets and inspects their fingerprints (fingerprinting is described below), headers, and payloads, SPI makes broad generalities about traffic based solely on evaluating the packet header. Although shallow packet inspection can't provide the same refined/detailed traffic assessments as DPI, it is much better at handling volume than DPI.

SPI is much less refined than DPI, but it is capable of handling a greater volume of traffic much more quickly. SPI is akin to judging a book by its cover. This method is prone to exploitation by users because they can disguise their packets to look like a different kind of traffic.

Packet Fingerprinting

This is a slightly more refined method of throttling packets than shallow packet inspection, as it looks not only at the packet header but at its length, frequency of transmission, and other characteristics to make a rough determination of its content. In this manner, the government can better classify packets and not throttle traffic sent out by key businesses.

Deep Packet Inspection (DPI) / Packet Content Filtering

DPI is the most refined method that governments have for blocking Internet traffic. As mentioned above, deep packet inspectors examine not only a packet's header but also its payload. For instance, certain keywords can be both monitored and the e-mail containing them can be kept from reaching its intended destination.

This gives governments the ability to filter packets at a more surgical level than any of the other techniques discussed so far. While providing the most targeted traffic monitoring and shaping capabilities, DPI is also more complicated to run and is far more labor-intensive than other traffic-shaping technologies.

Appendix B. Technologies Used to Circumvent Censorship[5000]

Each of the circumvention methods explained below can, in general, be considered an anonymous "proxy server." A proxy server is a computer system or an application program that acts as an intermediary for requests from a user

[5000] Adapted from Reporters Without Borders, "Handbook for Bloggers and Cyber-Dissidents," September 2005, http://www.rsf.org/IMG/pdf/Bloggers_Handbook2.pdf; and The Citizen Lab, "Everyone's Guide to By-Passing Internet Censorship for Citizens Worldwide," University of Toronto, September 2007, http://citizenlab.org/Circ_guide.pdf.

seeking resources from other servers, allowing the user to block access to his or her identity and become anonymous.

Web-Based Circumvention Systems

Web-based circumvention systems are special web pages that allow users to submit a URL and have the web-based circumventor retrieve the requested web page. There is no connection between the user and the requested website as the circumventor transparently proxies the request allowing the user to browse blocked websites seamlessly. Since the web addresses of public circumventors are widely known, most Internet filtering applications already have these services on their block lists, as do many countries that filter at the national level.

Examples: Proxify, StupidCensorhip, CGIProxy, psiphon, Peacefire/Circumventor.

Web and Application Tunneling Software

Tunneling encapsulates one form of traffic inside of other forms of traffic. Typically, insecure, unencrypted traffic is tunneled within an encrypted connection. The normal services on the user's computer are available, but run through the tunnel to the non-filtered computer which forwards the user's requests and their responses transparently. Users with contacts in a non-filtered country can set up private tunneling services while those without contacts can purchase commercial tunneling services. "Web" tunneling software restricts the tunneling to web traffic so that web browsers will function securely, but not other applications. "Application" tunneling software allows the user to tunnel multiple Internet applications, such as e-mail and instant messenger applications.

Examples: Web Tunneling: UltraReach, FreeGate, Anonymizer, Ghost Surf.
Examples: Application Tunneling: GPass, HTTP Tunnel, Relakks, Guardster/SSH.

Anonymous Communications Systems

Anonymous technologies conceal a user's IP address from the server hosting the website visited by the user. Some, but not all, anonymous technologies conceal the user's IP address from the anonymizing service itself and encrypt the traffic between the user and the service. Since users of anonymous technologies make requests for web content through a proxy service, instead of to the server hosting the content directly, anonymous technologies can be a useful way to bypass Internet censorship. However, some anonymous technologies require users to download software and can be easily blocked by authorities.

Examples: Tor, JAP ANON, I2P