Intelligence Community Whistleblower Protections: In Brief

Updated January 18, 2019

Congressional Research Service
https://crsreports.congress.gov
R45345

CRS REPORT
Prepared for Members and
Committees of Congress

Congressional Research Service
Informing the legislative debate since 1914

SUMMARY

R45345

January 18, 2019

Michael E. DeVine
Analyst in Intelligence and National Security

Intelligence Community Whistleblower Protections: In Brief

Whistleblowing is "the act of reporting waste, fraud, abuse and corruption in a lawful manner to those who can correct the wrongdoing." Intelligence community (IC) whistleblowers are those employees or contractors working in any of the 17 elements of the IC who reasonably believe there has been a violation of law, rule, or regulation; gross mismanagement; waste of resources; abuse of authority; or a substantial danger to public health and safety. The IC has publicly recognized the importance of whistleblowing, and supports protections for whistleblowers who conform to guidelines to protect classified information. The Director of National Intelligence (DNI) whistleblowing policy and guidance is publicly available and specifically addresses the process for making protected disclosures and whistleblower protections for IC contractors, members of the Armed Forces, and federal employees. There are differing opinions, however, on whether the IC's internal processes have the transparency necessary to ensure adequate protections against reprisal, and whether protections for IC contractors are sufficient.

IC whistleblower protections have evolved in response to perceptions of gaps that many believed left whistleblowers vulnerable to reprisal. The first whistleblower legislation specific to the IC was limited to specifying a process for IC whistleblowers to make a complaint but offered no specific protections. Subsequent legislation included only general provisions for protecting IC whistleblowers with no additional guidance on standards for implementation. Presidential Policy Directive (PPD)-19, signed in 2012, provided the first specific protections against reprisal actions for making a complaint. The Intelligence Authorization Act for Fiscal Year 2014 codified these provisions, which were further supported with IC implementation policy. Separate legislation under Title 10 of the U.S. Code, along with DOD implementing guidance, provides protections for members of the Armed Forces, including those assigned to elements of the IC. In early 2018, Congress passed legislation to address perceived gaps in protections for IC contractors.

Contents

Contacts

Introduction

Whistleblowing is "the act of reporting waste, fraud, abuse and corruption in a lawful manner to those who can correct the wrongdoing."[1] Intelligence Community (IC) whistleblowers are those employees or contractors working in any of the 17 elements of the IC who reasonably believe there has been a violation of law, rule, or regulation; gross mismanagement; waste of resources; abuse of authority; or a substantial danger to public health and safety. The essential distinction between whistleblowers generally and those in the IC (or those who otherwise have security clearances) is the concern for protecting classified information that may be involved in an IC-related incident or complaint. The IC has recognized that whistleblowing can save taxpayers' dollars, help ensure an ethical and safe working environment, and enable timely responses for corrective action.

Whistleblowing protections for employees and contractors in the IC are extended only to those who make a lawful disclosure. They do not cover disclosures that do not conform to statutes and directives prescribing reporting procedures intended to protect classified information, such as leaking to the media or a foreign government. The whistleblower protections do not apply to a difference of opinion over policy, strategy, analysis, or priorities for intelligence funding or collection unless there is a reasonable concern over legality or constitutionality. Whistleblowing protections also do not protect against legitimate adverse personnel or security clearance eligibility decisions if the agency can demonstrate that it would have taken the same action in the absence of a protected disclosure.

Congress and the executive branch have defined in statute and directives procedures for IC whistleblowers to make protected disclosures that also provide for the security of classified information. The Director of National Intelligence (DNI) whistleblowing policy and guidance is publicly available and specifically addresses whistleblower process and protections for IC contractors, members of the Armed Forces, and federal employees.[2] There are differing opinions, however, on whether the IC's internal processes have the transparency necessary to ensure adequate protections against reprisal, and whether protections for IC contractors are sufficient.

IC whistleblower protections have evolved in response to perceptions of gaps that many believed left whistleblowers vulnerable to reprisal. The first whistleblower legislation specific to the IC was the Intelligence Community Whistleblower Protection Act (ICWPA) of 1998. It was limited to specifying a process for an IC whistleblower to make a complaint but offered no specific protections. The Intelligence Authorization Act for Fiscal Year 2010 included provisions for protecting IC whistleblowers, though these were general and subject to different standards of implementation. Presidential Policy Directive (PPD)-19, signed in 2012, provided the first specific protections in response to perceptions that IC whistleblowers remained vulnerable to reprisal actions for making a complaint. The Intelligence Authorization Act for Fiscal Year 2014 codified the PPD-19 provisions and Intelligence Community Directive (ICD)-120 established a PPD-19 implementation policy. For members of the Armed Forces assigned to elements of the IC, 10 U.S.C. §1034 provides whistleblower protections. Department of Defense (DOD) implementing guidance for Section 1034 can be found in DOD Directive 7050.06, *Military Whistleblower Protection.* In January 2018, Congress passed P.L. 115-118. Section 110 amended

[1] Daniel Coats, Director of National Intelligence, "IC Leadership Support," *Introducing IC Whistleblowing*, at https://www.dni.gov/ICIG-Whistleblower/.

[2] https://www.dni.gov/ICIG-Whistleblower/process-how.html.

the National Security Act of 1947 and the Intelligence Reform and Terrorism Prevention Act of 2004 to include provisions to address perceived gaps in protections for IC contractors.

Intelligence Community Whistleblower Protection Act (ICWPA) of 1998

The Intelligence Community Whistleblower Protection Act of 1998 (ICWPA)[3] was intended to assist whistleblowers in the IC who are specifically excluded from the Whistleblower Protection Act of 1989. It should be noted that the ICWPA makes no explicit mention of members of the Armed Forces assigned to an IC element.[4] It amended previous acts of Congress—the Central Intelligence Agency Act of 1949 and the Inspector General Act of 1978—to enable an IC government employee or contractor "who intends to report to Congress a complaint or information with respect to an urgent concern" to report to the Inspector General (IG) of the employee's or contractor's IC agency.[5] Congress noted that the absence of this provision in law previously "may have impaired the flow of information needed by the intelligence committees to carry out oversight responsibilities."[6] Consequently, the ICWPA defines formal processes for submitting complaints that ensure the protection of classified information that may be involved:

- It requires the IG to report within 14 days all credible complaints to the Director of the CIA or to the head of the establishment who, in turn, is required to report the complaint to the congressional intelligence committees within 7 days.
- In the event the IG does not report the complaint or reports it inaccurately, the employee or contractor has the right to submit the complaint to Congress directly. This may be done (1) after the employee has provided notice to the IG, and (2) after the employee has obtained from the IG procedures for protecting classified information when contacting the congressional intelligence committees.

Although the ICWPA provides a process for IC whistleblowers—employees and contractors—to securely report complaints to Congress via the relevant IC agency IG, it offers no specific provisions for protecting whistleblowers from reprisal or punishment.[7]

[3] Title VII of the Intelligence Authorization Act for Fiscal Year 1999, P.L. 105-272 §§701-702.

[4] See below in this report. 10 *U.S.C.* §1034 provides whistleblower protections for members of the Armed Forces, including those who may be assigned to an element of the IC.

[5] The ICWPA defines an "urgent concern" as (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; (2) a false statement to the Congress on, or willful withholding from the Congress of, an issue of material fact relating to the funding, administration, or operation of an intelligence activity; or (3) an action constituting reprisal in response to an employee's reporting of an urgent concern. See P.L. 105-272, §702(a).

[6] P.L. 105-272, §701.

[7] Subsequent legislation that specifically prohibits actions taken in reprisal for an IC employee making a lawful disclosure (a disclosure that adheres to the 1998 ICWPA process for making a complaint while protecting classified information) underscores the perception that the ICWPA process alone did not constitute a protection for a whistleblower against adverse personnel action.

Intelligence Authorization Act (IAA) for Fiscal Year 2010

The IAA for FY2010 (P.L. 111-259) included the first general provisions for protection of whistleblowers as part of legislation that established the Office of the Inspector General of the Intelligence Community (OIGIC), headed by the Inspector General of the Intelligence Community (IGIC). Section 405(a)(1) of the IAA for FY2010 added a new Section 103H to the National Security Act of 1947. Section 103H(g) permitted lawful disclosures to the IGIC, but lacked the specificity of later whistleblower protection legislation and directives:

> (3) The Inspector General [of the Intelligence Community] is authorized to receive and investigate, pursuant to subsection (h), complaints or information from any person concerning the existence of an activity within the authorities and responsibilities of the Director of National Intelligence 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. Once such complaint or information has been received from an employee of the intelligence community—
>
> (A) the Inspector General shall not disclose the identity of the employee without the consent of the employee, unless the Inspector General determines that such disclosure is unavoidable during the course of the investigation or the disclosure is made to an official of the Department of Justice responsible for determining whether a prosecution should be undertaken; and
>
> (B) no action constituting a reprisal, or threat of reprisal, for making such complaint or disclosing such information to the Inspector General may be taken by any 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.[8]

Section 405 does cover contractors in addition to federal employees of IC elements:

> The Inspector General [of the IC] shall have access to any employee, or any employee of a contractor, of any element of the intelligence community needed for the performance of the duties of the Inspector General."[9]
>
> An employee of an element of the intelligence community, an employee assigned or detailed to an element of the intelligence community, or an employee of a contractor to the intelligence community 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.[10]

Section 425(d) of the IAA for FY2010 also amended the Central Intelligence Agency Act of 1949 clarifying existing protections against reprisals against CIA employees who make lawful disclosures to the CIA Inspector General.[11]

[8] 50 *U.S.C.* §3033(g).

[9] 50 *U.S.C.* §3033(g)(2)(B).

[10] 50 *U.S.C.* §3033(k)(5)(A).

[11] P.L. 111-259 §425(d). The provisions for prohibiting reprisal actions for lawful whistleblower disclosures to the CIA Inspector General can be found in 50 U.S.C. §3517(e)(3)(A)-(B).

Presidential Policy Directive (PPD)-19

PPD-19, *Protecting Whistleblowers with Access to Classified Information*, signed by President Obama on October 10, 2012, provided the first executive branch protections for IC whistleblowers. PPD-19 specifically protects some employees in the IC (it specifically excludes members of the Armed Forces)[12] with access to classified information, from personnel actions taken in reprisal for making a lawful disclosure.[13]

PPD-19 defines a protected disclosure in part as follows:

> a disclosure of information by the employee to a supervisor in the employee's direct chain of command up to and including the head of the employing agency, to the Inspector General of the employing agency or Intelligence Community Element, to the Director of National Intelligence, to the Inspector General of the Intelligence Community, or to an employee designated by any of the above officials for the purpose of receiving such disclosures, that the employee reasonably believes evidences (i) a violation of any law, rule, or regulation; or (ii) gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety.

- PPD-19 prohibits reprisals (1) that could affect a whistleblower's eligibility for access to classified information; or (2) involve a personnel action against the IC employee making a protected disclosure.[14]
- PPD-19 requires IC elements to certify to the DNI a process for IC employees to seek a review of personnel actions the employee believes are in reprisal for making a lawful disclosure. The review process also must provide for the security of classified information involved in a disclosure.
- As part of the review process, PPD-19 requires the IC element Inspector General to determine whether a personnel action was in reprisal for a lawful disclosure. The IG makes recommendations for corrective action in the event of a determination that a violation took place.
- The agency head "shall carefully consider the findings of and actions recommended by the agency Inspector General."[15] The agency head does not have to accept an IG's recommendation for corrective action.
- IC agencies also have to certify to the DNI that the agency has a review process that permits employees to appeal actions involving eligibility for access to classified information that are alleged to be in violation of prohibitions against retaliation for making lawful disclosures.

---

[12] In addition to excluding members of the Armed Forces, PPD-19 otherwise does not define *employee*, and does not include any reference to IC contractors. To some this is an important omission. The following year, 2013, Edward Snowden, a Booz Allen Hamilton contractor working at the National Security Agency, leaked classified documents to the media claiming there were no protections for someone with his status as a contactor to submit a whistleblowing complaint. The ICWPA of 1998, which provides for a process for submitting a whistleblowing complaint (but does not specify protections against prohibited reprisals), applies to contractors as well as federal IC employees. See Joe Davidson, "No Whistleblower Protections for Intelligence Contractors," *The Washington Post*, June 19, 2013, at https://www.washingtonpost.com/politics/federal_government/no-whistleblower-protections-for-intelligence-contractors/2013/06/19/dc3e1798-d8fa-11e2-a9f2-42ee3912ae0e_story.html?utm_term=.3319c1b46f47.

[13] The Directive pertains to all elements of the IC with the specific exception of the Federal Bureau of Investigation (FBI).

[14] Adverse personnel actions might include demotion, transfer, termination, suspension, lower performance evaluation or punitive changes in duties and responsibilities.

[15] Presidential Policy Directive (PPD)-19, *Protecting Whistleblowers with Access to Classified Information*, The White House, October 10, 2012, at https://www.va.gov/ABOUT_VA/docs/President-Policy-Directive-PPD-19.pdf.

- PPD-19 allows for a whistleblower to request an external review by an IG panel chaired by the IGIC if the employee has exhausted the agency review process. In the event the panel decides in the employee's favor, the agency must consider but does not have to accept the panel's recommendation for corrective action.
- It requires the IGIC to report annually to the congressional intelligence committees the IG determinations and recommendations and IC element head responses to the determinations and recommendations.
- PDD-19 requires the executive branch to provide training to employees with access to classified information (not including contractors or members of the Armed Forces) regarding protections for whistleblowers.

Title VI of the Intelligence Authorization Act (IAA) for Fiscal Year 2014

Title VI of the FY2014 IAA (P.L. 113-126) codified provisions of PPD-19 and provided the first expansive statutory protections for IC whistleblowers against personnel or security clearance actions made in reprisal for protected disclosures.[16]

- Section 601 of Title VI protected IC whistleblowers from any personnel action made in retaliation for a lawful disclosure.[17] This includes a lawful disclosure to the Director of National Intelligence (or any employees designated by the DNI for such purpose), the Inspector General of the Intelligence Community, the head of the employing agency (or an employee designated by the head of that agency for such purpose), the appropriate inspector general of the employing agency, and a congressional intelligence committee, or a member of a congressional intelligence committee.
- Section 601 of Title VI made no specific mention of protections for contractors, however.
- A lawful disclosure is defined in the legislation as a disclosure that an IC employee whistleblower reasonably believes is a violation of "Federal law, rule or regulation ... or mismanagement, a gross waste of funds, an abuse of authority, or substantial and specific danger to public health and safety."
- Section 602 of Title VI provided protections against retaliatory revocation of the security clearance of a covered government employee whistleblower for making a lawful disclosure.[18]
- Section 602 also requires the development of *appeal* policies and procedures for any decision affecting a whistleblower's security clearance that the whistleblower

[16] The provisions under this legislation cover all IC elements *except* the Intelligence Branch of the Federal Bureau of Investigation (FBI/IB). See 50 *U.S.C.* §3234(a)(2)(B).

[17] The scope of personnel actions covered by the legislation includes an appointment, promotion, disciplinary or corrective action, detail, transfer, reassignment, demotion, suspension, termination, reinstatement or restoration, a performance evaluation, a decision concerning pay, benefits or awards, a decision concerning education or training if such education or training may reasonably be expected to lead to an appointment, promotion, or performance evaluation, or any other significant change in duties, responsibilities or working conditions. See 50 *U.S.C.* §3234(a)(3).

[18] 50 *U.S.C.* §3341(j). Coverage for this legislation on protections against retaliatory revocation of security clearances includes all elements of the IC—including the FBI/IB—in addition to other Executive Branch departments and agencies. It makes no mention of members of the Armed Forces who might be assigned to an IC element.

alleges is in reprisal for having made a protected disclosure. This provision also enabled the whistleblower to retain his/her current employment status in the government, pending the outcome of the appeal.[19]

- Section 602 of Title VI did not permit judicial review, nor does it permit a private right of action.[20]
- Section 602 of Title VI does not make any mention of contractors.

Intelligence Community Directive (ICD)-120

First signed in 2014, and updated on April 29, 2016, ICD-120, *Intelligence Community Whistleblower Protection*, provides IC implementing guidance for PPD-19. ICD-120 provisions include the following:

- Protections against reprisal involving a personnel action against the IC employee making a protected disclosure.[21] ICD-120 excludes members of the Armed Forces, and makes no reference to contractors.[22]
- Protections from reprisal for a protected disclosure that could affect an IC whistleblower's eligibility for access to classified information.[23] This provision includes contractors and members of the Armed Forces.
- A requirement for each IC element to have a review process to permit appeals for any decision involving a security clearance allegedly in retribution for making a lawful disclosure. The provision allows the whistleblower to maintain his/her employment status while a decision is pending.
- Provision for an employee alleging a reprisal who has exhausted the internal agency review process to request an External Review Panel chaired by the IGIC.
- A requirement for IC-wide communications and training on whistleblower protections.

[19] 50 *U.S.C.* §3341(b)(7).

[20] A private right of action would permit an individual to bring a lawsuit.

[21] The ICD-120 provision protecting against personnel actions made in retaliation for a lawful disclosure covers all elements of the IC with the specific exception of the FBI. See ICD-120(E)(1)(d), at https://www.dni.gov/files/documents/ICD/ICD%20120%20-%20IC%20Whistleblower%20Protection%20(29%20Apr%202016).pdf.

[22] See ICD-120(E)(1)(b)(4). Protections for members of the Armed Forces against personnel actions made in reprisal for a lawful disclosure are covered by 10 U.S.C. §1034. See below, Whistleblower Protections for Members of the Armed Forces Assigned to the IC.

[23] "Employee" is defined to include a person "employed by, detailed or assigned to" an IC element including members of the Armed Forces, an expert or consultant to an agency, a contractor, licensee, certificate holder or grantee of an agency, or personal services contractor, or "any other category of person who acts for or on behalf of an agency as determined by the appropriate agency head." See ICD-120(F)(1)(b)(1).

Whistleblower Protections for Members of the Armed Forces Assigned to the IC

Section 1034 of Title 10 *U. S. Code* provides protections against personnel actions taken in retaliation for protected communications by members of the Armed Forces.[24] The Office of the DNI cites this statute as applicable to members of the Armed Forces assigned to the IC elements.[25] Section 1034—unlike the ICWPA, which makes no mention of applicability to the Armed Forces—does not provide a process for making a protected communication that also protects classified information. Section 1034

- allows members of the Armed Forces to communicate with a Member or Members of Congress; an Inspector General; a member of the DOD audit, inspection, investigation, or law enforcement organization; any person or organization in the chain of command; a court-martial proceeding; or any other organization designated pursuant to regulations or other established administrative procedures for such communications; or testimony, or otherwise participating in or assisting in an investigation or proceeding involving Congress or an Inspector General;
- specifies prohibited personnel actions in reprisal for a member of the Armed Forces making a protected communication;[26]
- enables the DOD to take action to mitigate hardship for an Armed Forces member following a preliminary finding concerning an alleged reprisal for a protected communication;[27]
- requires the inspector general conducting an investigation into a protected communication to provide periodic updates to Congress, the whistleblower, the Secretary of Defense, and the relevant service;[28] and
- requires the DOD Inspector General to prescribe uniform standards for (1) investigations of allegations of prohibited personnel actions, and (2) training for staffs of Inspectors General on the conduct of such investigations.[29]

---

[24] This statute uses the term *communication* instead of *disclosure*.

[25] See Office of the Director of National Intelligence, "What Are My Protections?" at https://www.dni.gov/ICIG-Whistleblower/protected.html. See also DOD Directive 7050.06, *Military Whistleblower Protection*, April 17, 2015.

[26] 10 *U.S.C.* §1034(b)(2)(A) states the following:

> The actions considered for purposes of this section to be a personnel action prohibited by this subsection shall include any action prohibited by paragraph (1), including any of the following:
>
> (i) The threat to take any unfavorable action.
>
> (ii) The withholding, or threat to withhold, any favorable action.
>
> (iii) The making of, or threat to make, a significant change in the duties or responsibilities of a member of the armed forces not commensurate with the member's grade.
>
> (iv) The failure of a superior to respond to any retaliatory action or harassment (of which the superior had actual knowledge) taken by one or more subordinates against a member.
>
> (v) The conducting of a retaliatory investigation of a member.

[27] 10 *U.S.C.* §1034(c)(4)(E).

[28] 10 *U.S.C.* §1034(e)(3)(A).

[29] 10 *U.S.C.* §1034, note ("Uniform Standards for Inspector General Investigations of Prohibited Personnel Actions and Other Matters"). The National Defense Authorization Act (NDAA) for Fiscal Year 2017 also required the Comptroller

Legislation to Address Perceived Gaps in Protections for IC Contractors

Coverage of contractors in existing IC whistleblower protection legislation is inconsistent. The ICWPA of 1998, which provides for a process for reporting a whistleblower complaint, does cover contractors, as do protections in Section 405 of the IAA for FY2010, and Title VI of the IAA of 2014. However, PPD-19 and ICD-120 do not mention contractors. There have been three subsequent efforts in Congress to address the gap in perceived coverage, culminating on January 19, 2018, when Congress passed P.L. 115-118, an amendment to the Foreign Intelligence Surveillance Act of 1978, which included Section 110 provisions to address perceived gaps in protections for IC contractors.

S. 2002, 115th Congress, Ensuring Protections for IC Contractor Whistleblowers Act of 2017

Senator McCaskill introduced S. 2002 on October 24, 2017. It was referred to the Senate Select Committee on Intelligence (SSCI) and no further action was taken. S. 2002 would have provided protections for IC employees—to include applicants, former employees, contractors, personal services contractors, and subcontractors—from being "discharged, demoted, or otherwise discriminated against" as a consequence of making a protected disclosure. It also included provisions for a process for making a complaint.

S. 794, 114th Congress, A Bill to Extend Whistleblower Protections for Defense Contractor Employees of Contractors of the Elements of the IC

On March 18, 2015, Senator McCaskill introduced S. 794. It was referred to the SSCI and no further action was taken. The bill would have amended Section 2409 of Title 10 *U.S. Code* by extending protections for contractor employees on a contract with DOD or other federal agencies to contractor employees on a contract with an IC element who comply with an existing lawful process for making a whistleblower complaint, to include protection of classified information that is part of a court action.[30]

General of the United States to review the integrity of the DOD whistleblower protection program and report to the Senate and House Armed Services Committees no later than 18 months after the date of enactment of the NDAA on whether the program satisfies Executive Branch whistleblower protection policy. See P.L. 114-328 §536(a)-(b). Department of Defense (DOD) implementing guidance for 10 *U.S.C.* §1034 can be found in DOD Directive 7050.06, *Military Whistleblower Protection.*

[30] 10 *U.S.C.* §2409(e)(1) currently excludes contractor employees of IC elements. See Joe Davidson, "No Whistleblower Protections for Intelligence Contractors," *The Washington Post*, June, 19, 2013, at https://www.washingtonpost.com/politics/federal_government/no-whistleblower-protections-for-intelligence-contractors/2013/06/19/dc3e1798-d8fa-11e2-a9f2-42ee3912ae0e_story.html?utm_term=.3319c1b46f47.

Section 110 of P.L. 115-118, Whistleblower Protections for Contractors of the Intelligence Community

On January 19, 2018, Congress passed P.L. 115-118, an amendment to the Federal Intelligence Surveillance Act of 1978. Section 110 amended Section 1104 of the National Security Act of 1947 by providing protections for IC contractor whistleblowers.[31] Section 110 amended existing whistleblower protections to enable IC *contractors* to make lawful disclosures to the head of the contracting agency (or an employee designated by the head of that agency for such purpose), or to the appropriate inspector general of the contracting agency, as well as to the DNI, IGIC, and the congressional intelligence committees (or members of the committees). These protections are similar to those for IC employees under Title VI of the IAA for FY2014 (P.L. 113-126). That legislation, however, included no provisions for contractors.

Section 110 provides unambiguous protections for IC contractors making a lawful complaint against any retaliatory personnel action involving an appointment, promotion/demotion, disciplinary or corrective action, detail, transfer or reassignment, suspension, termination, reinstatement, performance evaluation, decisions concerning pay, benefits, awards, education, or training. The protections extend to lawful complaints involving,

> a violation of any Federal law, rule or regulation (including with respect to evidence of another employee or contractor employee accessing or sharing classified information without authorization); or gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety.[32]

These protections extend to contractors of the FBI—including contractors of the IC element of FBI, the Intelligence Branch—similar to the protections for IC employees and contractors under the Section 3234 of Title 50, *U.S. Code,* as amended.[33]

Section 110 also amended Section 3341(j) of Title 50, *U.S. Code,* to include protections for IC contractors who make lawful whistleblower disclosures against retaliatory revocation of their security clearances.

Resources to Enhance Whistleblower Investigations

H.Amdt. 894, 113th Congress, to the DOD Appropriations Act for Fiscal Year 2015 (H.R. 4870), was agreed by a voice vote on June 18, 2014, redirecting $2 million dollars to fund the IC Whistleblower and Source Protection Directorate. This directorate exists within the OIGIC. The funds, which augmented the Intelligence Community Management Account, were to support the hiring of investigators and support staff to provide the IGIC greater ability to investigate fraud, waste, and abuse. Although it does not provide protections for whistleblowers per se, the measure addressed an underfunded capability in order to enable responsive follow-up on whistleblower complaints.[34]

[31] P.L. 115-118, §110.

[32] 50 U.S.C. §3234(c)(1)(A)-(B). The previous paragraph of §3234 governing lawful disclosures by IC agency employees differs from that for the paragraph for contractor employees only in one word: Contractor employees may disclose "*gross* mismanagement" while agency employees may disclose "mismanagement."

[33] See §110(b)(1)-(5) of P.L. 115-118.

[34] See Department of Defense Appropriations Act for Fiscal Year 2015 (H.R. 4870, 113th Cong.), Title VII, Amendment Offered by Mr. Holt, pp. H5466-H5467.

Author Information

Michael E. DeVine
Analyst in Intelligence and National Security

Disclaimer