S. HRG. 113–241

CYBERSECURITY: PREPARING FOR AND RESPONDING TO THE ENDURING THREAT

HEARING

BEFORE THE

COMMITTEE ON APPROPRIATIONS
UNITED STATES SENATE

ONE HUNDRED THIRTEENTH CONGRESS

FIRST SESSION

SPECIAL HEARING

JUNE 12, 2013—WASHINGTON, DC

Printed for the use of the Committee on Appropriations

Available via the World Wide Web: http://www.gpo.gov/fdsys/browse/committee.action?chamber=senate&committee=appropriations

U.S. GOVERNMENT PUBLISHING OFFICE
81–526 PDF WASHINGTON : 2016

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON APPROPRIATIONS

BARBARA A. MIKULSKI, Maryland, *Chairwoman*

PATRICK J. LEAHY, Vermont
TOM HARKIN, Iowa
PATTY MURRAY, Washington
DIANNE FEINSTEIN, California
RICHARD J. DURBIN, Illinois
TIM JOHNSON, South Dakota
MARY L. LANDRIEU, Louisiana
JACK REED, Rhode Island
FRANK R. LAUTENBERG, New Jersey [1]
MARK L. PRYOR, Arkansas
JON TESTER, Montana
TOM UDALL, New Mexico
JEANNE SHAHEEN, New Hampshire
JEFF MERKLEY, Oregon
MARK BEGICH, Alaska

RICHARD C. SHELBY, Alabama, *Ranking*
THAD COCHRAN, Mississippi
MITCH McCONNELL, Kentucky
LAMAR ALEXANDER, Tennessee
SUSAN M. COLLINS, Maine
LISA MURKOWSKI, Alaska
LINDSEY GRAHAM, South Carolina
MARK KIRK, Illinois
DANIEL COATS, Indiana
ROY BLUNT, Missouri
JERRY MORAN, Kansas
JOHN HOEVEN, North Dakota
MIKE JOHANNS, Nebraska
JOHN BOOZMAN, Arkansas

Charles E. Kieffer, *Staff Director*
William D. Duhnke III, *Minority Staff Director*

[1] Died on June 3, 2013.

CONTENTS

CYBERSECURITY: PREPARING FOR AND RESPONDING TO THE ENDURING THREAT

WEDNESDAY, JUNE 12, 2013

U.S. SENATE,
COMMITTEE ON APPROPRIATIONS,
Washington, DC.

The committee met at 2:02 p.m., in room SD–G50, Dirksen Senate Office Building, Hon. Barbara A. Mikulski (chairwoman) presiding.

Present: Senators Mikulski, Leahy, Murray, Feinstein, Durbin, Landrieu, Pryor, Tester, Udall, Merkley, Shelby, Cochran, Collins, Coats, Johanns, and Boozman.

OPENING STATEMENT OF SENATOR BARBARA A. MIKULSKI

Chairwoman MIKULSKI. This afternoon I am opening a hearing on cybersecurity. We are going to examine the efforts to protect the American people from cyber threats, to protect our domains of dot-mil, dot-gov, and dot-com. We need to make sure that the American people know what our programs are, know what we are spending our money for, and also to make sure that we make wise use of taxpayer dollars so that there are no techno-boondoggles. We hope to make sure we know how to help the private sector and to protect dot-com by real-time information-sharing about threats and helping the private sector develop the secure technologies we need. We need to prevent hackers, nation-states, and criminals from stealing our cyber identities, cyber espionage, cyber sabotage against our online commerce or our critical infrastructure, track and disrupt the hackers, and prosecute them when possible.

I have two goals for this hearing.

First, I want to make sure that we protect the American people from cyber threats by working together across the Government to protect, as I said, the domains of dot-mil, dot-gov, and dot-com.

Second, I want to examine how agencies will use cybersecurity funding in the budget. The administration is requesting more than $13 billion for fiscal year 2014. In this very stringent environment, we are concerned about techno-boondoggles. The Government is often very good at spending money, but we need to make sure we spend the money well. Over the years, there have been failures and inefficiencies in Government IT programs, and we do not want that to happen as we move forward in this cyber domain.

I called this hearing as the full committee chairwoman to work across the subcommittees to make sure there are not stovepipes, to make sure, as we look at this, the questions that we have related to governance, are we developing the right technologies to protect us, are we investing in the workforce we need, and how do we protect our civil liberties.

I am so proud of my subcommittee chairs. I want to acknowledge the work of Senator Durbin and the Ranking Member Cochran on Defense. I want to acknowledge the work of Chairwoman Landrieu and her ranking member, Senator Coats, both with a great deal of expertise. For me, we will have the Federal Bureau of Investigation (FBI) and National Institute of Science and Technology (NIST), and my great vice chairman, Senator Shelby.

This is a committee that is loaded with talent in this area, coming with enormous expertise from the authorizing committee. We have Senator Leahy from the Judiciary Committee, well versed on the issues of law on cybersecurity and a staunch protector of our civil liberties. We have Chairwoman Feinstein on the Intelligence Committee. From Armed Services, we have Reed, Shaheen, Graham, and Blunt. We have the former Chair of the Homeland Security Committee, Senator Collins, herself now a member of the Intelligence Committee. Rarely has a committee had so much talent coming together from both those of us from appropriations as well as the authorizers.

I hope that our country has a sense of urgency. We are already under attack. This is the new, enduring war. We are in a cyber war every day. Every time someone steals our identity, steals our State secrets or our trade secrets, we are at war. We now see the growing nexus between cyber criminals and nation states hacking our networks, planning disruptions of our business operations. Director Mueller of the FBI said that cyber crime will eventually surpass terrorism as our number one threat to America. Secretary Hagel and General Dempsey continue to warn us against cyber as an insidious threat. These are such critical concerns that President Obama, in his recent meeting with the Chinese President, raised cybersecurity as one of our great, great international tensions between both countries.

Now, last year, we tried to pass cybersecurity legislation. We all worked on a bipartisan basis. It was actually under the Collins-Lieberman bill. But it did not happen. The President has issued an Executive order. But just because authorizing has not happened does not mean that nothing is happening.

So in February, the President signed his Executive order, and it improves real-time information sharing, protects critical infrastructure, provides critical infrastructure in cyber risk, and brings private sector experts into the Federal service.

Each one of these goes through a different subcommittee, but here today we are going to do something pretty different. And I bring to your attention the President's fiscal year 2014 budget on the areas of cybersecurity. This will be the first time in one place that we can look across all of the areas to make sure we know what the request is, what they are not only in individual agencies, but do we get the synergistic effect necessary to protect our country. It is significant that this document that you all have, which is a public document, that we have in one place, a one-stop shop, really what the President is requesting.

The President of the United States in his budget message to the Congress has asked for $13 billion in order to execute the cybersecurity strategy across the agencies of the Federal Government. The purpose of this hearing today is to look at the cybersecurity threat, not every program from the National Security Agency (NSA), not every program being run by Homeland or the Department of Justice or the great work being done by NIST. It is to focus on the cybersecurity.

But it is a committee first and I might say a Senate first. No other committee has tried to hold a hearing across the different domains, agencies, and smokestacks, and also to do it in an open, public way.

And the expertise, as I said, here from both the subcommittee chairs and the authorizing is stunning. So we know that we are going to be able to do it.

The President has asked for $13 billion: $9.3 billion for the Department of Defense (DOD), $1.3 billion for the Department of Homeland Security (DHS), $670 million for the Department of Justice (DOJ), primarily the Federal Bureau of Investigation, and the National Institutes of Standards and Technology, $215 billion—$215 million. NIST has never seen $215 billion. That is the defense guys.

Today we will hear from our Government's lead people on this: General Alexander, the Director of the National Security Agency and the head of Cyber Command; Rand Beers, the Acting Deputy Secretary of Homeland Security; Dr. Gallagher, the Acting Deputy Secretary of Commerce but the Director of NIST; and Richard McFeely, the FBI Executive Assistant Director in charge of the Criminal, Cyber, and Response, and Services Branch.

I also want to acknowledge that in the last several days many intelligence issues have been in the press, and I understand that these are issues that are very much on the public's mind and Members of the Senate.

Last week, in my Commerce, Justice hearing with the Attorney General, this topic of particularly our surveillance program came up. I pledged to Senator Shelby, a former Chair of the Intelligence Committee, well versed on the topic, not of the surveillance but on this, that we would have a full committee hearing on that particular program. That is not today. That is for another day.

I understand that our colleague, Senator Chairwoman, the Chair of the Intelligence Committee, has scheduled a briefing for all Senators tomorrow. And this is the second hearing that Senator Feinstein has opened up the Intelligence Committee for a briefing for all Senators to be able to participate. After the Feinstein meeting tomorrow, if Senator Shelby continues to recommend that this committee hold a hearing on this matter, I will be happy to comply, and I pledge that to you, sir. I did last week and so on. But we will see if it is necessary, and if deemed so, we certainly will.

So, again, today's hearing will focus on the cyber threat, protecting the American people, protecting the taxpayer in their role as both citizen and taxpayer. I hope today's hearing will focus on this very important issue, and I say to my colleagues this is a committee hearing that is a first. It will be not the last on this topic or other matters related to our national security.

I now want to turn to my ranking member, Senator Shelby, who has been active on this matter, the vice chairman of the committee, former Chair of the Intelligence Committee. Senator Shelby.

STATEMENT OF SENATOR RICHARD C. SHELBY

Senator SHELBY. Thank you, Madam Chair.

As you have pointed out, this is a very important hearing on a topic that demands significant congressional involvement. The cyber threat, as we all know, is increasing and becoming more challenging as our adversaries grow bolder and more capable. We have seen recent and stark reminders of the threat with constant cyber attacks on the financial sector, the Chinese hacking of the New York Times and Wall Street Journal, Iranian attacks against a Saudi oil company, and reports that information on our most advance weapons systems were stolen by the Chinese.

Earlier this year, an information security company publicly reported that Chinese attackers are running an extensive cyber espionage campaign with the likely support of the Chinese Government. More recently, the same company exposed Iranian hacking in the United States.

These troubling developments remind us of how urgently we need a coordinated effort to counter and to respond to these attacks.

Madam Chair, this committee may be the only one with jurisdiction over the full complement of Government organizations involved in cybersecurity. Therefore, as you pointed out, I think it is appropriate that we take a lead role in the oversight of this effort, working with others. I would like to hear, for example, how each of you today perceive the threat and about your continuing efforts to protect critical infrastructure against attack and to address the cyber threat outside the recently issued Executive order. Cybersecurity is an immediate priority, but the framework envisioned in the Executive order will take time to develop and probably even longer to implement.

There are still areas that need more attention and may require legislation, such as information sharing. Additionally, the working relationship between the Government and the private sector is still a work in progress. Funding requirements also remain unclear in this time of fiscal uncertainty. Clearly, a lot needs to be done.

I look forward today to hearing from our panel of witnesses and perhaps they can suggest some of the best ways to protect Government systems and information as you partner with industry to strengthen our cyber infrastructure across the board.

Thank you, Madam Chair.

Chairwoman MIKULSKI. Thank you, Senator.

Now we will turn to our witness panel, and then we will go to questions, starting with myself and Senator Shelby and then the regular order that we follow in the order of arrival.

I would like to suggest that General Alexander go first, followed by Mr. Beers, Mr. McFeely representing Justice, and Dr. Gallagher, you are the wrap-up guy. General Alexander, the microphone is yours.

STATEMENT OF HON. GENERAL KEITH B. ALEXANDER, COMMANDER, U.S. CYBER COMMAND; DIRECTOR, NATIONAL SECURITY AGENCY; CHIEF, CENTRAL SECURITY SERVICE

General ALEXANDER. Senator, thank you very much.

I think what you and Senator Shelby have pointed out with respect to cyberspace is absolutely important for us to discuss. The threats that we face today continue to grow.

You know, it takes, for the Government, a team to work this. So before I go any further, I do want to point out that the team is here, and it is great to be part of that team because no one Government department or agency can do it itself. For us, it is going to take the partnership between DHS, between the FBI, and with the support of NIST especially on the Executive order that Senator Shelby brought up for us to work together.

You know, when I look at what is going on in cyberspace and the capabilities that are growing, this is an incredible opportunity for us as a Nation and for nations around the world. The technical capabilities that we have when you look at what our children are using, the iPhones, the iPads, the ability for education—this is a tremendous time. When we look at what we can do with this with respect to medical care in the future, it is a bright future for us, but it is complicated by the fact of cyber espionage, by cyber hacking, and the threats that Senator Shelby talked about. So I do want to hit on that.

You mentioned the evolution of this threat, and when you look at the threat as it has gone forward, some of the things that FBI and we see in the Department of Homeland Security work every day is a series of exploitations into our networks. The issue is how do you fix that. And that issue is complicated by the fact that it is not only exploitations that are going on, but we are seeing disruptive attacks against our Nation's infrastructure, Wall Street, with a potential for destructive attacks.

We as a Nation need to step forward and say how are we going to work this. The Government team that is here today cannot do it without support from industry. We have to have some way of working with industry because they own and operate the bulk of our Nation's infrastructure. But we have to do it in a transparent way, in a legal way, and we really appreciate the efforts of many on this panel, Senator, for what you and others have done to try to move that legislation along. But we do need to get there. We do need to have a way of working with industry. And Dr. Gallagher I know will talk about parts of this. We could not have a better person to lead it from NIST. So thanks for what you and the team are doing. We do need to begin that dialogue with industry. So part of what the Executive order does is give us that opportunity to have that dialogue.

At the same time, we have to look at what we need in legislation and get that moving forward. So, Senator, thanks for what you and the Intelligence Committee are doing to move that and others.

From my perspective, Senator, you asked what is it that we need to do. I think there are five key things that we are working on.

First, we have to create a defensible architecture. Both the Intelligence Community and the Defense Department are moving forward on what we call the "cloud architecture," a joint information environment for the Defense Department and the intel community's IT environment, the same thing for both communities moving forward to what is a more defensible architecture. And I think we need to move there. So that is the first thing.

Second, we need to be able to see what is going on in cyberspace so that we can work with industry and amongst ourselves because getting information after an attack only allows us to police it up. We have to have some way of stopping it while it is going on. So we need to be able to see it.

We need a concept for operating in cyberspace not just within the Defense Department, but amongst all three of us because we all have a role in this, and we all play vital roles, from the Department of Homeland Security's role for recovery and working with commercial industry to the FBI's law enforcement and investigative things to the Defense Department's responsibility to defend the Nation. We have to bring those together and then reach out to say, now, how is that going to work with industry and how can we share information that is vital to our common defense. We have to do that.

We need trained and ready forces. I think that is one of the most important things that the Congress expects of me of Cyber Command and of NSA to, within the Department, create trained and ready forces that are trained to a higher standard, both on the defense and on the offense, those capabilities that our Nation needs that are trained to that standard that know how to operate lawfully to protect American civil liberties and privacy and to protect this Nation in cyberspace. We have to be able to do all three.

And we have to have a capacity to act when authorized, the rules of engagement and the other authorities.

We are working those five.

From my perspective, the men and women of Cyber Command and NSA—we have tremendous technical talent. We really do. And these are great people. Our Nation has invested a lot in these people. They do this lawfully. They take compliance oversight, protecting civil liberties and privacy, and the security of this Nation to their heart every day. I could not be more proud of the men and women of NSA and Cyber Command. What we now need to do is take the next step in moving that forward.

That is all I have at this time, Senator. I will defer now to my colleague, Mr. Beers.

[The statement follows:]

PREPARED STATEMENT OF HON. GENERAL KEITH B. ALEXANDER

Thank you very much, Chairwoman Mikulski and Ranking Member Shelby, for inviting me to speak to you and your colleagues. I am here representing the Department of Defense in general and the men and women, military and civilian, who serve at U.S. Cyber Command (USCYBERCOM) and the National Security Agency/Central Security Service (NSA/CSS). It is my honor to appear today with colleagues from the Department of Justice (DOJ) and its Federal Bureau of Investigation (FBI), the Department of Homeland Security (DHS), and the National Institute of Science and Technology (NIST). I hope to describe some of the challenges we face in performing the difficult but vital missions of keeping U.S. national security systems secure, helping to protect our Nation's critical infrastructure from national-level cyber attacks, and working with other U.S. Government agencies, State and local authorities, national allies, and the private sector in defending our Nation's interests in cyberspace. Together we make up a team deeply committed to compliance with the law and the protection of privacy rights that works every day with other U.S. Government agencies, industry, academia, citizens, and allies, for only our combined efforts will enable us to make progress in cybersecurity for the Nation as a whole.

DEFENDING THE NATION IN CYBERSPACE

I would like to start today by discussing the two elements of this team that I lead. USCYBERCOM is a subunified command of U.S. Strategic Command in Omaha, though we are based at Fort Meade. USCYBERCOM's mission is to plan, coordinate, integrate, synchronize and conduct activities to direct the operations and defense of Department of Defense information networks. We also prepare to, and when directed, conduct full-spectrum military cyberspace operations in order to enable traditional military activities, ensure U.S./Allied freedom of action in cyberspace, and deny our adversaries the ability to harm us or our allies. USCYBERCOM has three operational focus areas: defending the Nation, supporting the Combatant Commands, and defending DOD Information Networks. As I noted when I testified before the Armed Services Committee in March, USCYBERCOM will address these three operational focus areas with its new Cyber Mission Forces, organized into National Mission Teams, Combat Mission Teams and Cyber Protection Teams.

Due to the intersecting responsibilities of the two organizations, USCYBERCOM was placed at the headquarters of NSA/CSS at Fort Meade. NSA/CSS collects signals intelligence on our cyber adversaries; and provides information assurance strategies and technologies to protect our national security systems. The conduct of these two missions is critical to enabling cyber operations. NSA/CSS also has multiple, technical capabilities critical to the cyber mission area, such as high-performance computing and large-scale, distributed processing and data storage. These are just some of the components of what we call the cryptologic platform; it constitutes the collection of signals intelligence and communications security capabilities that since 1952 have served users ranging from national customers, to departmental analysts, to battlefield commanders. The defense of U.S. military networks depends on knowing what those who would harm us are doing in cyberspace, which in turn depends on intelligence produced by NSA and other members of the Intelligence Community regarding adversary intentions and capabilities.

Cyberspace is characterized by high levels of convergence of separate and different networks and technology that have come together to form something greater than the sum of the parts. In this regard, USCYBERCOM's co-location with NSA/CSS mirrors the convergence in cyberspace and is a direct result of that technological shift. What we have learned is that if convergence is the reality of the cyber environment, then integration must be the reality of our response. Co-location promotes intense and mutually beneficial collaboration in an operational environment in which USCYBERCOM's success relies on net-speed intelligence. Although they are separate and distinct organizations with their own missions and authorities, NSA/CSS is a major force multiplier for USCYBERCOM, pairing the Command's operators, planners, and analysts with the expertise and assistance of NSA/CSS' cryptographers, analysts, access developers, on-net operators, language analysts, and support personnel. These are close working relationships that enable seamless, deconflicted operations that are vital to the success of the cyber mission. Co-location also improves the deconfliction of operations; physical proximity enhances mutual understanding and awareness of mission areas and helps forge effective partnerships that serve both organizations and the Nation well. Only a tightly integrated team, and tightly integrated solutions, can do what is required to address cyber threats at net speed.

I serve as the dual-hatted Commander, USCYBERCOM, and Director, NSA/Chief, CSS. The dual-hatting unifies the capabilities for full-spectrum cyber operations under a single official, maximizes the leverage of NSA/CSS cyber capabilities, capacities, and authorities, and establishes unity of effort in cyberspace for the Department of Defense. It allows deconfliction of the use of the cryptologic platform to occur with full knowledge of the needs of both organizations on a timely basis. Together, the people under my command and direction at USCYBERCOM and NSA/CSS work in concert but always under their respective authorities. They direct the operation of the Department's information networks, detect threats in foreign cyberspace, attribute threats, secure national security information systems, and help ensure freedom of action for the United States military and its allies in cyberspace—and, when directed, defend the Nation against a cyber attack.

In keeping with the DOD's Strategy for Operating in Cyberspace, USCYBERCOM and NSA/CSS are together assisting the Department in building: (1) a defensible architecture; (2) global situational awareness and a common operating picture; (3) a concept for operating in cyberspace; (4) trained and ready cyber forces; and (5) the capacity to take action when authorized. Indeed, with another key mission partner in DOD—the Defense Information Systems Agency (DISA), also based at Fort Meade—we are finding that our progress in each of these five areas benefits our efforts in the rest. We are improving our tactics, techniques, and procedures, as well as our policies and organizations. This means building cyber capabilities into doctrine, plans, and training—and building them in a way that senior leaders can plan and integrate such capabilities as they would capabilities in the air, land, and sea domains.

The imperative to accomplish this mission grows every day. We operate in a dynamic and contested domain that literally changes its characteristics each time someone powers on a networked device. Make no mistake: in light of the real and growing threats in cyberspace, our Nation needs a strong DOD role in cyberspace. While we feel confident that most foreign leaders believe that a devastating attack on the critical infrastructure and population of the United States by cyber means would elicit a prompt and proportionate response, it is possible, however, that some regime or cyber actor could misjudge the impact and the certainty of our resolve. In particular, we are not yet deterring the persistent cyber harassment of private and public sites, property, and data. Such attacks have not caused loss of life, but they have been destructive to both data and property in other countries. The remote assaults last summer on Saudi Aramco and RasGas, for example, rendered inoperable—and effectively destroyed the data on—more than 30,000 computers. Cyber programs and capabilities are growing, evolving, and spreading; we believe it is only a matter of time before the sort of sophisticated tools developed by well-funded state actors find their way to groups or even individuals who in their zeal to make some political statement do not know or do not care about the collateral damage they inflict on bystanders and critical infrastructure. The United States is already a target. Networks and Web sites owned by Americans and located here have endured intentional, state-sponsored attacks, and some have incurred degradation and disruption because they happened to be along the route to another state's overseas targets. Our critical infrastructure is thus doubly at risk. On a scale of 1 to 10, with 10 being strongly defended, our critical infrastructure's preparedness to withstand a destructive cyber attack is about a 3 based on my experience. There are variations in preparedness across sectors, but all are susceptible to the vulnerabilities of the weakest.

Let me draw your attention to another serious threat to U.S. interests: the continuing and systematic cyber exploitation of American companies and enterprises, and the resulting theft of intellectual property. Many such incidents are perpetrated by organized cybercriminals, but foreign government-directed cyber operators, tools, and organizations are targeting the data of American and Western businesses, institutions, and citizens. Certain nations have a resourced national strategy to grow their economies by intellectual property (IP) theft. They target any company with valuable IP or a leading position in its sector—and not just that company itself. Even companies that have protected their information have partners that could be "soft" targets. Are we susceptible? In the United States, intrusions have occurred against the best in the security business. The collective damage that such intrusions inflict on America's economic competitiveness and innovation edge is profound, translating into missed opportunities for U.S. companies and the potential for lost American jobs. Cyber theft jeopardizes our economic well-being.

THE U.S. FEDERAL CYBERSECURITY TEAM

No Federal department or agency is solely responsible for addressing the cyber threat, and none has been designated as the Federal cybersecurity lead because each brings unique authorities, resources, and capabilities to the effort. Cybersecurity requires a team approach, where the leadership and support roles change depending on the nature of the threat and the required response. Together, three departments carry out important roles and responsibilities as part of the broader U.S. Federal cybersecurity team in order to provide for the Nation's cybersecurity:

—The DOJ is the lead Federal department responsible for the investigation, attribution, disruption and prosecution of cybersecurity incidents. Within the DOJ, the FBI conducts domestic collection, analysis, and dissemination of cyber threat intelligence.

—The DHS is the lead Federal department responsible for national protection against, mitigation of, and recovery from domestic cybersecurity incidents. The DHS is also the lead for securing unclassified Federal civilian government networks and working with owners and operators of critical infrastructure to secure their networks through risk assessment, mitigation incident-response capabilities.

—The DOD is ultimately responsible for defending the Nation from attack in cyberspace, just as it is in all other domains. In the event of a foreign cyber attack on the United States with the potential for significant national security or economic consequences, the DOD, including USCYBERCOM with the support of NSA/CSS, will be prepared to respond.

These efforts depend on shared situational awareness and integrated operations across the U.S. Government, State and local authorities, and international partners. Together, we are helping to increase our global situational awareness through our growing collaboration with Federal Government mission partners and other departments and agencies, as well as with private industry and with other countries. That collaboration allows us to better understand what is happening across the cyber domain, which enhances our situational awareness, not only for DOD but also across the U.S. Government.

Under the joint leadership of DHS and NSA, the FBI and the other Federal cybersecurity centers created a framework to describe cybersecurity functions and information exchanges and are now developing an implementation plan for an information sharing environment that will create a cross-government shared situational awareness that is extensible to other partners such as the State and local governments and our allies. Implementing this capability to improve our collective response actions is one of the President's top cyber priorities for fiscal year 2014.

Successful operations in cyberspace depend on collaboration between defenders and operators. Those who secure and defend must synchronize with those who operate, and their collaboration must be informed by up-to-date intelligence. I see greater understanding today of the importance of this synergy across the Department, the government, and our public at large. Last fall the departments negotiated, and the President endorsed, a broad clarification of the responsibilities of the various organizations and capabilities operating in cyberspace, revising the procedures we employ for ensuring that, in the event of a cyber incident of national significance, we are prepared to act with all necessary speed in a coordinated and mutually-supporting manner. USCYBERCOM is also being integrated into the National Event response process, so that a cyber incident of national significance can elicit a fast and effective response, to include self-defense actions where approved, necessary, and appropriate.

As part of this progress, we in the Federal Government are working with State, local, international, and private partners. NSA/CSS, for example, is defining security dimensions that government and private users can utilize for "cloud" architectures, and has shown how we can manage large quantities of data and still preserve strong security. We have even shared the source code publicly so public and private architectures can benefit from it. USCYBERCOM has sponsored not only an expanding range of training courses but also two important exercises, CYBER FLAG and CYBER GUARD. The former is USCYBERCOM's major Command-level exercise, the most recent iteration of which brought in international partners to practice force-on-force maneuvers in cyberspace. The latter assembled 500 participants last summer, including a hundred from the National Guards of 12 States. They exercised State- and national-level responses in a virtual environment, learning each other's comparative strengths and concerns should an adversary attack our critical infrastructure in cyberspace.

RESOURCES

For the past 5 years, Federal cyber-related spending and performance reporting have been organized around the Comprehensive National Cybersecurity Initiative (CNCI), from which NSA/CSS received a significant amount of funding to provide specialized capabilities and foundational support to address the cyber threat. Last summer—and planned as a yearly exercise—the administration issued a data call, which includes CNCI and non-CNCI investments, in order to better understand and track cybersecurity and cyberspace operations funding. NSA/CSS's budget under this taxonomy represents spending under the major cybersecurity categories: (1) Prevent malicious cyber activity; (2) Detect, analyze, and mitigate intrusions; and (3) Shape the cybersecurity environment. These investments are fundamental to our overall cybersecurity strategy to develop and deploy unique cyber capabilities that leverage the use of signals intelligence to enhance network defense. Additional investments in cyberspace operations provide the foundational infrastructure necessary to build those capabilities as well as support full spectrum cyberspace operations in direct support of Combatant Command requirements (e.g., cryptanalysis, net-centric capabilities, data repositories, sensor deployments, and research).

From the operational perspective, the ultimate objective of cybersecurity is to deny the adversary any opportunity to exploit our systems. Doing so requires that we protect ourselves from both known and unknown threats as we execute our comprehensive strategy of hardening our networks, defending our networks, and leveraging all instruments of national power—both within our own networks and beyond. We have made significant progress in realizing the mission capabilities and cryptologic capacity required to meet the demands of operating in cyberspace. While there is still much work to do, I'd like to highlight a few of the ongoing efforts in implementing our strategy.

The Department of Defense is responsible for 7 million networked devices and thousands of enclaves. USCYBERCOM and NSA/CSS work around the clock with DISA to monitor what is happening on global networks and the functioning of DOD's information enterprise. We are also helping the Department build the DOD Joint Information Environment (JIE), comprising a shared infrastructure, enterprise services, and a single security architecture to improve mission effectiveness, increase security, and realize IT efficiencies. The JIE will be the base from which we can operate knowing that our networks are safer from adversaries. Senior officers from USCYBERCOM and NSA/CSS sit on JIE councils and working groups, playing a leading role with the office of the DOD's Chief Information Officer, Joint Staff J6, and other agencies in guiding the Department's implementation of the JIE. NSA/CSS in particular serves as the Security Advisor to the JIE, and is defining the security dimension of that architecture.

Moving to the JIE will make sharing and analytics easier while also enhancing security. I know this sounds paradoxical but it is nonetheless true, as NSA/CSS has demonstrated in its cloud capability and its support for the Intelligence Community's growing Information Technology Enterprise (IC ITE). Let me emphasize our confidence that the JIE will save resources for the Department—moving to it will give us greater capability and security at less cost.

Our progress, however, can only continue if we are able to fulfill our urgent requirement for sufficient trained, certified, and ready forces to defend U.S. national interests in cyberspace. Last December, DOD endorsed the force presentation model we need to implement this new operating concept. We are establishing cyber mission teams in line with the principles of task organizing for the joint force. The Services are building these teams to present forces for STRATCOM in support of USCYBERCOM-delegated Unified Command Plan mission. They will soon be capable of operating on their own, with a range of operational and intelligence skill sets, as well as a mix of military and civilian personnel. They will also have appropriate operating authorities under order from the Secretary of Defense and from my capacity as the Director of NSA/CSS. Each of these cyber mission teams is being trained to common and strict operating standards so that they can be online without putting at risk our own military, diplomatic, or intelligence interests.

I must also mention our concerns over the ongoing budget uncertainty. Foremost in the minds of many of our people are the looming furloughs which entail up to 11 days without pay between July 7 and September 21. While many of our personnel are exempted from the furloughs, others are not, and their absence will degrade our mission readiness and performance this summer and beyond, and make the development of a strong and capable cyber force more problematic. Our people truly are our most important capability. We can and have showcased the incredibly valuable contributions made by our entire workforce daily in securing our networks, supporting our war fighters, and providing unique insights into foreign intelligence targets. I want to emphasize the harmful impact of furloughs on the vital mission and functions we perform and on the people we have entrusted to perform or enable them. Furloughs make hiring new personnel harder and will drive our best personnel away to jobs awaiting in the private sector. Our USCYBERCOM and NSA/CSS workforce, regardless of funding stream, is one that by definition seamlessly collaborates across the many functions and disciplines that constitute our capabilities and operations. All are essential to the whole.

GUARDING PRIVACY AND CIVIL LIBERTIES

Let me emphasize that our Nation's security in cyberspace is not a matter of resources alone. It is an enduring principle and an imperative. Everything depends on trust. We operate in a way that ensures we keep the trust of the American people because that trust is a sacred requirement. We do not see a tradeoff between security and liberty. It is not a choice, and we can and must do both simultaneously. The men and women of USCYBERCOM and NSA/CSS take this responsibility very seriously, as do I. Beyond my personal commitment to do this right, there are multiple oversight mechanisms in place. Given the nature of our work, of course, few outside of our Executive, Legislative and Judicial Branch oversight bodies can know the details of what we do or see that we operate every day under strict guidelines and accountability within one of the most rigorous oversight regimes in the U.S. Government. For those of you who do, and who have the opportunity to meet with the men and women of USCYBERCOM and NSA/CSS, you have seen for yourself how seriously we take this responsibility and our commitment to earning and maintaining your trust.

LEGISLATION

Although the February 2013 Executive order will help raise the Nation's cyber defenses, it does not eliminate the urgent need for legislation in these and other areas of cybersecurity. The administration's legislative priorities for the 113th Congress build upon the President's 2011 Cybersecurity Legislative Proposal and take into account 2 years of public and congressional discourse about how best to improve the Nation's cybersecurity. We support legislation that:

—Facilitates cybersecurity information sharing between the government and the private sector as well as among private sector companies. We believe that such sharing can occur in ways that protect privacy and civil liberties, reinforce the appropriate roles of civilian and intelligence agencies, and include targeted liability protections;

—Incentivizes the adoption of best practices and standards for critical infrastructure by complementing the process set forth under the Executive order;

—Gives law enforcement the tools to fight crime in the digital age;

—Updates Federal agency network security laws, and codifies DHS' cybersecurity responsibilities; and

—Creates a National Data Breach Reporting requirement.

In each of these legislative areas, we want to incorporate appropriate privacy and civil liberties safeguards.

The administration wants to continue the dialogue with the Congress and stands ready to work with Members of Congress to incorporate our core priorities to produce cybersecurity information-sharing legislation that addresses these critical issues.

CONCLUSION

Thank you again, Madam Chairwoman and members of the committee, for inviting me to speak to you today. I also thank you on behalf of the men and women of USCYBERCOM and NSA/CSS for your support, and for the support of the Congress. We are working to mitigate the vulnerabilities inherent in any networked environment or activity while ensuring that the benefits that we gain and the effects we can create are significant, predictable, and decisive. If I could leave you with one thought about the course of events, it is that we have no choice but to "normalize" cyberspace operations and to make them part of the capability set of our senior policymakers and commanders. We are working closely with our interagency partners as well as other DOD elements. This is a necessity, for, as I suggest above, our Nation faces diverse and persistent threats in cyberspace that cannot be defeated through the efforts of any single organization. Most cyber operations are interagency efforts, almost by definition. We have gained valuable insight from the great work of partners like the Departments of Justice, Commerce, and Homeland Security, as well as from the collaboration of industry, academia, and allies. Indeed, the flow of information and expertise across the commands, agencies, departments and foreign mission partners here and overseas is improving slowly but steadily. We have much to gain from this partnership, but perhaps not much more time left before our situation in cyberspace becomes even more worrisome than today. And now I look forward to your questions.

STATEMENT OF HON. RAND BEERS, ACTING DEPUTY SECRETARY, DEPARTMENT OF HOMELAND SECURITY

Mr. BEERS. Thank you, General Alexander, and Chairwoman Mikulski, Ranking Member Shelby, and other distinguished members of the committee.

We all welcome this opportunity to appear before you. As you said, Senator Mikulski, this is a unique opportunity to talk about the range of cybersecurity activities across the Government, and we welcome that.

As most of you know, cybersecurity is one of the five major missions of the Department of Homeland Security and one that we take very seriously. The threats that we face are varied and serious, and in that regard, our cybersecurity mission focuses in two primary areas. They are to protect the Federal civilian networks and to work with the private sector to protect America's critical infrastructure.

In that regard and as the chairwoman mentioned, the President's policy initiatives for the year ahead are to secure Federal networks, to protect critical infrastructure, to improve incident response, to engage internationally, and to shape the future.

With respect to the first, this is one of the major areas that DHS is responsible for. We are investing about $600 million in protecting Federal networks through our intrusion protection systems and through our continuous diagnostics and mitigation systems. We are also working heavily with America's critical infrastructure, both public and private.

We are working under the Executive order with our partners in NIST to create the cybersecurity framework, and this is, as you know, an important initiative on our part. The Executive order, as you know, is the administration's effort after an attempt to get legislation last year. That is not to say that we still are not interested in getting that legislation, and that is certainly something that we want to talk about in the time ahead.

In addition to that, we are working to improve incident response, working with our partners in the FBI and with the National Security Agency. This is a "call to one, call to all" initiative in which we work together both in our headquarters and our operation center in terms of sharing information and where we work together in the field in the deployment of teams to go to particular sites of particular incidents in order to determine what happened and in order to be able to provide information to other parts of the private sector that will help them prevent the same kind of an incident from occurring.

We are also involved in the international area with individual countries and partners around the world, but also with the European Union as well. While it is a small program within the Department of Homeland Security, it is a very important program and we have a lot of key partners that we work with. And that is just in terms of the engagement in terms of face to face. In terms of the information sharing, our whole incident response structure, the National Cybersecurity Communications and Integration Center, on a regular basis shares information internationally with other computer emergency readiness teams around the world in order to do with them what we do for ourselves nationally in order to protect cyberspace around the world.

And finally, we work in terms of our research and development and other activities to try to shape the future.

This is an important effort that is ongoing, one in which, as General Alexander said, we could not do if we were doing it individually in DHS. It takes all of us here at the table to make this work.

And I want to thank you for the opportunity to speak with you today and to talk about DHS programs and our teamwork together. Thank you.

[The statement follows:]

PREPARED STATEMENT OF HON. RAND BEERS

Cyberspace is woven into the fabric of our daily lives. According to recent estimates, globally interconnected communications and information networks that operate in this space encompass more than 2 billion people with at least 12 billion computers and devices, including global positioning systems, mobile phones, satellites, data routers, ordinary desktop computers, and industrial control computers that run power plants, water systems, and more.

While this increased connectivity has led to significant transformations and advances across our country—and around the world—it also has increased the importance and complexity of our shared risk and requires a collaborative approach within government and between governments and the private sector. Our daily activities, economic vitality, and national security depend on the Nation's ability to secure cyberspace. A vast array of interdependent information technology (IT) networks, systems, services, and resources are critical to communication, travel, powering our homes, running our economy, and obtaining government services. No country, industry, community or individual is immune to cyber risks. The word "cybersecurity" itself encompasses prevention, protection and resilience against a broad range of malicious activity from a variety of actors perpetrating denial of service attacks, targeting our financial system to steal millions of dollars, accessing valuable trade secrets, and intruding into government networks and systems that control our critical infrastructure.

Cyber attacks and intrusions can have very real consequences in the physical world. The Department of Homeland Security (DHS) is the lead Federal civilian department responsible for coordinating the national protection, prevention, mitigation, and recovery from cyber incidents and works regularly with business owners and operators to take steps to strengthen their facilities and communities. The Department's National Cybersecurity and Communications Integration Center (NCCIC) works daily to enhance situational awareness among stakeholders, including those at the State and local level, as well as industrial control system owners and operators, by providing critical cyber threat, vulnerability, and mitigation data to a number of organizations including through Information Sharing and Analysis Centers, which are cybersecurity resources for critical infrastructure sectors. Last year DHS notified potential targets of a campaign of cyber intrusions that focused on natural gas and pipeline companies that was highly targeted, tightly focused and well crafted. With the assistance of our interagency partners, we responded to this campaign with a comprehensive effort that included outreach, technical assistance, and mitigation.

The U.S. Government has worked closely with the private sector during the recent series of denial-of-service incidents against the financial sector. Together with our interagency partners, we have provided classified cyber threat briefings and technical assistance to help banks improve their defensive capabilities. This includes identifying and releasing hundreds of thousands of distributed denial of service-related IP addresses and supporting information in order to help financial institutions and their IT security service providers improve their defenses. In addition to sharing with these private sector entities, DHS working with the Department of State (DOS) has provided this threat information to more than 120 international partners, many of whom have contributed to our mitigation efforts. These developments reinforce the need for greater information sharing and collaboration among government, industry, and individuals to reduce the ability for malicious actors to establish and maintain capabilities to carry out such efforts.

In addition to these attacks and intrusions, we also face a range of traditional crimes now perpetrated through cyber networks. These include child pornography and exploitation, as well as banking and financial fraud, all of which pose severe economic and human consequences. For example, in March 2012, the U.S. Secret Service (USSS) worked with U.S. Immigration and Customs Enforcement (ICE) to arrest nearly 20 individuals in its "Operation Open Market," which seeks to combat transnational organized crime, including the buying and selling of stolen personal and financial information through online forums.

Additionally, in late May 2013, the Secret Service, in close coordination with U.S. Immigration and Customs Enforcement's (ICE) Homeland Security Investigations (HSI) and the Global Illicit Financial Team, arrested five individuals and seized bank accounts containing approximately $20 million located in eight countries. The investigation of Liberty Reserve, a transnational online payment processor and money transfer system, led to the seizure of an online domain owned and operated by the company. It is alleged that Liberty Reserve is used by criminal elements worldwide to launder money and distribute illegal proceeds globally. Liberty Reserve had approximately 1 million users worldwide with more than 200,000 users in the

United States. It is estimated that Liberty Reserve processed more than 12 million financial transactions annually with a combined value of more than $1.4 billion. Overall, Liberty Reserve processed an estimated 55 million separate financial transactions and is believed to have laundered more than $6 billion in criminal proceeds. The United States Attorney's Office for the Southern District of New York is prosecuting this case.

As Americans become more reliant on modern technology, we also become more vulnerable to cyber exploits such as corporate security breaches, social media fraud, and spear phishing, which targets employees through emails that appear to be from people they know, allowing cyber criminals to steal personal and business information.

Cybersecurity is a shared responsibility, and each of us has a role to play. Emerging cyber threats require engagement from government, the private sector, law enforcement, and members of the public. The success of our efforts to reduce cybersecurity risks depends on effective identification of cyber threats and vulnerabilities, analysis, and enhanced information sharing between departments and agencies from all levels of government, the private sector, international entities, and the American public.

DEPARTMENT OF HOMELAND SECURITY MISSION IN PROTECTING GOVERNMENT NETWORKS AND CRITICAL INFRASTRUCTURE

DHS is committed to ensuring cyberspace is supported by a secure and resilient infrastructure that enables open communication, innovation, and prosperity while protecting privacy, confidentiality, and civil rights and civil liberties by design. The Department is achieving its cybersecurity mission by helping to create a safe, secure, and resilient cyber environment while promoting cybersecurity knowledge and innovation.

DHS has operational responsibilities for securing unclassified Federal civilian government networks and working with owners and operators of critical infrastructure to secure their networks through cyber threat analysis, risk assessment, mitigation, and incident response capabilities. The Department is also responsible for coordinating the Federal Government response to significant cyber or physical incidents affecting critical infrastructure consistent with Presidential Policy Directive (PPD) 21. In addition, the Department combats cyber crime by leveraging the skills and resources of the USSS and ICE and working in cooperation with partner organizations to investigate cyber criminals. In addition, pursuant to the President's recent Executive Order 13636 on Improving Critical Infrastructure Cybersecurity as well as Presidential Policy Directive 21 on Critical Infrastructure Security and Resilience, we are working with our partners to strengthen the security and resilience of critical infrastructure through an updated and overarching national framework that acknowledges the increased role of cybersecurity in securing physical assets.

RESPONSE TO CYBER EVENTS

The NCCIC is a key component of DHS's ability to work with government, industry, and international partners to protect critical cyber and communications systems. To create shared situational awareness, the NCCIC integrates internal analysis and data, Intelligence Community and law enforcement reporting, and data shared by private sector and international partners into a comprehensive series of actionable information products, including joint products with the Federal Bureau of Investigation (FBI). The NCCIC works closely with those Federal agencies most responsible for helping to enhance the cybersecurity of critical infrastructures, including the Departments of Treasury and Energy.

In addition to Federal partners, the NCCIC also actively engages with the appropriate private sector entities; information sharing and analysis centers; State, local, tribal, and territorial (SLTT) governments, including the Multi-State Information Sharing and Analysis Center (MS–ISAC); and international partners. As integral parts of the cybersecurity and communications community, these groups work together to protect the portions of critical information technology that they interact with, operate, manage, or own. The NCCIC leverages the collective capabilities of its partners to provide joint incident response to assist with forensic investigations, malware analysis, review network data, and security posture assessment.

To further increase awareness of both cyber threat and resources available, the NCCIC and the United States Computer Emergency Readiness Team (US–CERT) have conducted approximately 50 threat briefings thus far in fiscal year 2013 as a part of our outreach effort to our Federal, SLTT, and private sector partners. Since 2009, the NCCIC has responded to nearly half a million incident reports and released more than 26,000 actionable cybersecurity alerts to the Department's public and private sector partners. An integral player within the NCCIC, the US–CERT also provides response support and defense against cyber-attacks for Federal civilian agency networks as well as private sector partners upon request. US–CERT collaborates and shares information with State and local government, industry, and international partners, consistent with rigorous privacy, confidentiality, and civil liberties guidelines, to address cyber threats and develop effective security responses. In 2012, US–CERT processed approximately 190,000 cyber incidents involving Federal agencies, critical infrastructure, and the Department's industry partners—a 68-percent increase from 2011. In addition, US–CERT issued over 20,411 actionable cyber-alerts over the past 3 years that were used by private sector and government agencies to protect their systems.

Similar growth has been seen for the Department's Industrial Control Systems Computer Emergency Response Team (ICS–CERT) and National Coordinating Center for Telecommunications (NCC), whose outreach has resulted in providing access to cyber threat information to more than 980 and 300 entities, respectively. ICS–CERT also responded to 177 incidents last year while completing 89 site assistance visits and deploying 15 teams with US–CERT to assist with significant private sector cyber incidents. This rapid increase in production for ICS–CERT, including the dissemination of more than 800 products over the past 3 years, yielded them the award of Best Security Team by SC Magazine at the 2013 RSA Security Conference.

The effectiveness of DHS's cyber protection, response, mitigation and recovery relies heavily on sharing information with the private sector. In 2011, DHS launched the Cyber Information Sharing and Collaboration Program (CISCP), which is specifically designed to elevate the cyber awareness of all critical infrastructure sectors through close and timely cyber threat information sharing and direct analytical exchange. The Department is constantly enhancing the CISCP. In an effort to ensure the program continues to evolve with the needs of industry, DHS has conducted numerous feedback sessions, monthly collaboration conference calls, and three face-to-face technical exchanges. It is also working to automate the program so that it can share information in real-time.

In addition to the CISCP, DHS, in close collaboration with interagency and private sector partners, is continuing to expand the Enhanced Cybersecurity Services (ECS) program, which establishes a voluntary information sharing program that assists critical infrastructure owners and operators to improve protection of their systems from unauthorized access, exploitation, or data exfiltration. DHS works with cybersecurity organizations from across the U.S. Government to gain access to a broad range of cyber threat information. ECS consists of the operational processes and security oversight required to share sensitive and classified cyber threat information with qualified Commercial Service Providers (CSP). The ECS program develops threat "indicators" with this information and provides CSPs with those indications of active, malicious cybersecurity activity to better protect their critical-infrastructure customers.

In fiscal year 2013, DHS has already shared more than 200,000 indicators via the ECS program and other Joint Indicator Bulletin products with partners for computer network defense. CSPs may use these threat indicators to provide approved cybersecurity services to critical infrastructure entities. ECS augments, but does not replace, entities' existing cybersecurity capabilities. The program was also built with privacy and civil liberties protections in mind. Consistent with their commercial agreements with the protected entities, CSPs are not required to share with the Government, but may voluntarily do so. The incident information is anonymized, unless the protected entity consents to having its identity provided to DHS.

COMBATING CYBER CRIME

DHS employs more law enforcement agents than any other department in the Federal Government and has personnel stationed in every State and in more than 75 countries around the world. Since 2009, DHS has prevented $10 billion in potential losses through cyber crime investigations and arrested more than 5,000 individuals for their participation in cyber crime activities.

The Department leverages the 31 USSS Electronic Crimes Task Forces (ECTF), which combine the resources of academia, the private sector, and local, State and Federal law enforcement agencies to combat computer-based threats to our financial payment systems and critical infrastructure. A recently executed partnership between ICE Homeland Security Investigations and USSS demonstrates the Department's commitment to leveraging capability and finding efficiencies. Both organizations will expand participation in the existing ECTFs. In addition to strengthening each agency's cyber investigative capabilities, this partnership will produce benefits with respect to the procurement of computer forensic hardware, software licensing, and training that each agency requires. The Department is also a partner in the National Cyber Investigative Joint Task Force, which serves as a collaborative entity that fosters information sharing across the interagency.

In fiscal year 2012, the Secret Service arrested 1,378 individuals for cyber-crime violations while maintaining a 99.6-percent conviction rate; these criminals were responsible for over $335 million in fraud losses and could have potentially caused over $1.2 billion in fraud loss based on financial account information in their possession at the time of their arrest. As part of its protective duties, the Secret Service has developed a Critical Systems Protection Program, which assesses and mitigates the risks to critical infrastructure that could impact Secret Service protectees or National Special Security Events (NSSEs). This program applies risk management practices developed by the National Institute of Standards and Technology to help critical infrastructure owners and operators secure their systems from cyber threats. From October 2009 to May 2013 this program has conducted over 560 advances and secured eight NSSEs.

In the course of investigating cyber crimes over the last 30 years, the Secret Service has developed a number of cybersecurity capabilities to support its mission. The backbone of the ECTFs is its Electronic Crimes Special Agent Program (ECSAP), which is comprised of nearly 1,400 Secret Service special agents who have received at least one of three levels of computer crimes-related training. These agents are deployed in more than 98 Secret Service offices throughout the world and have received training in forensic identification, preservation and retrieval of electronically stored evidence. ECSAP-trained agents are computer investigative specialists, qualified to conduct examinations on all types of electronic evidence. These special agents are equipped to investigate the continually evolving arena of electronic and cyber crimes and have proven invaluable in the successful prosecution of criminal groups involved in computer fraud, bank fraud, identity theft, access device fraud and various other electronic and cyber crimes targeting our financial institutions and private sector. USSS also supports State and local law enforcement, in addition to other Federal agencies, by making these capabilities available to support their operations.[1] They include computer forensics specialists, mobile wireless investigation teams, and advanced research support.

To expand its collaborative efforts, the Secret Service provides its ECSAP training to investigators at the ICE Computer Crimes Center as well as via the National Computer Forensics Institute (NCFI), which is a result of a partnership between the National Protection and Programs Directorate, the Secret Service, the State of Alabama, the City of Hoover, Shelby County, the Alabama District Attorney's Association, and the Alabama Securities Commission, established to provide computer forensic training and tools to State and local law enforcement officers, prosecutors, and judges. Investigators are trained to respond to network intrusion incidents and conduct electronic and cyber crimes investigations. This training also has the benefit of providing State and local law enforcement with the skills and tools to combat a myriad of crimes in their community. Further, the NCFI has supported training for DHS Fusion Centers and the FBI's National Domestic Communications Assistance Center. Responding to the growth of cyber crimes and the level of sophistication these criminals employ requires training, resources and greater collaboration among law enforcement and its public and private sector partners.

Since opening in May 2008, NCFI has trained more than 2,050 State and local officials, including more than 1,360 police investigators, 525 prosecutors and 165 judges from all 50 States and three U.S. territories.

In addition to these activities, ICE HSI's Cyber Crimes Center (C3) delivers computer-based technical services to support domestic and international investigations into cross-border crime. C3 is made up of the Cyber Crimes Unit, the Child Exploi-

[1] Included are the following:

—Computer forensics specialists, which in fiscal year 2012 conducted more than 7,000 digital forensics exams, totaling more than 1,100 terabytes of data;

—Cell Phone Forensics Facility at University of Tulsa, which since opening in 2008 has supported 6,135 exams, and 305 advanced exams at the University of Tulsa;

—22 Mobile Wireless Investigations Teams, which in fiscal year 2012 conducted nearly 1,140 investigations, supporting primarily State and local law enforcement with this advanced capability and directly contributing to solving homicide cases and locating missing persons;

—Advanced research support at Carnegie Mellon and development of advanced tools for use by law enforcement partners; and

—Support of landmark research studies, like the Insider Threat Report, Verizon Data Breach Investigations Report, and the Trust Wave Global Security Report, which are an effective way to share law enforcement information, while protecting victim privacy, to develop national understanding of cyber risks.

tation Investigations Unit and the Computer Forensics Unit. This state-of-the-art center offers cyber crime support and training to Federal, State, local and international law enforcement agencies. C3 also operates a fully equipped computer forensics laboratory, which specializes in digital evidence recovery, and offers training in computer investigative and forensic skills.

COOPERATION ACROSS THE FEDERAL GOVERNMENT

Successful response to dynamic cyber threats requires leveraging homeland security, law enforcement, national defense, and intelligence authorities and capabilities, which respectively promote domestic preparedness, criminal deterrence and investigation, and national defense. DHS, the Department of Justice (DOJ), and the Department of Defense (DOD) each play a key role in responding to cybersecurity incidents that pose a risk to the United States. To achieve a whole of government response to specific cyber incidents, DHS, DOJ, and DOD synchronize their operations. The leaders of DHS, DOJ, and DOD have held a series of meetings to clarify the lanes in the road in cyber jurisdiction. The group agreed that DHS' primary role is to protect critical infrastructure and networks, coordinate mitigation and recovery, disseminate threat information across various sectors and investigate cybercrimes under DHS's jurisdiction. DOJ is the lead for investigation, enforcement, and prosecution of those responsible for cyber intrusions affecting the United States. As part of DOJ, the FBI conducts domestic national security operations; investigates, attributes, and disrupts cybercrimes; and collects, analyzes, and disseminates domestic cyber intelligence. DOD's role is to defend the Nation, gather intelligence on foreign cyber threats, and to protect national security systems. DHS supports our partners in many ways. For example, the United States Coast Guard as an Armed Force has partnered with U.S. Cyber Command and U.S. Strategic Command to prepare for military cyberspace operations as directed. In coordination with DOS, DHS also works with international partners in strategic and operational engagements.

While each agency operates within the parameters of its authorities, the U.S. Government's response to cyber incidents of consequence is coordinated among these three agencies such that "a call to one is a call to all." Synchronization among DHS, DOJ, and DOD not only ensures that whole of Government capabilities are brought to bear against cyber threats, but also improves Government's ability to share timely and actionable cybersecurity information among a variety of partners, including the private sector.

PRESIDENTIAL POLICY DIRECTIVE 21 AND CYBER EXECUTIVE ORDER 13636

America's national security and economic prosperity are increasingly dependent upon the cybersecurity of critical infrastructure. With today's physical and cyber infrastructure growing more inextricably linked, critical infrastructure and emergency response functions are inseparable from the information technology systems that support them. The Federal Government's role in this effort is to share information and to encourage enhanced security and resilience, while also identifying gaps not filled by the marketplace. As mentioned previously, the enhanced information sharing programs supported by Executive Order 13636 and PPD–21 help secure critical infrastructure and increase its resilience against cyber and physical attacks, as well as natural disasters and terrorist attacks.

To complement PPD–21, Executive Order 13636 promotes more efficient sharing of cyber threat information with the private sector and directs the establishment of a cybersecurity framework to identify and implement better security practices among critical infrastructure sectors. Through partnerships between the Government and private sector, the critical infrastructure cyber systems upon which much of our economic well-being, national security, and daily lives depend are being better protected. PPD–21 and Executive Order 13636 reinforce holistic thinking and action in the realms of security and risk management and the issuance of these important documents allows us to build upon and enhance our existing partnership model with our key private sector and SLTT partners. Implementation of Executive Order 13636 and PPD–21 will also drive action toward system and network security and resilience. The Department is well positioned to make advances in the space defined by the cyber-physical security nexus that PPD–21 and Executive Order 13636 address.

BUDGET PRIORITIES

The fiscal year 2014 budget supports initiatives to secure our Nation's information and financial systems and to defend against cyber threats to private-sector and Federal systems, the Nation's critical infrastructure, and the U.S. economy. Taken together, the administration's initiatives strengthen the security and resilience of critical infrastructure against evolving threats through an updated and overarching national framework that acknowledges the linkage between cybersecurity and securing physical assets.

Included in the fiscal year 2014 budget are enhancements to the National Cybersecurity Protection System (NCPS) to prevent and detect intrusions on Government computer systems and to the National Cybersecurity and Communications Integration Center to protect against and respond to cybersecurity threats. The budget also leverages the new operational partnership between ICE and USSS through the established network of USSS ECTFs to safeguard the Nation's financial payment systems, combat cybercrimes, target transnational child exploitation including large-scale producers and distributors of child pornography, and prevent attacks against U.S. critical infrastructure.

—*Federal Network Security.*—$200 million is included for Federal Network Security, which manages activities designed to enable Federal agencies to secure their IT networks. The budget provides funding to further reduce risk in the Federal cyber domain by enabling continuous monitoring and diagnostics of networks in support of mitigation activities designed to strengthen the operational security posture of Federal civilian networks. DHS will directly support Federal civilian departments and agencies in developing capabilities to improve their cybersecurity posture and to better thwart advanced, persistent cyber threats that are emerging in a dynamic threat environment.

—*NCPS.*—$406 million is included for Network Security Deployment, which manages NCPS, operationally known as EINSTEIN. NCPS is an integrated intrusion detection, analytics, information-sharing, and intrusion-prevention system that supports DHS responsibilities to defend Federal civilian networks.

—*US–CERT.*—$102 million is included for operations of US–CERT, which leads and coordinates efforts to improve the Nation's cybersecurity posture, promotes cyber information sharing, and manages cyber risks to the Nation. US–CERT encompasses the activities that provide immediate customer support and incident response, including 24-hour support in the National Cybersecurity and Communications Integration Center. As more Federal network traffic is covered by NCPS, additional US–CERT analysts are required to ensure cyber threats are detected and the Federal response is effective.

—*SLTT Engagement.*—In fiscal year 2014, DHS will expand its support to the MS–ISAC to assist in providing coverage for all 50 States and 6 U.S. territories in its managed security services program. MS–ISAC is a central entity through which SLTT governments can strengthen their security posture through network defense services and receive early warnings of cyber threats. In addition, the MS–ISAC shares cybersecurity incident information, trends, and other analysis for security planning.

—*Cybersecurity Research and Development.*—The fiscal year 2014 budget includes $70 million for the Science and Technology Directorate's research and development focused on strengthening the Nation's cybersecurity capabilities.

—*Cyber Investigations.*—The fiscal year 2014 budget continues to support ICE and USSS to strategically investigate domestic and international criminal activities, including computer fraud, network intrusions, financial crimes, access device fraud, bank fraud, identity crimes and telecommunications fraud, benefits fraud, arms and strategic technology, money laundering, counterfeit pharmaceuticals, child pornography, and human trafficking occurring on or through the Internet. The budget continues to enable these DHS law enforcement agencies to provide computer forensics support and training for law enforcement partners to enable them to effectively investigate cyber crime and conduct other highly technical investigations. ICE projects a fiscal year 2014 expenditure of $13.8 million for the Cyber Crimes Center supporting investigations to identify, disrupt, and dismantle domestic and transnational criminal organizations engaged in crimes facilitated by use of computers and cyberspace. In addition, ICE expects to spend $96.5 million on investigations of cyber crime/child exploitation. Other investigations of illicit trade, travel and finance all make use of cyber investigative techniques including computer forensic analysis. The Secret Service's ECTFs will also continue to focus on the prevention of cyber attacks against U.S. financial payment systems and critical infrastructure through aggressive investigation and information sharing.

—*Cyber Protection.*—The fiscal year 2014 budget includes $13.5 million to enhance the Secret Service's ability to secure protective venues, National Special Security Events and associated Critical Infrastructure/Key Resources from cyber attacks.

CYBER LEGISLATIVE PRIORITIES

It is important to note that the Executive order directs Federal agencies to work within current authorities and increase voluntary cooperation with the private sector to provide better protection for computer systems critical to our national and economic security. It does not grant new regulatory authority or establish additional incentives for participation in a voluntary program. We continue to believe that a suite of legislation is necessary to implement the full range of steps needed to build a strong public-private partnership, and we will continue to work with the Congress to achieve this.

To help us achieve our mission, we have created a number of competitive scholarship, fellowship, and internship programs to attract top talent. We are growing our world-class cybersecurity workforce by creating and implementing standards of performance, building and leveraging a cybersecurity talent pipeline with secondary and post-secondary institutions nationwide, and institutionalizing an effective, ongoing capability for strategic management of the Department's cybersecurity workforce. Congress can support this effort by pursuing legislation that provides DHS with the hiring and pay flexibilities we need to secure Federal civilian networks, protect critical infrastructure, respond to cyber threats, and combat cybercrime.

CONCLUSION

The American people expect us to secure the country from the growing danger of cyber threats and ensure the Nation's critical infrastructure is protected. The threats to our cybersecurity are real, they are serious, and they are urgent. I appreciate this committee's guidance and support as, together, we work to keep our Nation safe.

STATEMENT OF RICHARD A. MCFEELY, EXECUTIVE ASSISTANT DIRECTOR, CRIMINAL, CYBER, RESPONSE, AND SERVICES BRANCH, FEDERAL BUREAU OF INVESTIGATION, DEPARTMENT OF JUSTICE

Mr. McFEELY. Good afternoon, Madam Chairwoman, Vice Chairman Shelby, and members of the committee.

It is difficult to overstate the potential impacts cyber threats pose to our economy, our national security, and the critical infrastructure upon which our country relies. That is why the FBI, along with our key partners sitting at the table here, are strengthening our cyber capabilities in the same way we enhanced our intelligence and national security capabilities in the wake of 9/11.

I want to talk briefly about what the FBI's response has been, but I echo both of these two gentlemen's comments that this is a whole of Government approach when it comes to addressing this issue.

In the last year within the FBI, we have undergone a paradigm shift in how we conduct cyber operations. While we previously watched, collected information, and added to our understanding of the adversaries' intentions, we did not always take action by seeking to disrupt them as we might in a counterterrorism case. We are now, working with our partners, successfully disrupting and impacting the individuals behind the keyboard who have made it their mission to attack, steal, spy, and commit terrorist acts against our Nation and its citizens. Instead of watching foreign countries steal our intellectual property, we are going out to companies and trying to prevent it.

For example, working with DHS, we now routinely provide private industry and our law enforcement partners overseas with IP addresses that are responsible for launching attacks against our country. Just last week, the FBI, Microsoft, and the financial services industry conducted separate but coordinated operations to successfully disrupt more than 1,000 botnets, networks of compromised computers that had been infected with a malware known as Citadel. The botnets were part of a massive global cyber crime operation estimated to be responsible for more than half a billion dollars in financial fraud.

These actions are part of a larger U.S. Government strategy led by the National Cyber Investigative Joint Task Force, or NCIJTF, to target botnet creators and distributors. They exemplify how the FBI and our partners are using private/public partnerships both domestically and internationally to protect the public from cyber criminals.

At the NCIJTF, which serves as the deconfliction center on cyber threat investigations among 19 U.S. and two international agencies, the Government is coordinating its efforts at an unprecedented level. This coordination involves senior personnel at key agencies. While it is led by the FBI, it now has Deputy Directors from the National Security Agency, DHS, the Central Intelligence Agency (CIA), the U.S. Secret Service, and U.S. Cyber Command.

We must recognize that to work together we have to make sure that we keep pace and surpass the capabilities of our cyber adversaries. As General Alexander described earlier, the leaders of the FBI, DHS, and NSA met last fall and clarified the lanes in the road to cyber jurisdiction. And I believe that the collective opinion among the worker levels is that there is now an unprecedented level of cooperation not seen since the immediate post-9/11 era.

In addition to strengthening our partnerships in Government, we have significantly enhanced our collaboration with the private sector. As part of that outreach, we have begun to provide industry partners with classified threat briefings and other information and tools to help repel intruders. Among these tools is a new platform we are developing for trusted industry partners to report cyber incidents to all of Government in real time. Known as iGuardian, it is based on a successful guardian terrorist threat tracking and collaboration system developed after 9/11. We are also developing an automated malware analysis tool to which law enforcement and industry partners could submit samples of malware for triage and analysis. We expect an unclassified version of this system to be piloted with the private sector this fall.

And while we have been primarily focused on cyber intrusions, which we see as the greatest cyber threat to our national security, we are working with our State and local law enforcement partners to identify and address gaps in the investigation and prosecution of Internet fraud crimes. The FBI, the U.S. Secret Service should not bear all responsibility for this. We believe that there is a huge space for our State and local partners to join us in this fight.

To address these gaps, we have developed a pilot program, in collaboration with the International Chiefs of Police and other law enforcement organizations to enhance the Internet fraud targeting packages that the FBI's Internet Crime Complaint Center, or IC3, currently provides to State and local law enforcement for investigation and potential prosecution.

I thank you for the opportunity to be here today and look forward to answering questions.

[The statement follows:]

PREPARED STATEMENT OF RICHARD A. MCFEELY

Good afternoon Chairwoman Mikulski, Vice Chairman Shelby, and members of the committee. I appreciate the opportunity to appear before you today to discuss the cyber threat, how the Federal Bureau of Investigation (FBI) has responded to it, and how we are marshaling our resources and strengthening our partnerships to more effectively combat the increasingly sophisticated adversaries we face in cyberspace.

THE CYBER THREAT

As the committee is well aware, the frequency and impact of cyber attacks on our Nation's private sector and government networks have increased dramatically in the past decade, and are expected to continue to grow. Since 2002, the FBI has seen an 84-percent increase in the number of computer intrusion investigations.

Our adversaries in the cyber realm include spies from nation-states who seek our secrets and intellectual property; organized criminals who want to steal our identities and money; terrorists who aspire to attack our power grid, water supply, or other infrastructure; and hacktivist groups who are trying to make a political or social statement. It is difficult to overstate the potential impact these threats pose to our economy, our national security, and the critical infrastructure upon which our country relies. The bottom line is we are losing data, money, ideas, and innovation to a wide range of cyber adversaries and much more is at stake.

Director Mueller has said he expects the cyber threat to surpass the terrorism threat to our Nation in the years to come. That is why we are strengthening our cyber capabilities in the same way we enhanced our intelligence and national security capabilities in the wake of the September 11th attacks.

FEDERAL BUREAU OF INVESTIGATION RESPONSE

The FBI recognized the significance of the cyber threat more than a decade ago and, in response, created the Cyber Division and elevated the cyber threat to our number three national priority (only after counterterrorism and counterintelligence). We also significantly increased our hiring of technically trained agents, analysts, and forensic specialists and expanded our partnerships with law enforcement, private industry, and academia.

We have made great progress since the Cyber Division was first created in 2002. Prior to that, we considered it a success when we recognized that networks were being attacked. We soon enhanced our ability to determine attribution knowing who was breaking into our computers and networks and to track Internet Protocol (IP) addresses back to their source. Now, the question we ask ourselves is, "How are we going to take action on that information?"

The perpetrators of these attacks are often overseas, but in the past, tracking an IP address back to its source in a foreign country usually led to a dead end. To address this problem, we embedded cyber agents with law enforcement in several key countries, including Estonia, Ukraine, the Netherlands, Romania, and Latvia. We have also worked with several of these countries to extradite subjects from their countries to stand trial in the United States.

Building on the success of our international outreach, we are currently expanding our Cyber Assistant Legal Attaché program to the United Kingdom (U.K.), Singapore, Bulgaria, Australia, Canada, the Republic of Korea, and Germany.

RECENT SUCCESSES

A prime example of international collaboration came in the 2011 takedown of Rove Digital, a company founded by a ring of Estonian and Russian hackers to commit a massive Internet fraud scheme. The scheme infected more than 4 million computers in more than 100 countries with malware. The malware secretly altered the settings on infected computers, enabling the hackers to hijack Internet searches using rogue servers for Domain Name System (DNS) routers and re-route computers to certain Web sites and ads. The company received fees each time these Web sites or ads were clicked on or viewed by users and generated $14 million in illegitimate income for the operators of Rove Digital.

Following the arrest of several alleged co-conspirators in Estonia, FBI agents, linguists, and forensic examiners assisted Estonian authorities in retrieving and analyzing data linking them to the scheme. Seven individuals have been indicted in the Southern District of New York in this case. Two of the six for which the United States sought extradition have been remanded to U.S. custody and have recently pleaded guilty to wire fraud and computer intrusion.

While the FBI and our partners have had multiple recent investigative successes against the threat, we are continuing to push ourselves to respond more rapidly and prevent attacks before they occur.

One area in which we have had great success with our overseas partners recently is in targeting infrastructure we believe has been used in Distributed Denial of Service (DDOS) attacks, and preventing it from being used for future attacks. Since October 2012, the FBI and the Department of Homeland Security (DHS) have released nearly 168,000 Internet Protocol addresses of computers that were believed to be infected with DDOS malware. We have released this information through Joint Indicator Bulletins (JIBs) to more than 130 countries via DHS' National Cybersecurity and Communications Integration Center Team as well as our Legal Attachés.

These actions have enabled our foreign partners to take action and reduced the effectiveness of the botnets and the DDOS attacks. We are continuing to target botnets through this strategy and others.

NEXT GENERATION CYBER

The need to prevent attacks is a key reason we have redoubled our efforts to strengthen our cyber capabilities while protecting privacy, confidentiality, and civil liberties. The FBI's Next Generation Cyber Initiative, which we launched in 2012, entails a wide range of measures, including focusing the Cyber Division on intrusions into computers and networks—as opposed to crimes committed with a computer as a modality; establishing Cyber Task Forces in each of our 56 field offices to conduct cyber intrusion investigations and respond to significant cyber incidents; hiring additional computer scientists to assist with technical investigations in the field; and expanding partnerships and collaboration at the National Cyber Investigative Joint Task Force (NCIJTF).

At the NCIJTF—which serves as a coordination, integration, and information sharing center among 19 U.S. agencies and two foreign governments for cyber threat investigations—we are coordinating at an unprecedented level. This coordination involves senior personnel at key agencies. NCIJTF, which is led by the FBI, now has deputy directors from the National Security Agency (NSA), DHS, the Central Intelligence Agency, U.S. Secret Service, and U.S. Cyber Command. We recently invited our Five Eyes partners to join us at the NCIJTF. Australia agreed, and embedded personnel there in May. The U.K. is scheduled to do so in July 2013. By developing partnerships with these and other nations, NCIJTF is working to become the international leader in synchronizing and maximizing investigations of cyber adversaries.

We recognize that we must work together more efficiently than ever to keep pace with and surpass our cyber adversaries. To that end, the leaders of the FBI, DHS, and NSA recently held a series of meetings to clarify the lanes in the road in cyber jurisdiction. The group agreed that the Department of Justice (DOJ) is the lead for investigation, enforcement, and prosecution of those responsible for cyber intrusions affecting the United States. As part of DOJ, the FBI conducts domestic national security operations; investigates, attributes, and disrupts cybercrimes; and collects, analyzes, and disseminates domestic cyber intelligence. DHS's primary role is to protect critical infrastructure and networks, coordinate mitigation and recovery, disseminate threat information across various sectors and investigate cybercrimes under DHS's jurisdiction. The Department of Defense's role is to defend the Nation, gather intelligence on foreign cyber threats, and to protect national security systems.

Earlier this year, the U.S. Intellectual Property Enforcement Coordinator released the administration's Strategy on Mitigating the Theft of U.S. Trade Secrets. As part of the strategy, the Department of Justice, including the FBI, will continue to prioritize prosecutions and investigations of foreign corporate and state-sponsored trade secret theft. Further, the FBI is expanding its efforts to fight computer intrusions that involve the theft of trade secrets by individuals, foreign corporations, and nation-state cyber hackers.

While we are primarily focused with our Federal partners on cyber intrusions, we are also working with our State and local law enforcement partners to identify and address gaps in the investigation and prosecution of Internet fraud crimes.

Currently, the FBI's Internet Crime Complaint Center (IC3) collects reports from private industry and citizens about online fraud schemes, identifies emerging trends, and produces reports about them. The FBI investigates fraud schemes that are appropriate for Federal prosecution (based on factors like the amount of loss). Others are packaged together and referred to State and local law enforcement. However, we have learned that very few of these referred cases are being worked.

To close this gap, we have developed a pilot program in collaboration with the International Association of Chiefs of Police, the Major City Chiefs Association, and the National Sheriffs' Association to enhance the Internet fraud targeting packages IC3 provides to State and local law enforcement for investigation and potential prosecution. During the first phase of the pilot, IC3 will develop better investigative leads for direct dissemination to State and local agencies, beginning with the Utah Department of Public Safety.

PRIVATE SECTOR OUTREACH

In addition to strengthening our partnerships in government and law enforcement, we recognize that to effectively combat the cyber threat, we must significantly enhance our collaboration with the private sector. Our Nation's companies are the primary victims of cyber intrusions and their networks contain the evidence of countless attacks.

In the past, industry has provided us information about attacks that have occurred, and we have investigated the attacks, but we have not always provided information back. We realize the flow of information must go both ways. As part of our enhanced private sector outreach, we have begun to provide industry partners with classified threat briefings and other information and tools to help them repel intruders.

Among them is a new platform we are developing for trusted private industry partners to report cyber incidents to us in real time. Known as iGuardian, it is based on the FBI's successful Guardian terrorist threat tracking and collaboration system. Guardian has also been enhanced to accept cyber incident reporting from fusion centers and State and local law enforcement.

Over the past year, we have been engaged in classified briefs on nearly a daily basis at NCIJTF with private-sector partners and representatives of our Nation's most critical infrastructure sectors. Earlier this year, in coordination with the Treasury Department, we provided a classified briefing on threats to the financial services industry to executives of more than 40 banks who participated via secure video teleconference in FBI field offices around the country.

In addition to these actions, we are also expanding our partnerships with private industry and academia through initiatives like InfraGard—a public-private coalition of 55,000 members to protect critical infrastructure—and the National Cyber-Forensics and Training Alliance, a proven model for sharing private sector information in collaboration with law enforcement.

FISCAL YEAR 2014 BUDGET REQUEST

The combined result of these actions is that the FBI has undergone a paradigm shift over the past year in how we are responding to the cyber threat, particularly national security cyber threats. While we previously watched, collected information, and added to our understanding of our nation-state adversaries' intentions, we are now looking to disrupt and deter the individuals behind the keyboard who have made it their mission to attack, steal, spy, and commit terrorist attacks against our Nation and its citizens.

Instead of watching foreign countries steal our intellectual property, we're going out to companies and trying to prevent it. For example, in coordination with DHS, we will provide organizations with IP addresses that are likely to launch attacks against them or the e-mail addresses used to send their employees messages with links to malicious software, in a technique known as "spearphishing."

Undertaking these new actions and initiatives requires additional personnel and other resources. That is why, to help the FBI combat this rapidly developing and diverse threat, the fiscal year 2014 budget request includes an additional 152 positions (60 Special Agents, 1 Intelligence Analyst, and 91 Professional Staff) and $86.6 million to help address this threat.

CONCLUSION

In conclusion, Chairwoman Mikulski, to counter the threats we face, we are engaging in an unprecedented level of collaboration within the U.S. Government, with the private sector, and with international law enforcement.

We are grateful for the committee's support and look forward to continuing to work with you and expand our partnerships as we determine a successful course forward for the Nation to defeat our cyber adversaries.

Thank you again for the opportunity to be here today. I would be happy to answer any questions you may have.

STATEMENT OF HON. DR. PATRICK D. GALLAGHER, ACTING DEPUTY SECRETARY, DEPARTMENT OF COMMERCE; DIRECTOR, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

Chairwoman MIKULSKI. Dr. Gallagher.

Dr. GALLAGHER. Thank you. Chairwoman Mikulski and Vice Chairman Shelby, members of the committee, it is a distinct pleasure to be here today to join my colleagues to talk to you about cybersecurity.

Since I am batting cleanup, I want to touch quickly on just two topics.

First is the all-of-Government approach. Good teamwork is based on playing your position, and the NIST position is based on our mission. We are a measurement science and standards organization, and our role is to support industry, the owners and operators of this infrastructure, as they respond to the information that they get from our Intelligence Community, from our law enforcement community, and from Homeland Security.

This is a top priority for NIST. In our fiscal year 2014 budget request, there was a $24 million increase to cybersecurity R&D programs at NIST. This is on top of making our total investment of $68 million. This funding enables our R&D performance in a number of critical areas, including the National Initiative for Cybersecurity Education, an interagency effort; the National Strategy for Trusted Identities in Cyberspace; the National Cybersecurity Center of Excellence; and implementation of Executive Order 13636, “Improving Critical Infrastructure Cybersecurity.”

Second, I would like to give you a quick update on the Executive order. As many of you know, under the order, NIST has been directed to work with industry to develop a framework of cybersecurity practices, methods, and so forth that supports the performance goals established by the Department of Homeland Security. For this to be successful, two major elements have to be part of the approach.

First is an effective partnership between the agencies, and that is occurring. In fact, we memorialized this with a memorandum of understanding between DHS and NIST and with close working collaborations with my colleagues here.

And second, the cybersecurity framework must be developed through a process that is industry-led, open and transparent to all of the stakeholders because it is by having industry develop their own practices that are responsive to the performance goals that we end up with an output that is technically robust, because it draws on their expertise, and is aligned with business interests and practice.

This is not a new or novel or approach for NIST. We have utilized a similar approach in the recent past to address other national priorities, including the smart grid and cloud computing.

Madam Chair, I appreciate the challenge before us. The Executive order is very aggressive in the timing for the framework process. It is to be developed within 1 year. The first draft is due in 120 days. Today marks the halfway point in that process. We have issued, in support of this effort, a request for information and have gathered input from industry and other stakeholders. We have held the first two of four planned workshops to support this process, and we will use these workshops to finalize and develop the framework because it is this type of approach that allows us the appropriate level of collaboration and engagement with industry.

In May, we released the initial findings and the early analysis from the request for information. That release marks the transition from sort of gathering facts to actually building the framework. In 8 months, we will have an initial draft of the framework, including an initial list of standards, guidelines, and practices, and then following that, we will work with our agency partners to finalize the framework. But even after the framework is done, the work is really only just beginning. Adoption and use of the framework is going to raise new issues to address. The goal at the end of this process is for industry to adopt the framework themselves so it becomes an ongoing process that enhances cybersecurity.

The President's Executive order lays out an urgent and ambitious agenda, but it is designed around an active collaboration between the public and private sectors, and I wholeheartedly believe that partnership is the essential ingredient for its success.

In short, the cybersecurity challenge, both in the dot-gov and in the dot-com domain, is greater than it has ever been. Active collaboration among the private sector and between the public and private sectors is really the only way we can meet this challenge, leveraging both sides' roles, responsibilities, and capabilities.

And we have a lot of work, and I look forward to working with this committee to make it happen. Thank you.

[The statement follows:]

Prepared Statement of Hon. Dr. Patrick D. Gallagher

Chairwoman Mikulski, Vice Chairman Shelby, members of the committee, I am Patrick Gallagher, Under Secretary of Commerce for Standards and Technology and Director of the National Institute of Standards and Technology (NIST), a nonregulatory bureau within the U.S. Department of Commerce. I am also currently serving as the Acting Deputy Secretary of Commerce. Thank you for this opportunity to testify today on NIST's roles and responsibility for cybersecurity.

THE ROLE OF THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY IN CYBERSECURITY

NIST's overall mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life. Our work in addressing technical challenges related to national priorities has ranged from projects related to the Smart Grid and electronic health records to atomic clocks, advanced nanomaterials, and computer chips.

In the area of cybersecurity, NIST has worked with Federal agencies, industry, and academia since 1972, when it was given the responsibility for the development of the Data Encryption Standard. Our role to research, develop and deploy information security standards and technology to protect information systems against threats to the confidentiality, integrity and availability of information and services, was then strengthened through the Computer Security Act of 1987 and reaffirmed through the Federal Information Security Management Act of 2002.

Consistent with our mission, NIST actively engages with industry, academia, and other parts of the Federal Government including the Intelligence Community, and with elements of the law enforcement and national security communities. These collaborations inform our efforts in coordinating and prioritizing cybersecurity research, standards development, standards conformance demonstration and cybersecurity education and outreach.

Our broader work in the areas of information security, trusted networks, and software quality is applicable to a wide variety of users, from small and medium enterprises to large private and public organizations including agencies of the Federal Government and companies involved with critical infrastructure.

We employ collaborative partnerships with our customers and stakeholders in industry, government and academia, to take advantage of their technical and operational insights and to leverage the resources of a global community. These collaborative efforts and our private sector collaborations in particular, are constantly being expanded by new initiatives, including in recent years through the National Initiative for Cybersecurity Education (NICE), National Strategy for Trusted Identities in Cyberspace (NSTIC), the National Cybersecurity Center of Excellence (NCCoE), and through development of the Cybersecurity Framework under Executive order (EO) 13636, “Improving Critical Infrastructure Cybersecurity.”

My testimony has four parts today: I’ll discuss the role of NIST in protecting Federal information systems; our engagement with industry; our work under the President’s Executive order; and how our funding supports all of those efforts.

THE ROLE OF THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY IN PROTECTING FEDERAL INFORMATION SYSTEMS

The E-Government Act of 2002, Public Law 107–347, recognized the importance of information security to the economic and national security interests of the United States. Title III of the E-Government Act, known as the Federal Information Security Management Act of 2002 (FISMA), included duties and responsibilities for the National Institute of Standards and Technology to develop standards and guidelines for Federal information systems.

The NIST Special Publications (SPs) and Interagency Reports (IRs) provide management, operational, and technical security guidelines for Federal agencies and cover a broad range of topics such as BIOS management and measurement, key management and derivation, media sanitization, electronic authentication, security automation, Bluetooth and wireless protocols, incident handling and intrusion detection, malware, cloud computing, public key infrastructure, risk assessments, supply chain risk management, authentication, access control, security automation and continuous monitoring.

Beyond these documents—which are peer-reviewed throughout industry, government, and academia—NIST conducts workshops, awareness briefings, and outreach to ensure comprehension of standards and guidelines, to share ongoing and planned activities, and to aid in scoping guidelines in a collaborative, open, and transparent manner.

In support of FISMA implementation, in recent years NIST has strengthened its collaboration with the Department of Defense, the Intelligence Community, and the Committee on National Security Systems, through the Joint Task Force Transformation Initiative, which continues to develop key cybersecurity guidelines for protecting Federal information and information systems for the Unified Information Security Framework.

This collaboration allows the most broad-based and comprehensive set of safeguards and countermeasures ever developed for information systems. This unified framework provides a standardized method for expressing security at all levels, from operational implementation to compliance reporting. It allows for an environment of information sharing and interconnections among these communities and significantly reduces costs, time, and resources needed for finite sets of systems and administrators to report on cybersecurity to multiple authorities.

To support agency implementation of cloud technology, NIST has worked with the General Services Administration (GSA) to help establish the Federal Risk and Authorization Management Program (FedRAMP) to identify security assessment requirements, and prototype a process for approving Third-Party Assessment Organizations (3PAOs) that demonstrate capability in assessing Cloud Service Provider (CSP) information systems for conformance to identified standards and guidelines.

Given the Department of Homeland Security’s (DHS’s) important role in Federal agency cybersecurity, our partnership with DHS informs NIST’s collaborative efforts. Earlier in the year I signed a Memorandum of Agreement with DHS Undersecretary Rand Beers to ensure that our work with industry on cybersecurity standards, best practices, and metrics is fully integrated with the information sharing, threat analysis, response, and other work of DHS. We believe this will help enable a more holistic approach to addressing the complex nature of the challenge facing Federal agencies.

THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY'S ENGAGEMENT WITH INDUSTRY

It is important to note that the impact of NIST's activities under FISMA extend beyond providing the means to protect Federal IT systems. They provide the cybersecurity foundations for the public trust that is essential to our realizing the national and global productivity and innovation potential of electronic business and its attendant economic benefits. Many organizations voluntarily follow these standards and guidelines, reflecting their wide acceptance throughout the world.

Beyond our responsibilities under FISMA, under the provisions of the National Technology Transfer and Advancement Act, Public Law 104–113, and related OMB Circular A–119, NIST is tasked with the key role of encouraging and coordinating Federal agency use of voluntary consensus standards and participation in the development of relevant standards, as well as promoting coordination between the public and private sectors in the development of standards and in conformity assessment activities. NIST works with other agencies, such as the State Department, to coordinate standards issues and priorities with the private sector through consensus standards organizations such as the American National Standards Institute (ANSI), the International Organization for Standardization (ISO), the Institute of Electrical and Electronic Engineers (IEEE), the Internet Engineering Task Force (IETF), and the International Telecommunication Union (ITU).

A partnership with industry to develop, maintain, and implement voluntary consensus standards related to cybersecurity best practices promotes the interoperability, security and resiliency of this global infrastructure and makes us all more secure. It also allows this infrastructure to evolve in a way that embraces both security and innovation—allowing a market to flourish to create new types of secure products for the benefit of all Americans.

NIST also conducts cybersecurity research and development in areas such as security for Federal mobile environments and techniques for measuring and managing security. These efforts focus on improving the cybersecurity of current and future information technologies, and on improving the trustworthiness of IT components such as claimed identities, data, hardware, and software for networks and devices.

In addition, NIST recognizes that further development of cybersecurity standards will be needed to improve the security and resiliency of critical U.S. information and communication infrastructure. The availability of cybersecurity standards and associated conformity assessment schemes is essential to these efforts, which will help enhance the deployment of sound security solutions and build trust among those creating and those using the solutions throughout the country.

Additionally, the State of Maryland, Montgomery County, and NIST have jointly established the National Cybersecurity Center of Excellence (NCCoE), a public-private collaboration for accelerating the widespread adoption of cybersecurity technologies. Through the creation of standards-based reference designs, templates, and example "builds," the NCCoE will reduce barriers for companies that see the deployment of more secure technologies as too costly, too complicated, or technically infeasible. Reducing these economic, educational, and technical barriers to adoption can improve the security posture, and increase the competitiveness, of U.S. industry.

The NCCoE tackles some of the most pressing cybersecurity challenges identified by the members of one or more economic sectors. These challenges are then synthesized into specific "use cases" that include technical details that allow the NCCoE to develop an integrated solution based on commercially available technology. All of this work is done in an open and collaborative process: the use cases are published for public comment on the NCCoE Web site; the solutions are developed in collaboration with the private sector, other government agencies, and academia; the NCCoE hosts workshops and public meetings to exchange expertise and validate the practicality of the solutions under development; and when complete, the entire set of material necessary to recreate the NCCoE example solution is made available to the public.

The NCCoE is a unique opportunity that brings together, under one roof, experts from industry, government, and academia to develop practical, interoperable, and usable cybersecurity solutions. The center collaborates with the private sector primarily through three channels:

—*A Sector Community of Interest.*—Open to the public, with primary participation drawn from sector-specific businesses (e.g., healthcare, financial services, energy, etc.).

—*National Cybersecurity Excellence Partnership Companies.*—U.S. IT and cybersecurity companies that have committed to share technology and engineering staff with the NCCoE on persistent basis.

—*Use Case Collaborators.*—Companies that are providing a secure technology and engineering expertise as a part of an integrated solution for a specific use case.

The National Strategy for Trusted Identities in Cyberspace (NSTIC) is another key area in which NIST engages with industry. Under NSTIC, NIST is working with a wide array of stakeholders on creation of an online environment—the "Identity Ecosystem"—that addresses the myriad security and convenience problems caused by passwords, and allows individuals and organizations to better trust one another, with minimized disclosure of personal information. The Identity Ecosystem will be a user-centric online environment, supported by a framework of technologies, policies, and agreed-upon standards, which will enable individuals to transact business in a way that is more secure, convenient and privacy-enhancing everywhere they go online.

In the Identity Ecosystem, consumers will be able to choose in the marketplace from a variety of identity solutions—both private and public—that would issue trusted credentials that could be used in lieu of passwords across the Internet. Key attributes of the Identity Ecosystem include privacy, convenience, efficiency, ease-of-use, security, confidence, innovation, and choice. Creating this Identity Ecosystem requires a partnership between the private sector, advocacy groups, public sector agencies and others—all of whom are currently working to support NSTIC by collaborating in the privately led Identity Ecosystem Steering Group (IDESG). The request continues and expands existing efforts to coordinate Federal activities needed to implement NSTIC.

NIST also supports the continued work under the National Initiative for Cybersecurity Education (NICE). As we all know, cybersecurity is much more than technological solutions to technical problems; it is also highly dependent on educated users who are aware of and routinely employ sound practices when dealing with cyberspace. NIST will continue to work with the Federal Government, and with State, local, and tribal governments, for improving cybersecurity education. NIST will ensure coordination, cooperation, focus, public engagement, technology transfer, and sustainability of NICE. NIST works with DHS and other Federal agencies in the implementation of the cybersecurity education framework to address national cybersecurity awareness, formal cybersecurity education, Federal cybersecurity workforce structure, and cybersecurity workforce training and professional development.

Small businesses face particular cybersecurity challenges, as they tend to have more limited resources that must be well applied to meet the most obvious and serious threats. The vulnerability of any individual small business may not seem significant, other than to the owner and employees of that business. However, given that over 95 percent of all U.S. businesses are small- and medium-size businesses (SMBs), a vulnerability common to a large percentage of SMBs poses a threat to the Nation's economic base. SMBs frequently cannot justify an extensive security program or a full-time expert. Nonetheless, they confront serious security challenges and must address security requirements based on identified needs.

Cognizant of the needs of SMBs, NIST partners with the Small Business Administration (SBA) and the Federal Bureau of Investigation's InfraGard program to sponsor computer security workshops and provide online support for small businesses. Through these efforts, experts in computer security are made available to offer small business owners an overview of information security threats, vulnerabilities, and corresponding protective tools and techniques, with a special emphasis on providing useful information that small business personnel can apply directly or use to task contractor personnel.

In fiscal year 2012, NIST, SBA, and the FBI hosted 25 small business information security workshops in Oklahoma, Louisiana, Colorado, New Hampshire, Connecticut, Minnesota, Texas, California, Indiana, Ohio, and New Mexico, and provided online support to SMBs throughout the United States.

THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY'S ROLE IN EXECUTIVE ORDER 13636, "IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY"

As you know, on February 13, 2013, the President signed Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," which gave NIST the responsibility to develop a framework to reduce cyber risks to critical infrastructure (the Cybersecurity Framework). As directed in the Executive order, NIST, working with industry, will develop the Cybersecurity Framework and the Department of Homeland Security (DHS) will establish performance goals. DHS, in coordination with sector-specific agencies, will then support the adoption of the Cybersecurity Framework by owners and operators of critical infrastructure and other interested entities, through a voluntary program. NIST is also working closely with partners throughout the interagency—including the Intelligence Community—to ensure that the Framework leverages their expertise and role as the Framework is developed.

A Cybersecurity Framework is an important element in addressing the challenges of improving the cybersecurity of our critical infrastructure. A NIST-coordinated and industry-led Framework will draw on standards and best practices that industry already develops and uses. NIST coordination will ensure that the process is open and transparent to all stakeholders, and will ensure a robust technical underpinning to the framework. This approach will significantly bolster the relevance of the resulting Framework to industry, making it more appealing for industry to adopt.

This multi-stakeholder approach leverages the respective strengths of the public and private sectors, and helps develop solutions in which both sides will be invested. The approach does not dictate solutions to industry, but rather facilitates industry coming together to offer and develop solutions that the private sector is best positioned to embrace. Any efforts to better protect critical infrastructure need to be supported and implemented by the owners and operators of this infrastructure.

Underlying all of this work, NIST sees its role in developing the Cybersecurity Framework as partnering with industry and other stakeholders to help them develop the Framework. In addition to this critical convening role, our work will be to compile and provide guidance on principles that are applicable across the sectors for the full range of quickly evolving threats, based on inputs from DHS and other agencies. NIST's unique technical expertise in various aspects of cybersecurity related research, technology development and an established track record of working with a broad cross-section of industry and government agencies in the development of standards and best practices positions us very well to address this significant national challenge in a timely and effective manner.

NIST's initial steps towards implementing the Executive order included issuing a Request for Information (RFI) in February to gather relevant input from industry and other stakeholders, and asking stakeholders to participate in the Cybersecurity Framework process. NIST is following up the RFI process with continued engagement with stakeholders through a series of workshops and events to ensure that we can cover the breadth of considerations that will be needed to make this national priority a success. We have already initiated an aggressive outreach program to raise awareness of this issue and begin engaging industry and stakeholders. NIST will continue to bring many diverse stakeholders to the table. Last week, a 3-day workshop hosted by Carnegie Mellon University in Pittsburgh allowed NIST to engage with stakeholders to discuss the foundations of the Framework and the initial analysis.

The Executive order requirement for the Framework to be developed within 1 year, and a preliminary framework due within 8 months gives this task a sense of urgency. Throughout the year, you can expect NIST to use its capabilities to gather the input needed to develop the Framework.

In a year's time, once we have developed an initial Framework, we will continue to need to work with DHS, sector-specific agencies, and the specific sectors themselves to build strong voluntary programs for specific critical infrastructure areas. Their work will then inform the needs of critical infrastructure and the next versions of the Framework. The goal at the end of this process will be for industry to take and manage the Cybersecurity Framework—allowing it to evolve when needed.

Although this Executive order will help raise the Nation's cyber defenses, it does not eliminate the urgent need for legislation in these and other areas of cybersecurity. The administration's legislative priorities for the 113th Congress build upon the President's 2011 cybersecurity legislative proposal and take into account 2 years of public and congressional discourse about how best to improve the Nation's cybersecurity.

The administration is working toward legislation that:

—Facilitates cybersecurity information sharing between the Government and the private sector as well as among private sector companies. We believe that such sharing can occur in ways that protect privacy and civil liberties protections, reinforce the appropriate roles of civilian and intelligence agencies, and include targeted liability protections;

—Incentivizes the adoption of best practices and standards for critical infrastructure by complementing the process set forth under the Executive order;

—Gives law enforcement the tools to fight crime in the digital age;

—Updates Federal agency network security laws, and codifies DHS' cybersecurity responsibilities; and

—Creates a national data breach reporting requirement.

In each of these legislative areas, the right privacy and civil liberties safeguards must be incorporated. The administration wants to continue the dialogue with the

Congress and stands ready to work with members of Congress to incorporate our core priorities to produce cybersecurity information sharing legislation that addresses these critical issues.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY SUPPORT FOR CYBER RESEARCH AND DEVELOPMENT

As highlighted today cybersecurity is a top priority for NIST, which has been reflected in our recent budget requests. In fiscal year 2013 NIST has proposed to increase cybersecurity spending by $7.5 million with most of this increase supporting NIST's efforts to develop a framework to reduce cyber risks to critical infrastructure in support of the EO. In the President's fiscal year 2014 budget request NIST has requested a $24 million increase to its cybersecurity research and development (R&D) programs for a total NIST investment in cybersecurity and related efforts of $68 million. The requested increases for NIST in fiscal year 2014 will provide additional support for NIST's roles in cyber education, identity management, and will support R&D to improve the security and interoperability of our Nation's cyberspace infrastructure, accelerate the development and adoption of cybersecurity standards in support of administration priorities, and to support the leading-edge work of the National Cybersecurity Center of Excellence (NCCoE).

CONCLUSION

The cybersecurity challenge facing critical infrastructure—both in the "dot-gov" and the "dot-com"—is greater than it ever has been. Active collaboration within the public sector, and between the public and private sectors, is the only way to effectively meet this challenge, leveraging both sectors' roles, responsibilities, and capabilities.

Thank you for the opportunity to present NIST's views regarding cybersecurity security challenges. I appreciate the committee holding this hearing. I look forward to working with the committee to help address these pressing challenges. I will be pleased to answer any questions you may have.

Chairwoman MIKULSKI. Thank you very much, Dr. Gallagher and all four witnesses.

Today the way we will function is we will follow the 5-minute rule. We will go in order of arrival.

We also know that this hearing does not preclude the subcommittees from also continuing their own hearings where they will even probe more deeply. And also, after we have concluded all of our questioning, we will also understand that there will be certain aspects—in order to drill down, we will also have an additional classified forum this afternoon in the classified section in the Capitol Visitor Center. But now we will be in full and open session, not precluding further hearings by the subcommittees.

General Alexander—well, to all, just to reiterate the President's budget, the President has requested $9.2 billion for DOD: $1.2 billion, almost $1.3 billion, for DHS; for all of DOJ, including the FBI, $589 million; $215 million for Commerce, primarily in NIST; the National Science Foundation, $197 million; General Service Administration, $50 million; Department of State, $37 million.

When one hears $13 billion, that is a lot of money. However, we are in an enduring war where our citizens are under attack from identity theft to State secrets, trade secrets, business secrets, et cetera.

But our question today is, is $13 billion adequate in the various areas? Number one. And number two, when we spend the $13 billion, will we also avoid the kind of things where—sometimes we throw money at a new problem, and often we have what I call techno-boondoggles. We have seen it at the FBI in the past. We have seen in Homeland Security in the past. We have seen it at DOD. So this is what we are doing.

But let us go right to the President's request and the purpose. As I understand from the administration's priorities, the administration's priority—and if you look in the budget statement to us—secure the Federal networks, lead by example and make sure our networks are safe and secure, protect critical infrastructure, improve incident response, engage internationally. Number three, shape the future.

General Alexander, you will be getting—if we pass this budget where the request is for $9 billion, I understand that $3.5 billion will be to protect the DOD network. We understand that. But what will you use the other $5.8 billion to do and how will we get security for that dollar and avoid the problems of the past?

General ALEXANDER. Well, thanks, Senator. It is a lot of money, and I can tell you that from our perspective, what we are talking about here is not just protecting our networks, but developing the forces that we need. So part of that money goes for training and outfitting the teams at Cyber Command and our components need. Part of that money goes for the information assurance and fixing the networks—you hit on part of that—and developing future architectures.

So when I look at this from my perspective, I believe this is right, the right amount. I know the administration and the Defense Department has already looked internally to this budget to see where we can take cuts, and we did. We cut it back to what we thought was the minimum that we could use and still do this job.

You pointed out, Senator, that for the Defense Department, our job is to protect the Nation and our networks and building up the infrastructure that we need both within DOD and amongst the services and Cyber Command. That is where that $5.8 billion goes. So it is split across all those. It does not go to one lump. It helps each of the services, Defense Intelligence Agency, and Cyber Command do their missions.

$2.17 billion, as you pointed out and others, goes to NSA for doing their job and is part of the intel community's budget. So that is rolled in there as well.

$582 million goes to U.S. Cyber Command, and that is for five key areas: leases for teams, setting up the teams, training our teams, starting the military construction to have a place to house these teams, for our headquarters, and for research, development, training, another $68 million.

So I think it is the right number. I think we have looked at where we could take savings and have done that. I also think it is important to state that the Department sees this as an area to help ensure the Nation is ready as we look at the rest of our force posture. This is going to be key to our future.

That is all I have, Senator.

Chairwoman MIKULSKI. Just a follow-on question. In your testimony—this goes to protecting critical infrastructure, an obsession I think of this committee and something we have concentrated on very keenly when we were working on authorizing legislation under Lieberman-Collins, or Collins-Lieberman, or now Collins and a lot of us.

But in your testimony, sir, you say from 0 to 10 in our capacity to defend our critical infrastructure, you rate us at a 3. A 3. A 3 to protect our grid, a 3 to protect our financial services. And my question then is of the money that you are getting, I understand Homeland Security is supposed to protect us against domestic threats. Where do you come in and where does Homeland Security come in? And is part of your money also used to do the services to support them?

General ALEXANDER. Well, we do work together, but our monies—they are not overlapping in this case, as you point out.

Specifically, the Defense Department has two sets of roles and responsibilities here. One, to build, operate, and defend the DOD networks. That is the one responsibility and that is a big cost because that is our global forces, and that is the biggest bulk of the money that is here. The second part is to develop the teams to defend the Nation from a cyber attack, and that is where we come in.

Now, we work with DHS. We work with FBI in setting up the op centers and funding and supporting those op centers so that we can communicate amongst us, but DHS has that responsibility to work with industry to set the standards to work recovery and that part. FBI has the responsibility to do law enforcement investigations. We have the responsibility on the NSA side for the foreign intelligence and to defend against an attack. So what we are doing is developing the capabilities and the teams. We are still going to need legislation to do those operations.

Chairwoman MIKULSKI. Well, I could have follow-up, but I want to turn to Senator Shelby.

Senator SHELBY. Thank you, Madam Chairman.

Dr. Gallagher, I will address my first question to you. Since NIST has been tasked under the Executive order with developing a framework to reduce cyber risk of critical infrastructure, could you explain how the NIST process will work, how the development of a framework to reduce cyber risk differs from the development of standards to reduce such risk? And what do you believe will compel private industry, which I think is so important, to implement the framework that it has developed?

And given the evolution of technology, which you are very much into, all of you, generally in cyber threats specifically, how useful is the development of a broad-based, generic framework long term? Will NIST just be chasing its tail, so to speak, or will you be able to get ahead of the curve? I would be interested for you to share your thoughts here, how the framework and the standards and so forth will apply or could apply.

Dr. GALLAGHER. Well, thank you very much.

Senator SHELBY. I know that is a mouthful.

Dr. GALLAGHER. I am going to do my best.

The idea behind the framework is very simply to get industry to develop a set of practices, standards, methodologies, whatever it would take that if implemented would improve cybersecurity performance. So we used the term "framework" as a term of art to refer to whatever you would put into place that would result in enhanced cybersecurity performance. That will include a large measure of standards.

And the idea behind having industry do it, with NIST acting as a technical supporting role and a convener, has a couple of motivations. First of all, it addresses the capacity. Industry is the one developing IT technology and communication technology, and therefore, they know where this technology is going and they can bring that skill and that expertise into the process to develop these standards.

Second, this Internet is a global infrastructure, and these companies operate at a global scale. And by embedding security performance into the products and services themselves, we can, in fact, achieve a cybersecurity performance than is much broader than our borders, much broader than what we would buy directly. It embeds it in the market. It in fact gives our companies the power to shape those technologies around the world.

In terms of chasing our tail, I think in a time when this technology is moving so quickly and when the threat environment is changing right in front of us, this is going to be an ongoing challenge. But I think the bottleneck cannot be NIST. We are simply not large enough to support this on our own. Our role really has to be viewed as did we help industry come up with a vehicle where they can organize and be responsive to this. That is the only way sufficient technical capacity can be brought to bear in my view.

Senator SHELBY. Let me pick up on that, if I could. The Executive order, as I understand it, discusses the development of a broad framework which presumably, I would think, means it will be generic in order to have broad applicability to all critical infrastructure sectors. But how will, doctor, a generic framework address the inherent differences in our critical infrastructure and their unique needs for being protected against cyber attacks? In other words, if we are not addressing sector-specific needs, how can we be sure that we are actually helping to protect any of these industries from a cyber attack?

And last in this same vein, how do you bring industry on board? Because they have systems, trade secrets, formulas, everything, you name it, to protect and the Government would have to protect those and should. How will that work?

Dr. GALLAGHER. So you are exactly right. The question you asked about industry's capacity to come together and carry this out is actually the central question. How generic and how sector-specific this framework looks is, in fact, the exact question that the participants in the framework are tackling.

The good news is that in spite of the strong differences across sectors, looking at energy or agriculture or transportation and so forth, they are dependent on a core set of communication and IT technologies. And one of the big advantages they have to working together to set a common platform is that they can drive that performance into the market and they can buy these computer services and IT equipment at better cost because they are helping to shape the entire market.

And that really gets to one of the questions you raised earlier, which is how do you drive adoption of this framework. I think the bottom line is doing good cybersecurity has to become good business. In the end, this is all going to be about alignment. These framework practices have to be compatible with profitable and well run companies. It may very well turn out that the framework discussions are more about management and business practices than they are about technical controls, and that is okay if it helps us achieve the level of performance we are looking for.

Senator SHELBY. Thank you, Madam Chair.

Chairwoman MIKULSKI. Senator Leahy.

Senator LEAHY. Thank you, Madam Chair.

You know, like most Vermonters, I have had a lot of concern about section 215 of the PATRIOT Act, section 702 of the Foreign Intelligence Surveillance, the FISA. We have had a number of common sense proposals in the Judiciary Committee to improve these provisions, but the Intelligence Community has told us that really we obviously do not have the ability as simple Senators to know anything as well as you do, and so they do not need changes. I am told they are critical to our counterterrorism efforts. The Congress should not tinker with them at all. We should simply trust you to use them the right way, and they should not be made permanent.

I do not think that is wise. I think that there should be sunset provisions, and we should look at them periodically and we should actually debate them in a free and open society.

Now, we have information, recently declassified by the Director of National Intelligence, and I am not going into questions of whether he contradicted himself on a couple of answers. But taking what he has recently declassified, it appears that section 702 collection he said was critical to disrupting the *Zazi* case in New York City, but it is not clear that data collected pursuant to 215 of the PATRIOT Act was similarly critical or crucial.

So, General Alexander, let me ask you this. Aside from these two cases, has the Intelligence Community kept track of how many times phone records obtained through section 215 of the PATRIOT Act were critical to discovery and disruption of terrorist threats?

General ALEXANDER. I do not have those figures today.

Senator LEAHY. Are those figures available?

General ALEXANDER. We are going to make those figures available——

Senator LEAHY. How soon?

General ALEXANDER. Over the next week, it would be our intent to get those figures out. I have talked to the Intel Committee on that yesterday. I think it is important to——

Senator LEAHY. Wait a minute. You talked to the intel community about this yesterday, but you did not have the figures yesterday.

General ALEXANDER. I gave an approximate number to them in a classified——

Senator LEAHY. Okay.

General ALEXANDER. Classified. But it is dozens of terrorist events that these have helped prevent.

Senator LEAHY. Okay, so dozens.

Now, we collect millions and millions and millions of records through 215, but dozens of them have proved crucial or critical. Right?

General ALEXANDER. For both here and abroad in disrupting or contributing to the disruption of terrorist attacks.

Senator LEAHY. Out of those millions, dozens have been critical.

General ALEXANDER. That is correct.

Senator LEAHY. Would you get me the specific—even it has to be in classified, the specific cases you are talking about?

General ALEXANDER. We will, but we are going through the Intelligence Committee to do this. Tomorrow I will give as clear as we have vetted precisely what we have done on each of those. And the reason that I want to get this exactly right, Senator, is I want the American people to know that we are being transparent in here.

Senator LEAHY. No, no. You are not giving it to the American people. You are giving in a classified to specific Members of Congress. Is that correct?

General ALEXANDER. Well, there are two parts. We can give the classified. That is easy. But I think also for this debate what you were asking—and perhaps I misunderstood this, but I think you were also asking what we could put out unclassified. And so the intent would be to do both.

Senator LEAHY. You can do that within a week?

General ALEXANDER. That is our intent. I am pushing for that and perhaps faster, if I do not get any kicks from behind me.

Senator LEAHY. If you do not get any what?

General ALEXANDER. Kicks from the people behind me who are doing the work because we do want to get this right. And it has to be vetted across the community so that what we give you, you know, is accurate and we have everybody here, especially between the FBI and the rest of the Intelligence Community, who can say this is exactly correct.

Senator LEAHY. Now, DNI Clapper said that section 702 collection was critical to discovery and disruption of the plot to bomb the New York City subway system, the *Zazi* case. Is that correct?

General ALEXANDER. That is correct. In fact, not just critical, it was the one that developed the lead on it. So I would say it was the one that allowed us to know it was happening.

Senator LEAHY. But that is different than section 215.

General ALEXANDER. That is different than section 215.

Senator LEAHY. 215, phone records; 702——

General ALEXANDER. So if I could, I could explain this.

Senator LEAHY. No, go ahead.

General ALEXANDER. Because I do think it is important that we get this right, and I want the American people to know that we are trying to be transparent here, protect civil liberties and privacy, but also the security of this country.

On the New York City one, the *Zazi* case, it started with a 702 set of information based on operatives overseas. We saw connections into a person in Colorado. That was passed to the FBI. The FBI determined who that was, Zazi, and phone numbers that went to that. The phone numbers on Zazi were the things that then allowed us to use the business records, FISA, to go and find out connections from Zazi to other players throughout the communities, specifically in New York City. That is how those two worked together.

Senator LEAHY. Was 215 critical?

General ALEXANDER. I think 215 is critical in corroborating and in helping us understand——

Senator LEAHY. Was it critical in *Zazi*?

General ALEXANDER. Not to *Zazi* because the first part to *Zazi* went to the 702.

Senator LEAHY. And Headley? Was either 702 or 215 critical?

General ALEXANDER. 702 on Headley and some on the business record, FISA, for corroborating.

And I think it is important to understand because this is an issue that I think will be part of the debate. And I would put on there, Senator, also the Boston. I think we need to walk through that so that what we have on the business record, FISA, what we have on 702, what you debate, the facts that we can give you is what we do with that, how we tip that to the FBI, if we took that away, what we could not do, and is that something that when we look at this from a security perspective——

Senator LEAHY. Of course, in Boston, if you are talking about the marathon case, what the FBI could have done was to pass on the information to the Boston authorities. They said they did not. That might have been helpful too.

But my time is up. I mention this only because before it is brought up in the Judiciary Committee, we are going to be asking some very, very specific questions.

General ALEXANDER. So if I could, Senator, I just want to make sure that we are clear on one point. When I say "dozens", what I am talking about here is that these authorities complement each other in helping us identify different terrorist actions and help disrupt them. They complement each other. So what you are asking me is to state unequivocally that A or B contributed solely to that. The reality is they work together. And we have got to help make that clear to you——

Senator LEAHY. And I will be waiting to see those specific examples either in open or classified fashion.

Chairwoman MIKULSKI. Senator Cochran.

Senator COCHRAN. Madam Chair, thank you.

Let me first ask General Alexander a question. In testimony that was received by the Armed Services Committee, there was a discussion about how to provide incentives to talented military personnel who might be interested in becoming involved in the cybersecurity field. I know it is hard to contemplate how you just wave a magic wand and have all of the talented people available in the right places with the right responsibilities.

What do you see as a first step in trying to get an infrastructure of leadership organized appropriately to carry out these missions?

General ALEXANDER. Senator, thanks.

I think the most important part, top to bottom, is the training, coming up with a clear training program, which we have done with the services and with NSA to develop a set of standards. I think the training, in and of itself, helps us build a great cyber force, and it is that training for the leaders so we have training at the staff officer level, at the team level, all the way down to the individual operator. And we are standardizing that training amongst the services and between NSA and Cyber Command.

I think raising those standards up has a couple of benefits. The soldiers, sailors, airmen, marines, and civilians that come into this field get great training, and it is something that they look forward to. And the operations that they do are significant. I think they really feel good about what they are able to do for our country. So from my perspective, it starts with training and building that kind of a force.

You mentioned incentives, Senator, if I could. I think incentives is going to play a key part in this. As incentive pay for languages plays a key part, I think incentives for our cyber force is also going to play a key part. And we have had discussions with the services about how to start that. We do not have that in this program yet, but that is something that we are looking at.

Senator COCHRAN. Does the Department of Defense have the resources to maintain a number of cyber test ranges across the services and agencies, for training and research purposes? I know you carry out exercises that test the compatibility of cyber capabilities with conventional weapons and other weapons systems. Could you share with the committee what your thoughts are about cyber ranges and whether you plan to dedicate certain areas exclusively for these purposes?

General ALEXANDER. Senator, that is a great question and one that we are putting a lot of effort into because I do think we need to bring the ranges together so that we have a joint approach to this.

One of the things that I would point out is the service academies play a cyber defense exercise together, and this gets into your range issue. And when you look at so how do you defend your networks in a way—the service academies compete against each other for seeing who has the most defensible network. When you think about that, in a cyber range what you want people to do is to practice their tactics, techniques, and procedures in a sterile environment so nothing bad happens. It only happens inside that. They can learn. We have seen that on the military side. The National Training Center and other things are great places for that. We need to do the same here. So those that are defending our networks know what the adversaries are going to do and are prepared for all those contingencies. It helps raise that. And I think bringing the ranges together ensures that they are operating at the right level as a joint team.

Senator COCHRAN. My staff informed me that last week our committee received a notice that about one-half of NSA's personnel in the Cyber Threat Center could be furloughed as a result of sequestration. Now, that is a fine "How do you do?" Has there been any attention given to what you are going to do to address shortfalls due to sequestration?

General ALEXANDER. So we have worked this. It is across the Defense Department. So the sequestration for all the military has been standardized across all the departments. The NSA—on the intelligence side is not there—but all of Cyber Command—our civilians will be sequestered. Right now that is an 11-day or 1 day a week for the last 11 weeks of the fiscal year. That has a significant impact on us and all others that will be furloughed. I think that is a key issue and has significant impact on our people. And it goes right back to how do you hire good people and then furlough them. This is a tough issue that not only we face but the rest of the Department.

Senator COCHRAN. Thank you, Madam Chair.

Chairwoman MIKULSKI. Thank you, Senator Cochran, and thank you for raising the sequester issue. It has been raised at the intel hearing when we listened to the worldwide threat right as we were moving into the continuing funding resolution. DNI Clapper asked for more flexibility. Of course, he wanted more money but more flexibility. We were precluded by the House from putting that in the bill. I think the intel community, which is primarily particularly a DOD civilian force—you need that flexibility.

So we look forward to working on both sides of the aisle and both sides of the dome to be able to do this.

I just would like to share with the committee the order. We are going to go to Durbin, then Johanns, Merkley, Collins, Tom Udall, Senator Coats, Senator Landrieu, and Senator Feinstein, you came before the testimony started. So instead of alternating, we will go right to you. Then we will go to Senator Boozman and then Senator Pryor. That is our order of our lineup. So now it is going to be Durbin, Johanns, Merkley, Collins. Senator Durbin.

Senator DURBIN. Thank you, Madam Chair. And thanks as well to Senator Mikulski for bringing the cyber issue into sharp focus for the entire Senate with our bipartisan briefing.

I was on the Intelligence Committee right at the time of 9/11. I saw what happened immediately afterwards. There was a dramatic investment in intelligence resources for our Nation to keep us safe and a dramatic investment in the personnel to execute the plan to keep us safe.

I trusted—and I still do—that we were hiring the very best, trusting them to not only give us their best in terms of knowledge but also their loyalty to our country.

I would like to ask you about one of those employees who is now in a Hong Kong hotel, and what we know about him is as follows. He was a high school dropout. He was a community college dropout. He had a GED degree. He was injured in training for the U.S. Army and had to leave as a result of that. And he took a job as a security guard for the NSA in Maryland. Shortly thereafter, he took a job for the CIA in what is characterized as IT security in the Guardian piece that was published.

At age 23, he was stationed in an undercover matter overseas for the CIA and was given clearance and access to a wide array of classified documents.

At age 25, he went to work for a private contractor and most recently worked for Booz Allen, another private contractor working for our Government.

I am trying to look at this resume and background. It says he ended up earning somewhere between $122,000 and $200,000 a year. I am trying to look at the résumé background for this individual who had access to this highly classified information at such a young age with a limited educational and work experience, part of it as a security guard, and ask you if you are troubled that he was given that kind of opportunity to be so close to important information that was critical to the security of our Nation.

General ALEXANDER. I do have concerns about that. Over the process, Senator, I have grave concerns over that. The access that he had, the process that we did—and those are things that I have to look into and fix from my end and across the intel community, Director Clapper said we are going to look across that as well. I think those absolutely need to be looked at.

I would point out that in the IT arena, in the cyber arena, some of these folks have tremendous skills to operate networks. That was his job for the most part from the 2009/2010 as an IT, a system administrator within those networks. He had great skills in that area.

But the rest of it, you have hit on the head. We do have to go back and look at these processes, the oversight on those—we have those—where they went wrong and how we fix those.

Senator DURBIN. Let me shift to another topic raised by Senator Leahy, section 215. 10 years ago, I first introduced legislation known as the SAFE Act. It was a bipartisan bill to reform the PATRIOT Act. My cosponsors included Senators Chuck Hagel, John Kerry, and Barack Obama. My most significant concern with 215 was that it would be used to obtain sensitive personal information of innocent Americans who had no connection to any suspected terrorism or spy activity.

When the PATRIOT Act was up for reauthorization in 2005, I worked to establish a new standard for 215, and under the standard, the FBI would have broad authority to obtain any information, even tangentially connected to a suspected terrorist or spy, such as the examples you used in the *Zazi* case. 702 information could have led to 215 phone record information on any suspect. But under my provision, innocent Americans with no connection to any of these activities or suspects would be protected.

The Republican-controlled Senate approved my reform to 215 unanimously. However, the Bush administration objected. It was removed in the conference committee.

2009, I tried again with no success to put this protection of innocent Americans back into the PATRIOT Act.

Now the cloak has been lifted by media reports that the NSA obtained phone records of millions of innocent Americans with no connection to terrorism. The data includes the numbers of both parties to the calls, the location of the callers, the time and duration of the calls. I have been briefed on these programs, and I obviously will not discuss their details here. But it appears to me the Government could obtain the useful information we need to stay safe and still protect innocent Americans.

My question to you is this. Section 215 can be used to obtain, “any tangible thing” that could include medical records, Internet search records, tax records, credit card records, et cetera.

Last year, the Government filed 212 section 215 orders. That is an increase from 21 such orders in 2009. So clearly, this authority is being used for something more than phone records.

So let me ask you. Do you think section 215 giving you authority to secure tangible things could include the categories of information that I just listed?

General ALEXANDER. I do not use those, so I am not aware of anything that goes that—that would be outside of NSA. All we use this for today is the business records, FISA.

I would point out—I just want to characterize something that you said here. As you know, this was developed—and I agree with you. We all had this concern coming out of 9/11. How are we going to protect the Nation? Because we did get intercepts on Midar, but we did not know where he was. We did not have the data collected to know that he was a bad person. And because he was in the United States, the way we treat it is he is a U.S. person. So we had no information on that, and if we did not collect that ahead of time, we could not make those connections.

So what we create is a set of data and we put it out here, and then only under specific times can we query that data. And as you know, Senator, every time we do that, it is auditable by the committees, by the Justice Department, by the court, and by the administration. We get oversight from everybody on this.

Senator DURBIN. I am over my time, but here is the point. If you knew that a suspect had made a call into area code 312, the city of Chicago, it certainly defies logic that you need to collect all of the telephone calls made in the 312 area code on the chance that one of those persons might be on the other end of the phone. Now, if you have a suspected contact, that to me is clear. I want you to go after that person. What I am concerned about is the reach beyond that that affects innocent people.

General ALEXANDER. So we agree at least on that part.

And the next step, I think, in the debate that we actually need to talk about is so what happens if you do not know he is in 312 yet. And so something happens, and now we say who was he talking to. So let us take Midar. You had authorized us to get Midar's phones in California. But Midar was talking to the other four teams. Under the business record, FISA, because we had stored that data in a database, we now have what we call reasonable, articulable suspicion. We could take that number and go backward in time and see who he was talking to. And if we saw there were four other groups, we would not know who those people were. We would only get the numbers. We would say this looks of interest and pass that to the FBI. We do not look at the identities of it. We only look at the connections.

Senator DURBIN. I am way over time. I am not going to dwell on it.

You have just given a clear illustration where you had specific information about telephone contacts, which I do not quarrel with. What I quarrel with is collecting all of the information in California on telephone records to try to find that specific case. That to me seems overly broad.

Chairwoman MIKULSKI. Thank you very much.

Senator Johanns.

Senator JOHANNS. General Alexander, I want to talk to you about Cyber Command, but Senator Durbin has raised a very interesting question. And let me just follow up on this.

Would this lead—the scenario that he has laid out—to a telephone record search for all of Omaha? Or walk us through that.

General ALEXANDER. So the methodology would be what is put into a secure environment called "detail records." These are to/from records and at a selected time. So we do not know anything that is in there. We will not search that unless we have some reasonable, articulable suspicion about a terrorist-related organization. If we see that, we have to prove that we have that. Then given that, we can now look and say who was this guy talking to in the United States and why.

Senator JOHANNS. And so you could search across the breadth of telephone records.

General ALEXANDER. All you are looking for on that is so who did he talk to.

Senator JOHANNS. Yes.

General ALEXANDER. And so the system just gives us back who he was talking to. But if you did not collect it, how do you know who he was talking to? And so the issue really becomes if you do not have the information—so I do not give you any connections. I just give you a number and say, now, find who he is talking to. You do not have the information.

So this was the debate. I mean, you bring it up because this came up 10 years ago. So how do we do that? How do we solve this problem? And the answer was we want to protect civil liberties and privacy. We do. And we want to protect the country. So the thought was a reasonable approach that we all agreed on—the Congress, the courts, the administration—was we will put this in a way that we have tremendous oversight by the court. And so every time your people, a small set of those, can go in, they have to have a reason to go in and look at the data. And when they get something out, they have to look at it and say does this meet the reporting guidelines and put that in the report. Only a few reports a year go out on that, just a handful—handfuls.

Senator JOHANNS. Does this extend beyond telephone records? For example, could you check and see what that person is Googling? Could you check and see who that person is e-mailing?

General ALEXANDER. So there are two parts of your question here.

So going to the next step, once we identify a person of interest, then it goes to the FBI. The FBI will then look at that and say what more do we need to now look at that individual themselves. So there are issues and things that they would then look at if passed to them.

Senator JOHANNS. So the answer to the question is yes.

General ALEXANDER. Yes, you could. I mean, you can get a court order to do that. So in either case——

Senator JOHANNS. But would that take a court order?

General ALEXANDER. It would. To do any kind of search in these areas on a U.S. person, you have to have a court order.

Senator JOHANNS. So now you have gotten into phone records. You have gotten into who they might be Googling. You have gotten who they might be e-mailing. What else do you feel that you can get?

General ALEXANDER. So I am not sure of your question. On a terrorist acting in the United States——

Senator JOHANNS. Well, you do not know if it is a terrorist yet. You have got this reasonable suspicion, which is not even probable cause. You have just got this kind of uneasy notion, this feeling that something is happening here.

General ALEXANDER. So that is the——

Chairwoman MIKULSKI. Wait, wait. Let us just stop here a minute. We are not going to inhibit your questions, but I think we need to clarify that the activity in which you are operating, General Alexander—so we are getting into probable cause, a lot of these that are absolutely important in a debate. But you will be functioning also with a warrant.

Senator Feinstein, did you want to clarify? Just if we could.

Senator FEINSTEIN. If I may.

Chairwoman MIKULSKI. And I am going to come back and give you more time. Senator Johanns, you will get more time.

Senator JOHANNS. Thank you.

Senator FEINSTEIN. If I may quickly, Senator.

It is my understanding you have the metadata. You have the records of what appears on a phone bill, and if you want to go to the content, then you have to get a court order, the same thing you would do in a criminal case. You would have to get a court order that would permit you to collect the content of the call. You can ask him if that is right or wrong.

General ALEXANDER. But it is correct.

Senator JOHANNS. And I assume that, but I am not talking about content at this point. I am not asking if you can read somebody's emails. I am assuming at some point there would be a legal standard by which you could do that. Being a lawyer, I know that.

What I am only getting to is you have identified for us that you can get phone contacts. I am asking can you get Google contacts. Can you get e-mail contacts? I am not talking about reading the e-mail or seeing what they are saying back and forth. I am not at that point. But what I worry about is how far do you believe this authority extends. Can you get Google contacts? Can you get e-mail contacts? Again, I am not asking about reading the e-mail.

General ALEXANDER. So I think there are a couple things here that I want to make sure that we have got.

The BR–FISA only talks about phone contacts, phone metadata. That is all that program talks about. So any program that we have—and Senator Feinstein, if you want to get the content, you would have to get a court order. In any of these programs, you know we have court orders for doing that, with oversight by the Congress, by the courts, and by the administration.

So my concern in all of this is that I think this is an area where we have to give you both the detail—and I think we need this for the American people. They need to understand it so they can see what we are doing and what the results of it are. I do think that is important.

I also believe—you know, we had this debate several times—and Senator Durbin brought it up—from 2001 on. And this is one now where we need to bring out, because of these leaks, the rest of the story, show what we do, what it protects the country from, and have the debate. Does it make sense? In order to do that, I think what we have to give you is the rest of that data. Tomorrow we will put that in a classified session, but the intent would be to try to get as much out publicly so that everybody has the information, where we can.

And the reason that I hesitate a little bit here is I do not want to make the mistake that causes the statements that I have for our country to lose some form of protection and we get hit with a terrorist attack because I made that mistake.

Senator JOHANNS. And I thank the Chair for the additional time. I will wrap up with a comment.

The concern here—the American public is fearful that in this massive amount of data you get, that there is the ability of the Federal Government to synthesize that data and learn something more than maybe what was ever contemplated by the PATRIOT Act. That would be number one.

The second thing is a more personal issue, and it kind of gets into some of the concerns about Cyber Command. And that is, you are in this hugely unique role. We have always had this view of separating the civilian leadership politically elected from the military leadership, and yet you have got this dual hat. And it creates a concern not about you because you have got a remarkable record, and I thank you for your service. But it is a very, very concerning role that we find you in, at least for Mike Johanns. And I just think we have got to get some information out to the public because right now we are all getting bombarded with questions that many of us at the rank and file level in the Senate cannot answer. I am not the chair of the Intelligence Committee. I am not the ranking member. I do not serve on the committee. And the impression has been created that people are parked in our office giving us daily briefings on this or monthly briefings and that has not been the case. So we need to know.

Chairwoman MIKULSKI. Senator Johanns, I think you had an excellent line of questioning, and I must say the tone and demeanor are appreciated.

Senator JOHANNS. Thank you.

Chairwoman MIKULSKI. And, General Alexander, we are going to move on from this topic. I think you have that. Senator Merkley has been waiting. What we are now moving into is a domain that is not the parameters of this hearing, though this Senator will not inhibit any Senator from asking any question they want.

I want to remind the Senators that tomorrow in the Feinstein hearing, many of these can be followed and I hope it is a learning experience that when you go to Feinstein, your questions will even be as cogent and comprehensive as they are here today.

So, Senator Merkley, we are going to turn to you now.

Senator MERKLEY. Thank you very much, Madam Chair.

And thank you, General. You referred to section 215, and 215 requires an application for production of any tangible thing. And it says in it that this application must have a statement of facts showing reasonable grounds that the tangible things sought are relevant to an authorized investigation. So we have several standards of law embedded in this application, a statement of facts, reasonable grounds, tangible things that are relevant to an authorized investigation.

Now, as it has been described in this conversation and in the press, the standard for collecting phone records on Americans is now all phone records all the time all across America. How do we get from the reasonable grounds, relevant authorized investigation, statement of facts to all phone records all the time, all locations? How do you make that transition and how has the standard of the law been met?

General ALEXANDER. Well, so this is what we have to deal with the court, and I think that we go through this court process. It is a very deliberate process where we meet all of those portions of 215. We lay out for the court what we are going to do, and to meet that portion that you just said, the answer is we do not get to look at the data. We do not get to swim through the data.

Senator MERKLEY. Let me stop you there because these are requirements to acquire the data, not to analyze the data, to acquire the data. This is the application to acquire the data.

So here I have my Verizon phone, my cell phone. What authorized investigation gave you the grounds for acquiring my cell phone data?

General ALEXANDER. I want to make sure I get this exactly right. You know, I think on the legal standards and stuff, on this part here, I think we need to get the Department of Justice and others because it is a complex area. And you are asking a specific question. I do not want to shirk that, but I want to make sure I get it exactly right. And so I do think what we should do, as part of perhaps the closed hearing tomorrow, walk through that with the intent of taking what you have asked and seeing if we can get it declassified and out to the American people so they see exactly how we do it because I do think that should be answered.

Senator MERKLEY. General, thank you. Let me fill in the middle piece here. In between——

Chairwoman MIKULSKI. Senator Merkley, I would like to help you out. I think Senator Merkley has asked an excellent question, and you want to get it right. And the answer, I would suggest, should be in writing. That way you get it right and he gets his answer. How does that sound?

General ALEXANDER. We will take that for the record.

Senator FEINSTEIN. If you will yield. I have asked that that question get answered tomorrow at the hearing by DOJ, Senator Merkley, exactly as you have delivered the question.

Chairwoman MIKULSKI. Okay. But either way, Senator Merkley should get his answer, and I would suggest perhaps both in writing, your hearing, and into his hands.

Senator MERKLEY. I thank the Chair, both chairs.

If I can elaborate on the piece that I would like answered, is that okay, Madam Chair?

Chairwoman MIKULSKI. It is your time.

Senator MERKLEY. In between these two pieces, a FISA court gives an interpretation of the plain language of the law. Their interpretation is what translates the standards in the law into what is governable in terms of what you can do.

I had an amendment last December that said these findings of law that translate the requirements that are in the law into what is permissible needs to be declassified so we can have the debate.

I believe that what you just said is you want that information to be declassified that explains how you get from these standards of law to the conduct that has now been presented publicly. Did I catch that right? And do you support the standards of law, the interpretations of the FISA court of the plain language to be set before the American people so we can have this debate?

General ALEXANDER. I think that makes sense. I am not the only decisionmaker in the administration on this process. So there are two issues. I am not equivocating. I just want to make sure that I have put this expectation exactly right, and that is I do not want to jeopardize the security of Americans by making a mistake and saying, yes, we are going to do all that. But the intent is to get the transparency there.

So, Senator, I will work hard to do that, and if I cannot do that, I will come back to you and tell you why and then we should have that discussion and run it out. And I would defer to the chair of the Intel Committee, but I think that is reasonable to get this out.

Now, having said that, I do not have the legal background that perhaps you have in this area. I want this debate out there for a couple reasons. I think what we are doing to protect American citizens here is the right thing. Our agency takes great pride in protecting this Nation and our civil liberties and privacy and doing it in partnership with this committee, with this Congress, and with the courts. We have everybody there. We are not trying to hide it. We are trying to protect America. So we need your help in doing that. This is not something that is just NSA or the administration doing it on its own. This is what we—that our Nation expects our Government to do for us. So we ought to have that debate. We ought to put it out there and we have got to put those two together. So I just want to put that one caveat there, and if I can make it happen, I will.

Senator MERKLEY. General, I thank you for your expression of support.

I also want to thank Chair Feinstein who helped develop and sent a letter expressing this concern about the secrecy of the interpretations of the FISA court. I do think it is time that that become understandable in public because otherwise how in a democracy do you have a debate if you do not know what the plain language means. I do have concerns about that translation. I will continue this conversation and thank you.

Chairwoman MIKULSKI. Senator Collins.

Senator COLLINS. Thank you, Madam Chairman.

Madam Chairman, I am actually going to ask a question about computer security, but before I do so, I do want to give General Alexander a chance to answer a very quick question that has to do with Americans' concern about their own private computer security and privacy.

I saw an interview in which Mr. Snowden claimed that due to his position at NSA, he could tap into virtually any Americans' phone calls or emails. True or false?

General ALEXANDER. False. I know of no way to do that.

Senator COLLINS. Thank you. I just wanted to clarify that because perhaps that is one issue we could put to rest.

Now let me switch to the computer security question.

Chairwoman MIKULSKI. Oh, boy.

General ALEXANDER. We are not ready for those.

CRITICAL INFRASTRUCTURE: INCIDENTS REPORTING

Senator COLLINS. In the President's budget, it is mentioned that the Nation has four top cyber risks, and the first one listed is one that has been of great concern to me since we produced the bill last year that, unfortunately, could not get past a filibuster, and that is attacks that are aimed at our critical infrastructure. And Secretary Beers, I am going to ask you this question.

The General has alluded to the fact that much of our critical infrastructure is owned or operated by the private sector. In fact, it is 85 percent that is in the private sector. And our FBI witness has talked about the iGuardian program which encourages private industry partners to report cyber incidents to the Government in real time.

Our legislation last year had a requirement that the owners and operators of critical infrastructure—not all infrastructure, critical infrastructure—would be required to report major cybersecurity incidents. Does the administration still support mandatory reporting in such cases?

Mr. BEERS. Senator, that was our position then and that remains our position at this point in time. Obviously, we are prepared to work with the Congress. You all ultimately write the legislation. But that remains the administration's position.

Senator COLLINS. Thank you.

In that legislation, we did pay attention to the need for a more expert cyber workforce, and boy, this latest account, which Senator Durbin did such a great job of going through the résumé of this individual, just underscores how much work there is to be done in making sure that whether it is public sector or private sector, that we have a well vetted, well qualified cyber workforce.

I would like to hear from all four of you on whether you are having difficulties in recruiting individuals who have the skills that you need and doing the appropriate vetting of them so that we can avoid having the hiring of a young high school dropout, community college dropout, did not complete his military service, young person with so little experience being given access to so much classified information. And, General Alexander, we will start with you and then just go down the panel.

General ALEXANDER. Well, Senator, I would just like to state first that in the military, we are going to hire young folks out of high school, who graduate from high school, to work in this area. And the key will be the training that we give them.

Now, ideally we would like to get 4 years out of a top-notch engineering school for some of the military positions, but we will not get that. So what we have is a responsibility to train them, bring them into the force and train them. And we have a program, but it takes several years to get somebody trained in this area, as you know. So in effect, what we are running is a cyber college for many of our young enlisted folks to get them to the requisite skills.

On the NSA side, we are able to hire more college graduates into the Government side of that.

What I need I think is greater scrutiny. What I need to go back and look at is what am I getting with my contract support and what are their capabilities and how do we manage that from a Government perspective. So that is something I have concerns about and I have got to go back and address.

QUALIFIED WORKFORCE: RECRUITING AND RETAINING

Senator COLLINS. Secretary Beers.

Mr. BEERS. Senator, we have a major initiative underway, as you are well aware. We have defined our cyber workforce. We are matching the positions with the skill set that is required to serve in those positions. We are also in the process of looking to hire another 600 individuals to augment that 1,500-person workforce. We have a series of programs, one with community colleges where we are looking to find people who have taken the correct, appropriate courses at the community college level who we can hire as beginning workforce members and train them up. We also have a program in conjunction with NSA that goes to colleges and universities that have Centers for Excellence that provide us with top-notch 4-year graduates. And then we have an effort to reach out to the private sector to find individuals there.

I think we have an excellent workforce, but we have, as you well know, a provision that was in the bill that you worked on——

Senator COLLINS. Correct.

Mr. BEERS [continuing]. And that we would like to see in any cyber legislation that gives us some assistance in terms of both recruiting and retaining that kind of a workforce which would allow us comparable pay and benefits to what NSA is able to offer to its workforce.

Thank you.

Senator COLLINS. Thank you. I know my time has expired. So I am going to ask the other two witnesses to submit their answers for the record.

But I thank the whole workforce issue is absolutely critical. We did have that as an important part of our bill last year.

Thank you, Madam Chairman.

Chairwoman MIKULSKI. I think you are absolutely right, Senator Collins, and thank you for asking a question actually on the topic, though it is our security.

And we are going to turn now to Senator Udall, but just to add to that, as we go to Senator Udall, we keep hearing Snowden had the skills. Well, maybe he did. You know, but just because you are a swimmer and you are a champion swimmer does not mean we ought to make you a Navy SEAL. So I will leave it at that.

Senator Udall.

Senator UDALL. Thank you, Madam Chair, and I thank the entire panel for their service to the country in these very difficult times.

First, I would like to welcome Dr. Pat Gallagher. Although his career took him away from Albuquerque, Dr. Gallagher is a native of New Mexico, and I want to recognize him for his leadership at NIST and his commitment to public service. Pat, it is good to have you here today.

American citizens, businesses, and Government agencies face serious cyber threats, and you have talked about some of these here today. Personal data, trade secrets, and national security secrets are at risk from intrusion by independent hackers and foreign governments. And I have supported cybersecurity legislation in the Senate, and I support funding for our cybersecurity defense.

But the elephant in the room today here is—and we have been talking about it some—that many Americans are also becoming more concerned about what their own Government is doing with domestic surveillance. Last week, we learned of widespread collection of Americans' phone records under section 215 of the PATRIOT Act, also the massive-scale online surveillance through the PRISM system conducted under FISA section 702.

I want to let you know, I voted against the PATRIOT Act in 2001 and the FISA Amendment Act in 2008. I have also voted against their reauthorizations since then. Several of us attempted to add privacy protections to these laws but faced strong resistance, as Senator Durbin indicated.

Today I am sending a bipartisan letter to the Privacy and Civil Liberties Oversight Board asking them to make it a priority to investigate the bulk phone records collection and the PRISM program to determine whether they, number one, are conducted within the statutory authority granted by Congress and, number two, take the necessary precautions to protect the privacy and civil liberties of American citizens under the Constitution.

The Board was created by the Congress based on a recommendation of the 9/11 Commission, but it has taken years—many of you realize this and know this—to get a full membership and a chairman. I have been working to get this Board operational since I was in the House, and I believe it can provide an important check against civil liberties abuses.

Richard Clarke, who was the counterterrorism aide under three Presidents I believe, just wrote an article recently on this and suggested we would not have the problems today if we had stood up this Board much more quickly.

General Alexander, will the NSA cooperate with any investigation conducted by the Privacy and Civil Liberties Oversight Board into the agency's collection and analysis programs?

General ALEXANDER. Senator, we will. And I think, in fact, my Deputy met with the Board yesterday and actually briefed them for a couple of hours on both programs so that they understood. And I do not know if you have gotten feedback from that, but my understanding is I think it went well.

I think you bring up a very important point here because I do think what we are doing does protect Americans' civil liberties and privacy. The issue is to date we have not been able to explain it because it is classified. So that issue is something that we are wrestling with. How do we explain this and still keep this Nation secure? That is the issue that we have in front of us.

So you know that this was something that was debated vigorously in the Congress, both the House and the Senate, within the administration and now works for the court. So when you look at this, this is not us doing something under the covers. This is what we are doing on behalf of all of us for the good of this country. Now what we need to do, I think, is to bring as many facts as we can out to the American people.

So I agree with you, but I just want to make that clear because the perspective is that we are trying to hide something because we did something wrong. We are not. We want to tell you what we are doing and tell you that it is right and let the American people see this. I think that is important, but I do not want to jeopardize the security of our country or our allies. So that is what we have to weigh in what we look at what we are going to declassify to allow this very public debate.

Senator UDALL. General, I very much appreciate your answer, but it is very, very difficult, I think, to have a transparent debate about secret programs approved by a secret court issuing secret court orders based on secret interpretations of the law.

I know there are many other questions here, and I am going to ask the ones in closed session when we get together later in the week. I have several other questions on cybersecurity, but I see my time has expired and so I will submit those for the record.

But thank you very much for your answers, and I very much appreciate you meeting with the Board and briefing them on what you are doing. I think that they are a good counterbalance in terms of what is going on here in terms of asking questions and then being able to, I hope, have the credibility of the American people to answer some of these questions also. Thank you.

Thank you, Madam Chair.

Chairwoman MIKULSKI. We are now going to turn to Senator Coats, but before we do, I want to respond to a Tweet about me from Rosie Gray. Rosie Gray said on her Tweet 17 minutes ago, "Senator Barb is trying hard to keep the other Senators from asking General Alexander any more about data mining programs. Not everybody might be watching C–SPAN." So I want to say to Rosie and to others who might read from Rosie there is no attempt here to muzzle, stifle any Senator from asking any line of questions.

And so we have an open hearing, but the purpose of the hearing was on the enduring war of cybersecurity. While we might be concerned about data mining and who is reading our—the phone records, et cetera, we are also concerned about stealing the—the cyber fraud that is going on against our senior citizens, our identity theft, stealing our cures for cancer that are pending over at the Food and Drug Administration (FDA). So we are here on cyber. But any Senator can ask any question at this hearing that they want to.

So, Rosie, it is an open hearing. "Hi." Look forward to keeping in touch.

Senator Coats.

Senator COATS. Well, I want to send a message to Rosie also.

As a member of the other party, Senator Mikulski, chairwoman of this committee, has been extremely tolerant of our diversion from what the purpose of this appropriations hearing was. This is the Appropriations Committee. Our purpose is to determine what kind of financial resources our agencies need to address critical issues facing our country, and we have diverted, thanks to the tolerance of the Chair, to a critical question but one that, as General Alexander said, is scheduled to be and will be thoroughly discussed with every Member of Congress and with the public to the extent that is possible.

General, I appreciate your answer to Senator Udall's last question. You are walking a very difficult tightrope here because there are demands that you release previously classified information to not just Members of Congress, but to the general public. And if you do not do that, this frenzy of mischaracterization of these programs will continue in the public. And so you are caught between a rock and a hard place. I regret that.

I have been urging my colleagues that before they draw a conclusion and go public with that conclusion, they first learn about the counterterrorism program because the more you learn about the program, the more you realize the enormous effort that has been made to respect the privacy and civil liberties of Americans and the hurdles you have to go through to get the most minimal list of information.

I think as the public hears more mischaracterizations of this program, like the government listens to and saves all the phone records all the time and the public interprets that as meaning everything that has been said over a phone is stored somewhere and you can go in and retrieve it or abuse the use of these programs. You have tried to clarify the program a number of different times in terms of what you collect and what you do not collect and how you have to go through a legal process in order to even begin to ascertain information that is necessary for you to come to some conclusion about whether or not this country is about to be attacked by terrorists.

Well, let me ask you this question. Given the fact that this issue has swept across the country and we are in a position where we have to disclose more about it in order to calm the public misperception of what it is, are there consequences? Do we have to look at both sides of this question, one, being transparent, addressing civil liberties but, two, the importance of keeping some missions and some activities in a classified manner so that those that are intending to do us harm do not learn about our counterterrorism efforts and therefore make adjustments to bypass the very methods that we have to potentially prevent a serious attack against the United States?

I would like you to address that question, particularly in relationship to what you have said about 9/11 and how perhaps if we had had these programs in place at the time, we could have prevented that, and a little bit more about the consequences of—as some have suggested—simply opening this up for the whole world, including people sitting in places where they are trying to determine how they can best attack the United States.

General ALEXANDER. Senator, thank you for the question because that is my concern. Great harm has already been done by opening this up, and the consequence I believe is our security is jeopardized. There is no doubt in my mind that we will lose capabilities as a result of this and that not only the United States but those allies that we have helped will no longer be as safe as they were 2 weeks ago. So I am really concerned about that.

I am also concerned that as we go forward, we now know that some of this has been released. So what does it make sense to explain to the American people so they have confidence that their Government is doing the right thing? Because I believe we are and we have to show them that. And you said it right. We have great people working under extremely difficult conditions to ensure the security of this Nation and protect our civil liberties and privacy. They do a great job. Actually I would like the American people to know that because they would be tremendously proud of the men and women of NSA who have done this for us for the last decade. It is a great story.

The issue is that we then have to debate is how much do we give out and what does that do to our future security. That is where the real debate is going to take place because that is the issue that is now before us. There is water, broken glass, and everything else on the floor. We now can look at that, but what we are going to have to do as a Nation going forward is say what can we do, and that is where the Congress, I believe, has to stand up on behalf of the American people.

Some of these are still going to be classified and should be because if we tell the terrorists every way that we are going to track them, they will get through and Americans will die. That is wrong. And our allies. We have got to come up with a way of doing this.

And you know, I thought the great part about this program was that we brought the Congress, the administration, and the courts all together. We did that. That is what our Government stands for under the same Constitution. We follow that Constitution. We swear an oath to it.

So I am concerned and I think we have to balance that. I would rather take a public beating and people think I am hiding something than to jeopardize the security of this country.

Now, having said that, some of this is out there, and it is right that we have that debate. And so what makes sense to put out there so that people will know that what we are doing is right, we ought to do that. And I think that part will be good for the country.

And there are other parts that I think you need to weigh in and say, but do not do that. And that is where you, the administration, and potentially the courts ought to come together and say, so now what do we do.

Chairwoman MIKULSKI. Thank you.

Senator COATS. Thank you. I appreciate that statement and I think it should be made in the record and published across the Nation.

Chairwoman MIKULSKI. Senator Landrieu.

Senator LANDRIEU. Thank you so much.

I would like to follow up by saying, General Alexander, I am so proud of you for being in charge of this because your demeanor through this whole hearing has, once again, proven to me that you are the right person for this job, and the four stars that you wear indicate a great understanding of the balance that you are trying to achieve.

Perhaps these facts might support what Senator Coats and others have been trying to express, given the important, but difficult questioning.

U.S. Cyber Command says there are 250,000 attacks on U.S. Government networks every hour, 6 million a day. And among the attackers are 140 foreign spy organizations. This is what our men and women are up against. We are not in a scrimmage. We are in a war. It is a very serious issue, and we are way behind the eight ball in my view in terms of allocation of resources, as much as we are struggling to clarify roles and responsibilities and balance this new war that we have never fought before under a Constitution that is probably the best and most open in the world. I think they need a little space.

Second, I have every confidence in this chairman to provide leadership. This hearing is one of the best hearings, Madam Chair, I have ever participated in in the almost 18 years I have been here. I thank you for it.

And I have great confidence in Senator Feinstein. I do not think there is a Member of the Senate in either party that would question her integrity on this issue as head of our Intelligence Committee trying to balance the civil liberties representing the State of California, which probably has the strongest views on this of any State, and the military which has been engaged in war since the beginning of time but never one like this.

So I just want to say I am very proud of our military and very proud of you, General Alexander. And I hope that in the classified hearing that more of this can be brought to light. And I most certainly am going to be explaining this to my constituents in an appropriate, balanced way.

CRITICAL INFRASTRUCTURE: CYBERSECURITY IMPROVEMENTS

But I want to say one other thing to you, Mr. Beers. Your staff is terrific. They briefed me privately yesterday on several briefings. I want to share this and then ask a question.

When I asked them to sort of describe the scope of cybersecurity and the challenge before us, they said, well, Senator, somebody has described it like this. They said the DOD is dot-mil. It is the Coke bottle cap. You think about a Coke bottle. It is just the cap of the Coke bottle. The Federal civilian Government, which is dot-gov, is like the Coke bottle itself, and the companies and citizens, which is dot-com, is the entire room the bottle is in. So while all the questions are being peppered right now to the top of this Coke bottle, Madam Chair, the room that we are in is the battleground that we are fighting in. And it takes huge resources and an unbelievable amount of commitment and compromise between the Government and the private sector.

So what I want to ask the Secretary of Homeland, since that is my—and I am very proud to be the chair of the subcommittee. When the President issued his Executive order on improving critical infrastructure cybersecurity, it requires not only you, Mr. Secretary, but Commerce—Treasury is not here—to come up with a report. That report is actually due today. It is 120 days from it. Do you have the report? Can you comment about, if you do not have it, when you are going to have it and one or two of the top findings in that report that you are going to be giving to the Congress I hope sometime soon?

Mr. BEERS. Senator, yes, the report is done. The report has been sent to the Office of Management and Budget (OMB) and the White House. I trust that Commerce and Treasury have also submitted their report on incentives. It will be subjected by OMB to an interagency process, and at the end of the process, the expectation is to release it to you all and the private sector for comment.

What we want out of this is to pull together—and we have had workshops to talk about incentives. We had one—what—last week in Pittsburgh to draw in the private sector to give us their ideas about incentives to have critical infrastructure adopt the cybersecurity framework.

That report will cover such things as insurance as a possibility. It will cover such things as certification with some liability protections as a possibility. These are all still ideas that are in a formative stage, and I do not think it is appropriate at this point to make those initial reports public. But the intention of the administration is to make those reports public to you, the Congress, and to the private sector.

Chairwoman MIKULSKI. But not because they are secret. It is because they are incomplete. Is that correct?

Mr. BEERS. Yes, ma'am. That is correct. What we need to make sure is that everybody who has a stake in this in the Government has an opportunity to comment on it and then to get it back out to you and the private sector.

Senator LANDRIEU. My time is up. And I am going to ask General Alexander in writing what his view is of the goal of the National Guard in cybersecurity for the Nation. You know, they play a very interesting role in our States. I have written you several times about it. I am going to write again to clarify their role.

And finally, for the record, to follow up on Senator Collins, the Department of Homeland Security under your leadership, Secretary, has awarded a $300,000 grant to the Cyber Innovation Center in Louisiana which is starting a very scalable and proven model to create the cyber warriors of the future. And I look forward to talking with you more about that in conjunction with the chairman.

Chairwoman MIKULSKI. Thank you, Senator Landrieu. You, as the chair of the Homeland Security Subcommittee, along with Senator Coats, who is your ranking member I believe—I really would hope you would do your due diligence in getting ready for the bill—pursue this topic because we covered a lot of topics today. But we really count on you in the homeland security area.

Senator Feinstein.

Senator FEINSTEIN. Thanks very much, Madam Chairman, and thank you for holding this hearing, and I thank all our witnesses for their service to our country.

Just to be corrected, if I need to be corrected, I would like to just quickly read my understanding of section 215.

The section 215 business records provision was created in 2001 in the PATRIOT Act for tangible things, hotel records, credit card statements, et cetera, things that are not phone or e-mail communications. The FBI uses that authority as part of its terrorism investigations.

The NSA only uses section 215 for phone call records, not for Google searches or other things. Under section 215, NSA collects phone records pursuant to a court record. It can only look at that data after a showing that there is a reasonable, articulable suspicion that a specific individual is involved in terrorism actually related to al Qaeda or to Iran. At that point, the database can be searched, but that search only provides metadata of those phone numbers of things that are in the phone bill. So the vast majority of records in the database are never accessed and are deleted after a period of 5 years. To look at or use content of a call, a court warrant must be obtained.

Is that a fair description or can you correct it in any way?

General ALEXANDER. That is accurate, Senator. Thank you.

Senator FEINSTEIN. Thank you very much.

Let me express my hope once again. You expressed some things to us yesterday in Intelligence. I think it is really very important to show the cases where this has been used and has been effective and do that tomorrow at the classified briefing for all Senators. Will you do that?

General ALEXANDER. Senator, we are going to bring those. We will bring a layout of all those that have happened. And we will work with the interagency as quickly as possible so that the aggregate numbers can be released by you and others so that the Nation knows how much this has really done to protect us and our allies.

Senator FEINSTEIN. Good. That is appreciated.

Now, let me go to cyber. As you know, the vice chairman of our committee, Saxby Chambliss, with whom I work closely—we have been sitting down trying to forge a consensus information-sharing bill in cyber. Senator Coats, Senator Collins, Senator Mikulski are all members of this committee. And one of the main things is the extent of liability protection, the importance of the domestic portal of entry for cyber attacks.

I would like to ask that you describe what is meant by a civilian portal for Senators assembled here today and also the rationale, why this is important for privacy and other reasons.

General ALEXANDER. Senator, thanks for that question.

The reason, from my perspective, for a portal to one of the civilian infrastructures is so the Nation knows that somebody is not going directly to an intelligence or a military thing with secret information, but rather, give it to, for example, DHS and it can be pushed to FBI and NSA Cyber Command because we all see the data at the same time. And the public will have great confidence that what we are doing is exactly right. Or send it to FBI depending on the type and then FBI can shoot it to both of us. So you have a way of doing this. I think that is critical, given the discussion that we have on the other parts, is that the American people know that we are being transparent.

We do not look at our cyber infrastructure to know what is going into Wall Street, as an example. And so if there is an attack on Wall Street, I will not see it until afterward. And so think of that as a missile coming into Wall Street. The people that do see it, like the Internet service providers, could tell us that—could—but there is no guarantee and there is no quick way of doing that.

Cyber legislation is needed for that. We need to be able to share that information, and all of us need it because we all will have a role there. Our role would be defend the country. If this is a nation state trying to take down Wall Street, you want us to act.

So I think that is the reason for having that civilian portal. That was a longer answer than you probably wanted, but that is why I think all of that is needed.

Senator FEINSTEIN. Thank you.

Let me go to another subject quickly and that is liability protection. And you talked to us a little bit about what the liability protection standards should be in a bill. There are two parts of it. One is for use of a Government countermeasure, and the other is voluntary information-sharing between two companies. I think many members feel companies will not share unless they have immunity from liability. Could you comment on that?

General ALEXANDER. So there are two different aspects, as you stated, and one is how do you share with the Government and what action do you take. And so here is where I think my personal thoughts on this are that if the Government asks the company to do something to protect the networks or to do something and a mistake is made and it was our fault, then they should have liability protection for that. And they should not stand up and have to be sued. So I think there is a case for that.

But if they go company to company or if they are sharing data back and forth, as they do today, I am not sure that the Government needs to provide liability insurance that way.

So I think there are two different things.

Now, this is something that the administration—your folks and we ought to bring everybody together, if that is the key point, and iron that out. I think we want to get it right. There are subtleties to what we just said. So there are different cases and conditions upon when we would act and how we would act and what level of liability you would have. And so I think those are the ones that we truly got to get exactly right.

From my perspective, we just cannot grant everybody gets liability protection. And on the other hand, we do not want to say do something for the Government and if it goes bad, you are on your own. So I think there is something in the middle there that we have to get right, and from my perspective it is when the Government is asking them to do something, we ought to have at least part of that liability protection.

Senator FEINSTEIN. Thank you.

Thank you, Madam Chairman.

Chairwoman MIKULSKI. Senator Boozman and then Senator Tester.

Senator BOOZMAN. Thank you, Madam Chair, and thank you all so much for being here.

I do have some questions about the situation we are in, but I think what I would like to do is wait until we get into the classified. I think you have said about as much as you could say in a setting like this.

I do think that the Senator from Nebraska, though, raised an important consideration that we are probably not talking about enough. I think by any standards, this is a very far-reaching program that really does have tremendous implication to the general public. And having the military—as he said, your record is exemplary. You are a tremendous American. My dad did 20 years active duty, and I will do anything I can to help you all in that regard.

But I do think that the idea of having military control—we have had those firewalls in the past, and that is a discussion at some point that I think we need to have and would appreciate again at some point your contribution in that. But I do think that that is very, very important. And like you said, we are not talking about that.

In regard to cybersecurity, Secretary McFeely, what are the top countries—and you can chime in on this also, General. What are the top countries that are pinging us? Who is involved in this?

Mr. MCFEELY. We do have an answer for that. I believe that would be a more appropriate discussion in our classified setting.

Senator BOOZMAN. So it is not okay to say who is getting after us?

Mr. MCFEELY. I do not believe in this setting based on the fact that our information and our assessment is based on our classified work—I do not believe that—I think I would be overstepping a line.

Senator BOOZMAN. Okay.

You mentioned in your testimony the FBI's collaboration with State and local law enforcement. Again, it is hard for them to deal with this. This is something that they are not, most of the time, equipped to do. Do you feel that the Federal Government, specifically the FBI, is doing enough to aid our State and local departments when they are faced with a cyber attack?

Mr. MCFEELY. You mean specific governments or are we working with State and local law enforcement——

Senator BOOZMAN. Yes, State and local law enforcement.

Mr. MCFEELY. So I think the short answer to that is no, but I am happy to report that we have, I believe, a working plan moving forward. About 2 months ago, we met with various associations representing the police and sheriffs and investigators at the State and local side. And through conversation going through really a discussion of where law enforcement is with the cyber threat, we realized collectively that information is not flowing down to the State and local departments, and even in the instances where it was, they did not have the capability or the level of competence to even address it.

We decided that we needed to address that. We have worked a pilot plan out, and the centerpiece of this will be the Internet Crime Complaint Center where we literally get thousands of complaints in a year from people who have been defrauded over the Internet. Most of the complaints that come in do not meet Federal prosecutive guidelines. In other words, it is not something that a United States Attorney's office would routinely prosecute and it is not something, because these are fraud-type complaints, either the FBI or Secret Service would routinely investigate. But because State and local's competence level is not at the level where it should be, it is just simply falling off.

Chairwoman MIKULSKI. I could not hear your word to Senator Boozman. I could not hear you. Are you saying "confidence" or "competence"?

Mr. MCFEELY. Competence, technical capabilities.

So what we have worked out is a pilot project where we are going to package up these types of threats and actually disseminate them direct to the major departments where the victims are located. At the same time, we are going to increase our outreach to State and local law enforcement and give them the tools and the training that they need to get them up to that level of technical competence that they need.

Senator BOOZMAN. Thank you.

Mr. BEERS. Senator, could I add to that, please?

COLLABORATION WITH STATE AND LOCAL LAW ENFORCEMENT

Senator BOOZMAN. Yes, sir, sure.

Mr. BEERS. So our Secret Service, working with the FBI in a number of cases, as Mr. McFeely indicated, in the joint task force—we have a National Computer Forensics Institute in Alabama. We have trained over 1,300 State and local law enforcement prosecutors and judges in order to be able to deal with this.

What we are dealing with here—that is, mostly their competence or the part of, not the national security threats but the criminal fraud threats—is the stealing of credit cards and other personally identifiable information and using that to take money out of banks around the world. You heard about the $46 million that was taken out of two banks from the Middle East, including a large amount in this country. That is the kind of training where we can give them the competence and we can work with them, and that is something that we and the FBI are trying to do very much. The outreach that we have had to the various police associations and other things are part of it.

But the main thing is to get the training and then to work together. A lot of this happens overseas and that is where we have to be involved in order to be able to trace those activities overseas, which State and local law enforcement do not really have the ability to do. But it is a joint program and really quite successful.

Senator BOOZMAN. Thank you, Madam Chair.

Chairwoman MIKULSKI. Senator Tester.

Senator TESTER. Thank you, Madam Chair.

And I want to thank you all for being here, particularly General Alexander. I want to thank you for coming today. Thank you for your service to our country. And I have been looking at the slides the committee provided, and they are very helpful. We are going to spend more than $13 billion in unclassified cyber activities. Seven agencies are involved, excluding the network defense that every agency must do.

According to my notes, after the WikiLeaks incident in 2010, a Presidential Executive order directed agencies to improve classified network security and create a committee to oversee those improvements. So we have had 3 years to improve the control of classified networks and information. Whatever one thinks of Edward Snowden, it looks to me as if we have also got a big problem that is internal, not external.

So you tell me that the President has requested $13 billion in cyber spending for fiscal year 2014, and yet a contractor, not even somebody who is accountable to your chain of command or anyone else in the Government, is able to get his hands on a copy of a FISA court order allowing the collection of metadata from Verizon. How on earth does this happen? And why does a contractor have access to information that we are spending $13 billion to prevent outsiders from getting their hands on?

General ALEXANDER. So that is one of the grave concerns we both have in that in our networks, the system administration of those networks, the IT infrastructure, was outsourced about 14 years ago to push more of our work out to contractors. As a consequence, many in Government, not just us, have system administrators who are contractors working and running our networks. Now, they do not have total visibility of the network, but they get key parts to it. And in this case, this individual was a system administrator with access to key parts of the network. So we have got to address that. That is of serious concern to us and something that we have to fix.

Senator TESTER. I mean, from your perspective, do you anticipate a recommendation coming forward that this work be done in house instead of contract?

General ALEXANDER. Senator, I am not prepared to make that statement yet. I do not want to react because there are good contractors out there that are doing a good job. I think what we have to do is come back and perhaps look at the oversight mechanism that we have, the checks and balances that are in the system, the automated checks and balances that exist, and what we can do to improve those. As you may know, what the Department is going through in the joint information environment would greatly assist in protecting this data. So going to what we call JIE is a huge step in the right direction.

I think those cloud security and encrypting data is things that we can and should do, but that is going to take time. I do not want to mislead you. This is a significant effort for the Defense Department to move to, but it is one that I know I have personally talked to the Secretary on and the Chairman. We are pushing this. It is the right way to go. I wish we had it. I wish we would go back in time. NSA is doing the same.

BANK ATTACKS

Senator TESTER. Financial services. I am told by folks that I deal with on the Banking Committee that almost every night somebody is trying to hack their system.

Do you have the mechanism by which you can follow up if a bank gave you an IP address that they think that is doing the problem? And if it is not the right question for you, General, you can ship it any way you want. Or do you not have the mechanism to be able to follow up?

General ALEXANDER. So we do as a team, the team here. Almost assuredly, if it is a criminal or other, it would start with the FBI being on the team. We may have people on the team. If the FBI saw this was a foreign one, they would tip that over to us. So we act as a part. DHS has a key role in that team to see what it is. We have made great progress in bringing that team together.

The bottom line to your answer is someone on this team would take it. Normally that leadership would probably be, the cases you described, FBI with DHS and us.

Mr. BEERS. Sir, on that, we gave out 200,000 IP addresses to individuals within this country—to the banks—excuse me—to block when those distributed denial of services attack. Some of those were overseas. We also sent them to friendly governments overseas. So as a matter of course, we do this on a regular basis as part of this tripartite team.

Senator TESTER. Okay. So let me ask you this. If a bank comes to you with an IP address that they believe was trying to hack their system, do you guys follow up on that?

Mr. BEERS. In exactly the same way. The three of us, the three agencies that we represent, go and provide some forensic assistance with respect to that particular incident, and then we provide a larger mitigation message out to the rest of the community so that particular form of attack cannot be replicated.

Senator TESTER. Then do you go back to the bank that has initiated this investigation and tell them what you have done?

Mr. BEERS. We do, and when we put out the information, we do not necessarily indicate which bank was affected. We anonymize that information unless that particular firm wants it public.

Senator TESTER. Okay. So when a bank comes up to me and says, look, we give them IP addresses and they do not follow up on it, you would classify that as being baloney?

Mr. BEERS. Sir, I cannot speak to each and every one of those instances, but what I am telling is the way we work as a team in order to try to do that. And if there are banks that have spoken to you about this, we would be happy to get back to them if they are prepared for you to tell me about that.

Senator TESTER. I do not know that they are, but maybe they are. I cannot say. Actually multiple banks have talked to me about that.

So I just want to say thank you very much. I will tell you that there has been a lot—if I might editorialize just for a second, Madam Chair. There has been a lot of concern about what has happened in the last couple weeks. And I do not serve on the Intelligence Committee. I do serve on Homeland Security, but I do not serve on the Intelligence Committee. And I will tell you that I think it is positive for this country to be having the discussion we are having. And there may be some negatives involved here, but I think it is positive to have the discussion so that we are thinking about civil liberties and we are thinking about freedom as it relates to our national security. You guys all have a tough job, but we will get through this and hopefully we will secure both our security and our freedoms when this is done.

Thank you very much.

Chairwoman MIKULSKI. Senator Murray.

Senator MURRAY. Madam Chairman, thank you very much for having this hearing.

Is "baloney" a Montana name?

Senator TESTER. I was being very nice. I was going to refer to cow excrement here.

QUALIFIED WORKFORCE: CENTERS OF EXCELLENCE

Senator MURRAY. We were lucky.

Again, thank you so much for having this hearing.

Let me just start by saying that I think our Nation's most important cybersecurity resource is its cyber workforce. Without the right people using it, even the most sophisticated technology is really only of limited use. That is why I think it is important that we successfully identify, recruit, and train a cyber workforce to form the foundation of any national cybersecurity plans.

DHS and NSA's Centers of Academic Excellence are really important tools in this effort, and my State, Washington State, hosts a number of these Centers of Excellence. We have the Information

Assurance Education Centers at the University of Washington—Tacoma and the University of Washington—Bothell. We have the Information Assurance Research Center at the University of Washington—Seattle, and the Information Assurance 2-year Education Center at Whatcom Community College. And together those programs offer cybersecurity education and training at the 2-year, undergraduate, masters, and Ph.D. level.

Secretary Beers and General Alexander, if you could comment on how you think these Centers of Excellence play into your respective cyber hiring pipelines and workforce development programs, I would love to hear your comments on that.

Mr. BEERS. Let me go first on that. We absolutely are dependent upon that form of education as a way to get qualified individuals into our workforce. We at DHS have an outreach program to community colleges generally but also to these Centers of Excellence as well as to universities. The only comment that I would make is we do not have enough people around the country trained to do all the jobs that we in Government and the private sector need to have done. I think that is really one of the educational frontiers for this country is to create that kind of a workforce for all of us. So that is certainly something that we support very much at DHS.

Senator MURRAY. General, do you want to comment?

General ALEXANDER. Senator, thank you for that question because that is a huge program that we do with more than 140 different schools collectively between DHS, NSA. And the curriculums that we set up there with those schools—this is not just you get a thing, you go do it. They actually set up a curriculum that helps ensure that the students that are going through that will have the background we need in information assurance, and now in cyber operations, a new one. So there are double credentials that they can get. And I just encourage your schools. I know everybody is looking at that, and we are getting tremendous pressure.

These are very difficult to get into. This is not something that we just grant. It is interesting because we got a number of schools to bring this forward. Some of them do not meet the qualifications and do not get that accreditation. So they work through that. We work with them. We have a great outreach. I think this is great for our country to build these kinds of people——

Senator MURRAY. We absolutely must have that workforce. I agree.

I know that a coherent national cybersecurity strategy really requires some cooperation. You have got to have collaboration between Government, private industry, and academia. And as we saw with the development of the information economy on the Internet, clustering these universities, companies, and the appropriate Government agencies together offer some really great benefits. Within the cybersecurity industry, the South Puget Sound in my State has emerged as a leading cyber cluster, if you will. The unique and nationally recognized resources the region has to offer have created a great environment for cybersecurity to really flourish. They have some great stakeholders who help make this possible, including the Center for Information Assurance and Cybersecurity at the University of Washington. We also have great influential technology and defense companies, Microsoft, Amazon, Boeing, and we have two military installations, Joint Base Lewis-McChord and Washington National Guard Camp Murray in the South Puget Sound. And I have seen personally how those relationships have really benefited that region.

And, Secretary Gallagher, I would love it if you could talk about the importance of these so-called cyber clusters like the one we have in my State and what steps NIST and Commerce are taking to really promote those.

Dr. GALLAGHER. So the notion of clusters as a way of sort of creating this amplification effect that you talk about is broader even than just cybersecurity. In fact, it is a key part of our strategy in other areas like advanced manufacturing. And what tends to happen is you get sort of a critical mass where you have enough expertise that it creates an attracting and pooling, and that talent base really starts to create wins. So you attract the right kinds of companies and government agencies and academic programs.

I think it has to be a key part of the cybersecurity education effort as well because in the end, you are talking about workforce development. And so you are going to have to bring together—that is one of the reasons the public/private partnerships are going to be such a key element here. We are seeing some of that already. Senator Mikulski provided a program funded through NIST, the National Cybersecurity Center of Excellence, which leverages Maryland and Virginia which have also been looking at this sort of effect, to bring in companies to work collaboratively on cybersecurity and create this tipping-in effect that you so eloquently described that are part of clusters.

Senator MURRAY. Great. Well, I am a big proponent of that.

I am out of time, but I did want to submit a question about the National Guard. I think as we move forward, we are going to have to make sure that we are coordinating with them. They are going to be our boots on the ground if there is ever an issue, and I am hoping that we are doing the right things to support them. So, Madam Chairman, I would like to just submit that question.

Chairwoman MIKULSKI. Thank you very much, Senator. And we hope that through the respective subcommittees, there will be follow-ups that will go even deeper to this.

In terms of your clustering, we in Maryland feel we are at the epicenter of cybersecurity because we have the National Security headquartered there. We have the National Institute of Standards headquartered there. We hope to have the FBI headquartered there. We have the University of Maryland——

Senator MURRAY. Yes. Well, we will take the west side of the country.

Chairwoman MIKULSKI. But thank you very much.

I think, Senator Shelby, did you want to say something, sir?

Senator SHELBY. I just have one last observation. I just want to thank the panel, all of you, for your service to the country, the way you have conducted yourself before you got here today, and what you have done here for the day for America. And I think it has to be said. We have worked together a long time. Thank you.

ADDITIONAL COMMITTEE QUESTIONS

Chairwoman MIKULSKI. Well said, Senator Shelby.

If there are no further questions this afternoon, Senators may submit additional questions for the committee's official record, and we request the witnesses' response within 30 days.

[The following questions were not asked at the hearing, but were submitted to the Departments for response subsequent to the hearing:]

QUESTIONS SUBMITTED TO HON. GENERAL KEITH B. ALEXANDER, COMMANDER, U.S. CYBER COMMAND DIRECTOR, NATIONAL SECURITY AGENCY CHIEF, CENTRAL SECURITY SERVICE

QUESTIONS SUBMITTED BY SENATOR PATTY MURRAY

Question. Currently, the development, marketing, sale, and resale of software exploits, including attack capabilities, is legal and unregulated making it one of the few remaining unregulated weapons markets.

Is it in the United States' interest to allow the open and unfettered sale of these exploits and other attack capabilities? What steps are currently being taken to protect the United States against the proliferation of these capabilities?

Answer. We share the concerns of the Committee and others about the unfettered proliferation of malicious cyber tools and the potential misuse of those tools to inflict harm against U.S. interests and those of our allies. With other agencies, we are studying the global export market for cyber technologies, and what actions may be prudent for national security, while being mindful of U.S. industry's need to innovate to meet global demand for cyber defense capabilities.

Question. Given the risk that cyber attack poses to critical infrastructure and other important domestic systems, creating and maintaining a robust cyber civil defense is essential. Traditionally, National Guard units have played a central role within civil defense and in Washington State, the 262nd Network Warfare Squadron—the first operational non-flying wing within the Air National Guard—has extended its response and support capabilities to cyberspace.

What steps is CYBERCOM taking to coordinate with Guard units like the 262nd to improve homeland readiness and resilience in the face of cyber attack?

Answer. Currently, we conduct exercises and training with the 262nd Network Warfare Squadron focused on responding to a domestic cyber attack against critical U.S. infrastructure. These events involve intense collaboration and coordination across Federal, State, and private sector boundaries. Going forward, we are working with USNORTHCOM and the National Guard Bureau to develop a broad framework for integrating the National Guard into the Cyber Mission Forces. This framework will guide the Service components as they work to incorporate additional cyber capabilities into their forces.

QUESTIONS SUBMITTED BY SENATOR RICHARD J. DURBIN

CYBER EXECUTIVE ORDER—ROLE OF THE EXECUTIVE ORDER VERSUS CYBER LEGISLATION

Question. President Obama issued Executive Order (EO) 13636 in February of this year. What is the effect of this Executive order? Is it improving your ability to share information with the private sector?

Answer. The overall effect of the Executive order is to jump-start some key initiatives that begin to address the cybersecurity threat.

—With implementation of the Enhanced Cybersecurity Services, a USG/industry partnership program, the robust cybersecurity protections currently afforded only to the Defense Industrial Base primarily through cleared commercial service providers will be made available to all critical infrastructure sectors while minimizing the potential for divulging our classified sources and methods.

—The cybersecurity framework to be developed by the National Institute of Standards and Technology in partnership with industry will help owners and operators of critical infrastructure to understand the levels of security measures that are needed to make it more difficult for adversaries to penetrate their networks.

—The voluntary certification program is designed to encourage and assist owners and operators of critical infrastructure to adopt those standards to harden their networks.

- —All three efforts recognize that cybersecurity is a team effort and must be done with full collaboration within Government and with industry and other private stakeholders.

I think it is essential; however, that all parties realize that the Executive order (EO) is only a first step in addressing the threat and not a substitute for actual legislation. The EO can move us only so far, and it does not eliminate the need for Congress to enact cybersecurity legislation.

While the Executive order does make some headway in enabling and facilitating some cybersecurity information sharing across a larger portion of the critical infrastructure, such sharing remains largely one-sided—from the USG to private sector. With so much of the critical infrastructure owned and operated by the private sector, the Government is often unaware of the malicious activity targeting our critical infrastructure. These blind spots prevent the Government from being in a position to either help defend the critical infrastructure or to defend the Nation from a cyber attack, if necessary. This can only be overcome through legislation that removes statutory barriers to cybersecurity information sharing and provides the narrowly scoped liability protections needed to incentivize two-way, real-time information sharing between the private sector and the Government. Similarly, we need legislation that encourages industry cooperation in the development and implementation of the cybersecurity standards that will secure their networks.

Question. When he signed the Executive order, President Obama also underscored the need for comprehensive cybersecurity legislation, since the scope of the Executive order is limited. What are your legislative priorities in terms of items you believe should be included in cyber legislation?

Answer. I believe that cyber legislation needs to:

- —Eliminate the statutory information sharing barriers and facilitate two-way, real-time cybersecurity information sharing between the private sector and the Government as well as among private companies. Any legislation must instill confidence that such sharing will protect privacy and civil liberties, and will preserve the longstanding, respective roles and missions of civilian and intelligence agencies. It also needs to provide reasonable liability protections for companies in order to incentivize such information sharing.
- —Build on the efforts under EO 13636 to develop a cybersecurity standards framework and certification program by incentivizing the private sector to adopt the framework to protect its networks.

CYBER EXECUTIVE ORDER—PROTECTING PRIVACY AND CIVIL LIBERTIES

Question. The Executive order requires Federal agencies to develop cybersecurity efforts in accordance with the Fair Information Practice Principles, as well as other policies, principles, and frameworks to protect privacy and civil liberties. I worked with a number of other Senators to ensure that the Cybersecurity Act of 2012 included provisions to protect privacy and civil liberties.

What specific steps can government agencies take to ensure that privacy and civil liberties are protected as we enhance our Nation's cybersecurity?

Answer. I believe that the U.S. Government could take the following steps to ensure that privacy and civil liberties are protected:

- —Ensure transparency by establishing processes and procedures based on Fair Information Practice Principles for the U.S. Government receipt, retention, use, and disclosure of cyber threat information received from the private sector.
- —Require independent review and oversight to ensure that use and sharing restrictions are being enforced.
- —Leverage technology to establish a transparent, real-time, policy-based, machine-to-machine messaging construct that automatically enforces the policy/rules for use and any restrictions on sharing.

QUESTIONS SUBMITTED BY SENATOR MARY L. LANDRIEU

CYBERSECURITY ROLE FOR THE NATIONAL GUARD

Question. On June 13, 2013, the day of the Appropriations Committee hearing entitled "Cybersecurity: Preparing for and Responding to the Enduring Threat", the Committee received a report from the Department of Homeland Security (DHS) and Department of Defense (DOD) which was due to Congress on May 1, 2012, as prescribed in the joint explanatory statement accompanying the fiscal year 2012 DHS Appropriations Act (Public Law 112–74). The purpose of the report was to outline the capabilities of a coordinated response to a cyber attack by DHS and the National Guard and how critical relationships can be established across the agencies to fulfill cybersecurity responsibilities. The information provided, which was submitted separately by the two agencies, outlines on a high-level, the programs DHS and DOD (as a whole) are maintaining for a response. Unfortunately, the report falls short of providing Congress an understanding of the DHS and National Guard's capacity to respond to a cyber attack jointly. In order for Congress to better understand the gap between capacity and need, a sense of scope is required.

How many National Guard cybersecurity personnel currently exist, and where? Are they employed in teams or individually? If they are employed in teams, how many teams are there and where are they located?

Answer. Although these questions are better directed to the National Guard Bureau, I understand that there are approximately 1,000 National Guard personnel in cybersecurity positions. The U.S. Army National Guard is filling 8-person Computer Network Defense teams in each State that operate part-time in support of State missions. Additionally, the U.S. Air Force has established Air National Guard units in Washington, Delaware, Rhode Island, Maryland, California, and Kansas. USCYBERCOM continues to explore with the Services the unique capabilities the National Guard brings to the Total Force and the role they will have in securing our Nation in cyberspace.

Question. As DOD and DHS are building the capacity the Federal Government needs to protect against and respond to a cyber attack: what specific role is being considered for the National Guard; and how is the Guard's ability to switch between title 32 authorities and title 10 authorities being taken into consideration?

Answer. We are working through the best way to strategically integrate the National Guard into the cyber national defense mission to include the Guard's particular authorities and capabilities. Most importantly, National Guard forces should complement the Total Force in the same way that they do for other missions. As part of a Total Force solution, the National Guard forces will need to be trained to the same standard as the active forces to meet those requirements.

Although we are focused on working with the Services and the National Guard Bureau on how these personnel can help meet DOD requirements, the Department is actively engaged with its interagency partners and the States to improve our ability to respond to cybersecurity challenges in a whole-of-Government approach that leverages all appropriate authorities.

It is also important to note that, as Chairman of the Joint Chiefs of Staff General Martin Dempsey stated in recent congressional testimony, title 32 may not provide authorities for operating in cyberspace. Any activities on networks within a State's jurisdiction which have effects outside of that jurisdiction would have to be conducted under title 10 authorities. This will be an important factor in the planned integration of the National Guard into the cyber national defense mission.

Question. Is there a cost savings associated with utilizing the National Guard based on current training? How much?

Answer. In coordination with the services, the Department is working out how to create an effective cyber workforce by looking across the Total Force in a way that best meets DOD cyber requirements. As a critical element of building its force structure, USCYBERCOM has established common training requirements for all of its personnel, Active component, Reserve component, or civilian.

We are eager to leverage the skills and training of all our team members while we ensure that they are properly trained and certified to carry out their USCYBERCOM mission. It is very difficult to estimate potential savings based upon current training of personnel, as it will be highly dependent both upon the particular training and certification an individual has previously received and how much training meets the requirements of roles to which the personnel will be assigned.

Question. Are there skills identified within the National Guard that cut down the time needed to train a cyber airman or soldier to be able to respond to a cyber attack?

Answer. The services retain training and accreditation authorities for all training. Each service will make a determination on what civilian skills, experience, and credentials might be credited for required military training.

USCYBERCOM is establishing common training requirements for all of its forces. Skills may help them progress and support their ability to operate, while ensuring that all of our forces are trained to the same standard.

CYBER TEST BEDS/RANGES

Question. General Alexander testified that the services, departments, and agencies need to work together to ensure that they have adequate test bed and range space to safely organize, train, and equip the cyber warriors, operators, managers, researchers, and agents across the Federal Government.

What are the specific requirements that your departments and their various agencies have for test bed and range space?

Answer. Test bed and range spaces must support training on all aspects of the USCYBERCOM mission as specified by the Joint Cyber Training and Certification Standards and the Cyber Forces Concept of Employment. They also need to be capable of supporting training, exercise, and mission rehearsal events from multiple locations on a 24/7/365 basis.

Question. What specific outcome will those established requirements render in trained personnel and tactics?

Answer. Testing and range space that fulfills those requirements will foster an environment that ensures the Cyber Mission Forces are consistently trained and certified to perform operations in defense of the Nation and, when authorized, to project force. Methods of training tactics development will include force on force, force vs. simulated opposition forces, and force vs. live opposition forces.

Question. What is the current test bed and range capacity available to each of your departments?

Answer. USCYBERCOM has access to the Department of Defense's four cyber ranges that support testing and training: the Joint Information Operations Range, the Department of Defense Information Assurance Range, the National Cyber Range, and the C4 Assessment Division. USCYBERCOM also has limited in-house standalone test labs.

Question. What is the wait time or backlog based on the access you currently have?

Answer. Currently, exercise events are developed to meet specific requirements for the training audience. In correlation with the development, wait time varies based on range schedule availability and planning. Based on historical data from recent range events, the average wait time is 60–90 days for a small (10–15 participants) event, and 6–9 months for large-scale exercises such as Cyber Flag.

Question. Have you identified additional test bed or range space that you would like to acquire, use, or lease?

Answer. USCYBERCOM is working with the Joint Information Operations Range, the DOD Information Assurance Range, the National Cyber Range, and the C4 Assessment Division to identify future capacity needed to accommodate projected DOD cyber testing and training requirements.

Question. What are the fiscal year 2013 and 2014 funding levels for testing and training space?

Answer. Although USCYBERCOM has access to these ranges, we do not program their funding nor are the ranges under a single program manager. The Command is collaborating with the range program managers in a federation of the willing in order to coordinate strategic planning/programming. For specific USCYBERCOM events, COCOM Engagement and Training Transformation funding was allocated from the baseline USCYBERCOM fiscal year 2013 exercise funding and fiscal year 2014 funding will likely be similar.

Question. What percentage of your required testing and training needs will you be able to meet in fiscal year 2013 and 2014?

Answer. Of the projected training and certification events to support the Cyber Mission Force, approximately 30 percent of the events can be supported by the test beds and ranges currently available to USCYBERCOM. However, the Command is working with the Joint Information Operations Range, the DOD Information Assurance Range, the National Cyber Range, and the C4 Assessment Division to identify the capacity needed in fiscal year 2014 and beyond to accommodate projected DOD cyber testing and training requirements.

QUESTIONS SUBMITTED BY SENATOR TOM UDALL

ROLE OF NATIONAL LABORATORIES IN PROMOTING CYBERSECURITY

Question. General Alexander, our National Labs—which are the crown jewels of our Nation's research system—are active in efforts to promote cybersecurity. In my home State of New Mexico, Sandia National Laboratories is engaged in efforts to secure the national electrical grid from cyber attack. Los Alamos National Laboratories is a leader in quantum cryptography. Sandia also has partnerships with universities and the private sector. They're helping computer science students become cyber professionals.

Could you discuss what role our National Labs should have in protecting our Nation from cyber attack?

Answer. Our National Labs are incredible resources that continue to make vital contributions to cybersecurity and broader national security. The three areas that you have identified are three of the most important ways that the National Labs are supporting U.S. cybersecurity efforts: advanced research to secure our vulnerable infrastructure from cyber threats; the improvement of our abilities to transmit and store data securely; and, potentially most importantly, the development of the cybersecurity professionals that are our most critical asset.

NEED FOR INTERNATIONAL COOPERATION FOR CYBERSECURITY STANDARDS

Question. General Alexander, your testimony describes how USCYBERCOM is working to defend the Nation against threats from cyberspace, especially those that could involve attacks directed by foreign states. But cyberspace does not really recognize national borders, and we have many shared interests in terms of cybersecurity with other nations. Stopping cyber criminals, for example, requires cooperation from other countries. Earlier this year, a criminal network involving hackers from several countries allegedly stole $45 million from banks using fake ATM cards.

How do we ensure our national security while also working toward better international cooperation in the area of cybersecurity?

Answer. International cooperation on cybersecurity is a requirement to ensure our national security. Global cooperation is necessary to address the threat, build consensus on the norms of responsible conduct in cyberspace, and address ongoing malicious activity. For our military, cybersecurity cooperation, including shared situational awareness, is foundational to interoperability and mission success globally as is the case in other domains.

Question. How do we reduce cyber vulnerabilities while protecting a free and open Internet for all?

Answer. As the President's International Strategy for Cyberspace says, "To realize fully the benefits that networked technology promises the world, these systems must function reliably and securely. People must have confidence that data will travel to its destination without disruption Assuring the free flow of information, the security and privacy of data, and the integrity of the interconnected networks themselves are all essential to American and global economic prosperity, security, and the promotion of universal rights." A cyberspace that rewards innovation, empowers individuals, develops communities, safeguards human rights, and enhances personal privacy will strengthen national and international security. We will reduce our cyber vulnerabilities and defend our networks with smart policies that combine national and international resilience with vigilance and a range of credible response options. Building capacity and fostering innovation is necessary to achieve reliable, secure, and safe platforms and build confidence in globally interconnected networks. This is why partnerships are so important: domestic and international, public and private sectors.

CHINA AND THEFT OF INTELLECTUAL PROPERTY

Question. General Alexander, your testimony mentions the systematic theft of American intellectual property. This is a serious challenge, particularly if aided and abetted by foreign states. President Obama reportedly raised concerns about this with Chinese President Xi Jinping last week.

How should our Nation respond if such directed cyber thefts are not curtailed?

Answer. In February 2012, the administration published a comprehensive strategy on mitigating the theft of U.S. trade secrets, which is currently being implemented. Consistent with the Strategy, we need to respond to cyber intrusions that result in the theft of American intellectual property in three ways. First, the U.S. Government must work with like-minded countries to clearly define acceptable and unacceptable behaviors in cyberspace and to promote related international norms, including effective criminal and civil enforcement. Second, the U.S. Government must work with private sector entities to develop more defensible network architectures and computing devices that do not contain vulnerabilities that countries such as China can exploit for economic gain. As these network architectures and computing devices are hardened, we must promote development, sharing and deployment of industry-led voluntary best practices in the private sector to protect U.S. intellectual property, including trade secrets. Third, the U.S. Government must continue to develop and implement defensive cyber capabilities to protect the Nation from threats to its economic health and stability.

QUESTIONS SUBMITTED BY SENATOR THAD COCHRAN

Question. All witnesses, we have heard about the importance of cooperation and clearly defined lanes of responsibility across the Federal Government for our cybersecurity efforts. What are your respective roles in receiving and sharing threat information with the private sector?

Answer. We are leaning forward to the maximum extent authorized to share knowledge across the U.S. Government and private sector. In accordance with EO 13636, and consistent with its legal authorities and mission responsibilities, NSA/CSS provides classified cyber threat information and associated network defense guidance to DOD, DHS, and DOJ/FBI to use in support of their specific cybersecurity roles and responsibilities. Through the voluntary Enhanced Cybersecurity Services and Defense Industrial Base Enhanced Cybersecurity Services programs, NSA/CSS is working with DHS and DOD to provide classified cyber threat and technical information to eligible critical infrastructure companies or commercial service providers that offer security services to critical infrastructure.

Question. All witnesses, I think we all recognize the importance of defending our Nation's critical infrastructure against cyber attacks. A foreign or terrorist cyber attack on our electric grid, water systems, or financial systems could cause widespread damage and even have detrimental effects on our economy and consumer confidence. There has been much discussion about how involved the Federal Government should be in defending infrastructure owned by non-Federal entities. How would you define the threshold for what types of non-Federal infrastructure might qualify as "critical" for these purposes?

Answer. I believe the definition of "critical infrastructure" used in PPD–21 Critical Infrastructure Security and Resilience is a reasonable one, and it applies to both Federal and non-Federal critical infrastructures. It defines critical infrastructure as those "systems and assets, whether physical or virtual, determined by a sector specific agency or DHS to be 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 or safety, or any combination of those matters."

Question. General Alexander, a British newspaper recently reported on a program called "Prism," in which it referred to collection under section 702 of the Foreign Intelligence and Surveillance Amendments Act. The newspaper reported that the law "allows for the targeting of any customers. . . who live outside the U.S. or those Americans whose communications include people outside the U.S." Can you explain if and how this description may be inaccurate?

Answer. The quoted statement is inaccurate. Section 702 does not allow the Government to target Americans inside or outside the United States.

Section 702 of FISA allows "the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information." 50 U.S.C. 1881a(a).

Additionally, the statute provides several express limitations, namely that such acquisition:

(1) may not intentionally target any person known at the time of acquisition to be located in the United States;

(2) 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;

(3) may not intentionally acquire any communication as to which the sender and all intended recipients are known at the time of acquisition to be located in the United States; and

(4) shall be conducted in a manner consistent with the fourth amendment to the Constitution of the United States.

50 U.S.C. 1881a(b).

An acquisition authorized under section 702 must be conducted in accordance with targeting procedures reasonably designed to "ensure that any acquisition authorized. . . is limited to targeting persons reasonably believed to be located outside the United States." 50 U.S.C. 1881a(c) and (d)(1). These targeting procedures are subject to judicial review and approval by the Foreign Intelligence Surveillance Court (FISC). 50 U.S.C. 1881(d)(2). Minimization procedures must also be adopted and are subject to FISC review. 50 U.S.C. 1881(e)(2) Among other requirements, joint authorizations by the U.S. Attorney General and Director of National Intelligence under section 702 must attest that "a significant purpose of the acquisition is to obtain foreign intelligence information" and that the acquisition complies with the above limitations. 50 U.S.C. 1881a(g)(2).

Question. All witnesses, we've often heard that there is a potential for a Cyber Pearl Harbor, or an unexpected cyber attack on our Nation by a foreign entity that has dramatic and lengthy consequences. I think it may be difficult for most Americans, and even members of this Committee, to visualize how exactly such an attack would be carried out and what it would look like. Can you help us to better understand these things? Are the appropriations this Committee has been recommending sufficient to help prevent such an attack?

Answer. In a 20 July 2012 opinion piece published online in the Wall Street Journal, President Obama reflected on lessons learned from a national-level exercise conducted the previous month to test how well Federal, State, and local governments and the private sector can work together in a crisis. According to the exercise scenario, that crisis was the result of a cyber attack by unknown hackers who had inserted malicious software into the computer networks of private-sector companies that operate most of our transportation, water, and other critical infrastructure systems. The simulated consequences included train derailments across the country, including one carrying industrial chemicals that exploded into a toxic cloud. Water treatment plants in several State had shut down, contaminating drinking water and causing Americans to fall ill. This worst-case scenario included both cyber and physical consequences and targeted our Nation's critical infrastructure. In October 2012 Secretary of Defense Panetta described a cyber Pearl Harbor as just such a combination of events.

We believe the administration budget requests are on target and we appreciate the Committee's willingness to fund them. Our strength in facing this threat relies on the entire U.S. Federal Cybersecurity Operations Team including DHS, DOJ/FBI, and DOD to counter cyber threats. We each have specific, critical roles, responsibilities, and authorities. We are already working together as part of the Federal effort to counter cyber threats, and we are partnering to implement EO 13636 to improve the cybersecurity of our critical infrastructure. There are issues with being able to see and prepare for a cyber attack, as no single public or private entity has all of the required authorities, resources, or capabilities to either respond to or prevent a serious cyber attack on our critical infrastructure. We must address this threat as a team by sharing the unique insights into cyber threats that both the Government and the private sector have and by hardening our critical infrastructure and making it more resilient to cyber threats. We need legislation that removes existing barriers to the sharing of cyber threat information between the private sector and the U.S. Government at network speed, while ensuring that privacy and civil liberties are protected. We also need legislation that offers incentives to encourage core critical infrastructure operators to harden their networks.

QUESTIONS SUBMITTED BY SENATOR MIKE JOHANNS

CYBER COMMAND

Question. General Alexander, I would like to ask several questions about the potential elevation of Cyber Command to a unified combatant command. Last year's National Defense Authorization Act included language that instructs DOD to brief Congress on any proposal to elevate the command. The language asks for specific information such as a clear statement of mission, an outline of national security benefits, as well as a cost estimate.

Has DOD prepared this required information and have you shared it with Congress?

Answer. If the administration were to make such a significant change to the Unified Command Plan, it would certainly share the details with Congress.

Question. Do you agree that it would be inappropriate to stand up a new unified command without possessing this information and sharing it with Congress for review?

Answer. I believe that Congress should be informed on the analysis, decision-making factors, and outcome of any changes to the Unified Command Plan.

Question. In particular, what would be the costs associated with elevating Cyber Command to a unified combatant command beyond the initial establishment of the command—costs specifically related to operations?

Answer. If the decision is made to elevate USCYBERCOM to a unified command, it is unknown at this time whether there would be costs beyond the initial establishment of the command related to operations. Any cost increases or decreases will be dependent upon the responsibilities and authorities assigned.

Question. I have heard some assert that no additional allocation would be needed to elevate Cyber Command. Regardless of whether costs are absorbed by taking away from other DOD missions or expending newly allocated tax dollars, there will be operational expenses. What is DOD's estimation of these expenses?

Answer. If the decision is made for significant changes to the Unified Command Plan—such as creating an additional unified command—there will likely be costs involved. The exact costs and any potential effect on the overall DOD budget, however, will be dependent upon a variety of implementation factors including assigned responsibilities, authorities and manning.

Question. What do you believe are the advantages and disadvantages of dual-hatting an individual as both the commander of a unified command and of the National Security Agency?

Answer. Currently, the dual-hatting of the Director of the National Security Agency and the Commander of USCYBERCOM is a strategic advantage for the Nation. It has enabled DOD to leverage NSA's capabilities needed for the conduct of USCYBERCOM's mission. The concept ensures that the most knowledgeable officer on the global cryptologic platform maintains superior situational awareness, empowering swift and effective decisionmaking associated with national intelligence and military objectives.

Question. In light of the widespread concern about an appropriate balance between national security and the privacy rights of American citizens, is there wisdom in avoiding giving one person virtually unprecedented power as the head of both a unified command and a civilian intelligence agency?

Answer. I do not believe that there is. It is imperative that the Commander of USCYBERCOM understand the global cryptologic platform. The dual-hat relationship facilitates this knowledge and ensures that the Commander can maintain situational awareness and respond when required in an extremely high-paced, complex, technical environment—while applying to both jobs a single ethos of protecting privacy rights.

Question. What is the timeline for Secretary Hagel's decision?

Answer. I do not know if there is a timeline for any decision on this topic.

Question. At one point there was talk that DOD might slip this important change into an out-of-cycle adjustment to the Unified Command Plan (UCP). Can you assure us this will not be the case?

Answer. Any final recommendation on changes to the Unified Command Plan to the President will be made through the Secretary of Defense.

Question. Will you commit to us that before a final decision is made, Congress will be provided a mission statement, clearly defined parameters for combat action, and cost estimate?

Answer. I am sure that the Secretary of Defense will work with the White House to ensure that our oversight committees have the information that they need to be comfortable with any decisions regarding the status of this command.

QUESTIONS SUBMITTED TO HON. RAND BEERS, ACTING DEPUTY SECRETARY, DEPARTMENT OF HOMELAND SECURITY

QUESTIONS SUBMITTED BY SENATOR PATTY MURRAY

Question. Currently, the development, marketing, sale, and resale of software exploits, including attack capabilities, is legal and unregulated making it one of the few remaining unregulated weapons markets.

Is it in the United States' interest to allow the open and unfettered sale of these exploits and other attack capabilities? What steps are currently being taken to protect the United States against the proliferation of these capabilities?

Answer. The Department of Homeland Security (DHS) works closely with public and private sector partners to coordinate the discovery and responsible disclosure of software vulnerabilities before they can be exploited. DHS cybersecurity experts are following the evolution of the software vulnerability marketplace, including legitimate "bug bounty" programs, to ensure that our resources are being applied to address gaps in vulnerability discovery and mitigation that industry alone cannot correct. DHS's Science and Technology Directorate, through its Software Quality Assurance project, is developing technologies to improve techniques in software quality assurance tools to better detect these types of vulnerabilities in software systems. DHS S&T will offer these technologies and improvements through the Software Assurance Marketplace (SWAMP), a state-of-the-art facility designed to advance our Nation's cybersecurity by providing a collaborative research environment to improve software development activities that will protect the national cyber and critical infrastructure systems against the proliferation of these software vulnerabilities and threats. In addition, DHS is working with our international industry and government partners to ensure that software and supply chain risks can be proactively addressed worldwide.

Question. The North American Electric Reliability Corporation (NERC) has been among the more successful industry solutions to ensuring basic levels of cybersecurity across whole sectors of critical infrastructure. While its mandatory cybersecurity standards are broadly implemented across the bulk power system, NERC's voluntary standards are minimally adhered to. Compounding this dynamic is the length of time NERC takes to issue new mandatory standards; many of the voluntary standards issued since the last ruling are recognized as essential cybersecurity measures in the face of today's cyber threats. Given that NERC is a leader across the greater realm of critical infrastructure, I am concerned with the cyber readiness of other sectors.

How can Congress facilitate the formulation and adoption of acceptable standards within the current regulatory framework and create the structures needed to develop these standards in the first place within the sectors that lack them?

Answer. Congress can leverage the consultative process adopted during the development of the National Institute of Standards and Technology's Cybersecurity Framework called for in section 7 of Executive Order (EO) 13636, as well as regulatory agencies' assessments of current regulatory frameworks from section 10 of the EO, to assess the need for new or updated standards and ensure that such standards are flexible and adaptable given evolving technologies and unique risk environments. Congress can also work with DHS, Sector-Specific Agencies (SSAs), the independent regulatory agencies, and the private sector to understand the constraints that limit adoption and to implement voluntary or legislative solutions to reduce burdens or increase benefits of adoption or compliance. By assessing whether, and how, a lack of standards or standard adoption is resulting in sub-optimal cybersecurity outcomes, Congress can promote solutions associated with a measurable business case, and encourage the adoption of particular standards by sector organizations, SSAs, insurers, and other relevant bodies. This may also include the promotion of particular incentives, such as those identified in the DHS, DOC and Treasury responses to the EO 13636/Presidential Policy Directive-21 tasking on incentives studies.

QUESTIONS SUBMITTED BY SENATOR RICHARD J. DURBIN

CYBER EXECUTIVE ORDER—ROLE OF THE EXECUTIVE ORDER VERSUS CYBER LEGISLATION

Question. President Obama issued Executive Order 13636 in February of this year. What is the effect of this Executive order? Is it improving your ability to share information with the private sector?

When he signed the Executive order, President Obama also underscored the need for comprehensive cybersecurity legislation, since the scope of the Executive order is limited. What are your legislative priorities in terms of items you believe should be included in cyber legislation?

We'd like to hear from all the witnesses on this issue.

Answer. Facing persistent and constantly evolving threats to our Nation from cyber attacks that could disrupt our power, water, communication and other critical infrastructure, the President issued Executive Order (EO) 13636 on Improving Critical Infrastructure Cybersecurity and Presidential Policy Directive (PPD) 21 on Critical Infrastructure Security and Resilience. These policies reinforce the need for a holistic approach to security and risk management.

Implementation of the EO will drive action toward system and network security and resiliency, and will also enhance the efficiency and effectiveness of the U.S. Federal Government's work to secure critical infrastructure and make it more resilient. Information sharing is a critical component of a comprehensive strategy, and section 4 of the EO directs the Department of Homeland Security (DHS) to expand its reporting and dissemination of cyber threat information, expedite security clearances, and expand the use of private sector subject matter experts in the Federal Government in order to build and strengthen information sharing partnerships.

Section 4 also directs DHS to expand the Enhanced Cybersecurity Services (ECS) program to all critical infrastructure sectors.

The ECS program coordinates the protection, prevention, mitigation, and recovery from cyber incidents through information sharing initiatives with business owners and operators to strengthen their facilities and communities. ECS is a voluntary information sharing program that assists critical infrastructure owners and operators as they improve the protection of their systems from unauthorized access, exploitation, or data exfiltration. DHS works with cybersecurity organizations from across the Federal Government to gain access to a broad range of sensitive and classified cyber threat information. DHS develops indicators based on this information and shares them with qualified Commercial Service Providers (CSP), thus enabling them to better protect their customers who are critical infrastructure entities.

ECS augments, but does not replace, an entity's existing cybersecurity capabilities. It does not involve any Federal Government monitoring of private networks or communications, and information relating to threats and malware activities detected by the CSPs is not directly shared between the critical infrastructure CSP customers and the Federal Government. Any information shared by a CSP customer is done so voluntarily, in an anonymized fashion. As directed in EO 13636, the ECS program is available to each of the 16 critical sectors.

Although this EO will help to bolster the Nation's cyber defenses, it does not eliminate the urgent need for legislation in these and other areas of cybersecurity. The administration's legislative priorities for the 113th Congress build upon the President's 2011 Cybersecurity Legislative Proposal and take into account 2 years of public and congressional discourse about how best to improve the Nation's cybersecurity.

The administration believes that legislation should:

1. Facilitate cybersecurity information sharing between the Government and the private sector, as well as among private sector companies, while protecting privacy and civil liberties, reinforcing the appropriate roles of civilian and intelligence agencies, and including targeted liability protections;
2. Incentivize the adoption of best practices and standards for critical infrastructure by complementing the process set forth under the EO;
3. Give law enforcement the tools to fight crime in the digital age;
4. Update Federal agency network security laws, and codify DHS's cybersecurity responsibilities;
5. Create a National Data Breach Reporting requirement that includes notification to law enforcement personnel.

Privacy and civil liberties safeguards must be a core component of each of these legislative areas.

CYBER EXECUTIVE ORDER—PROTECTING PRIVACY AND CIVIL LIBERTIES

Question. The Executive order requires Federal agencies to develop cybersecurity efforts in accordance with the Fair Information Practice Principles, as well as other policies, principles, and frameworks to protect privacy and civil liberties. I worked with a number of other Senators to ensure that the Cybersecurity Act of 2012 included provisions to protect privacy and civil liberties.

What specific steps can government agencies take to ensure that privacy and civil liberties are protected as we enhance our Nation's cybersecurity?

Answer. The Department believes that protecting privacy and civil liberties requires attention in all phases of cybersecurity activities. In addition to following the Fair Information Practice Principles and any applicable laws or other frameworks that protect individual rights, agencies can do the following to ensure that privacy and civil liberties are protected as we enhance our Nation's cybersecurity:

1. Proactively engage with program managers and staff to identify cybersecurity activities;
2. Identify any potential privacy or individual rights concerns associated with those activities;
3. Implement proactive privacy and civil liberties protections
4. Assess activities in a way to minimize risks to privacy and individual rights;
5. Develop policies and procedures to mitigate any remaining risks to individual rights.

The Department recognizes that the involvement of the privacy and civil rights and civil liberties advocacy community is helpful both for purposes of establishing an advisory relationship and for building robust oversight into security processes. For EO and PPD implementation, DHS hosted five sessions with these communities to educate them on the Department actions for critical infrastructure security and resilience and to solicit their expert guidance as programs are put into place.

Privacy is an integral component of the DHS cyber mission. Within the Office of Cybersecurity and Communications (CS&C), the ECS program and the National Cybersecurity Protection System (NCPS), or EINSTEIN, are good examples of how DHS builds privacy and civil liberties protections into cyber activities. DHS conducted both classified and unclassified Privacy Impact Assessments (PIA) for both programs, to fully assess the privacy protections in place. These PIAs provide a comprehensive understanding of the CS&C cybersecurity programs, further increasing transparency. The DHS Office for Civil Rights and Civil Liberties has also provided advice to both ECS and EINSTEIN program leadership since the inception of the programs to ensure that appropriate protections are built in. The Office has also provided civil liberties training to the U.S. Computer Emergency Readiness Team (US–CERT) personnel, articulating principles for operators to ensure the protection of individual rights.

Specifically, the ECS program exemplifies how the Department is working to build cybersecurity partnerships based off of transparency and privacy protections. ECS is a voluntary information sharing program through which the Federal Government provides sensitive and classified cyber threat indicators to Commercial Service Providers (CSP), enabling them to augment the cybersecurity services available to critical infrastructure entities. ECS does not monitor private networks or communications. While CSPs may provide anonymized, aggregated information about encountered threats, this high-level information is strictly used to ascertain the effectiveness of information sharing and to help DHS better respond to critical infrastructure's needs.

Additionally, DHS conducts quarterly reviews of indicators and signatures and has conducted an overall Privacy Compliance Review of the EINSTEIN program. We also work to ensure that NPPD collects only the data necessary to support computer network defense activities. Standard operating procedures ensure that we minimize data collection to only the information that we determine is analytically relevant to pre-defined known or suspected cyber threats.

This commitment to the protection of privacy and civil liberties in DHS cybersecurity activities is longstanding. As part of the Cyberspace Policy Review conducted by the administration in 2009, the Department met with privacy and civil liberties advocates and academics (at a Top Secret/Sensitive Compartmented Information [TS/SCI] level) to discuss the Advanced Persistent Threat landscape and the Federal Government response. That meeting led to the creation of a subcommittee of DHS's Data Privacy and Integrity Advisory Committee (DPIAC), which is briefed regularly at the TS/SCI level. Last year, the DPIAC subcommittee produced a report that sets forth recommendations for DHS to consider when evaluating the effectiveness of cybersecurity pilots and for specific privacy protections for DHS to consider when sharing information from a cybersecurity pilot with other agencies.

Questions Submitted by Senator Mary L. Landrieu

CYBERSECURITY ROLE FOR THE NATIONAL GUARD

Question. On June 13, 2013, the day of the Appropriations Committee hearing entitled "Cybersecurity: Preparing for and Responding to the Enduring Threat", the Committee received a report from the Department of Homeland Security (DHS) and Department of Defense (DOD) which was due to Congress on May 1, 2012 as prescribed in the joint explanatory statement accompanying the fiscal year 2012 DHS Appropriations Act (Public Law 112–74). The purpose of the report was to outline the capabilities of a coordinated response to a cyber attack by DHS and the National Guard and how critical relationships can be established across the agencies to fulfill cybersecurity responsibilities. The information provided, which was submitted separately by the two agencies, outlines on a high-level, the programs DHS and DOD (as a whole) are maintaining for a response. Unfortunately, the report falls short of providing Congress an understanding of the DHS and National Guard's capacity to respond to a cyber attack jointly. In order for Congress to better understand the gap between capacity and need, a sense of scope is required.

How many National Guard cybersecurity personnel currently exist, and where? Are they employed in teams or individually? If they are employed in teams, how many teams are there and where are they located?

As DOD and DHS are building the capacity the Federal Government needs to protect against and respond to a cyber attack: what specific role is being considered for the National Guard; and how is the Guard's ability to switch between title 32 authorities and title 10 authorities being taken into consideration?

Is there a cost savings associated with utilizing the National Guard based on current training? How much?

Are there skills identified within the National Guard that cut down the time needed to train a cyber airman or soldier to be able to respond to a cyber attack?

Answer. Successful response to dynamic cyber threats requires leveraging homeland security, law enforcement, and military authorities and capabilities, which respectively promote domestic preparedness, criminal deterrence and investigation, and national defense. DHS, the Department of Justice (DOJ), and the Department of Defense (DOD) each play a key role in responding to cybersecurity incidents that pose a risk to the United States. While each agency operates within the parameters of its authorities, the U.S. Government's response to cyber incidents of consequence is coordinated among these three agencies such that "a call to one is a call to all." Synchronization among DHS, DOJ, and DOD not only ensures that whole-of-government capabilities are brought to bear against cyber threats, but also improves the Federal Government's ability to share timely and actionable cybersecurity information among a variety of partners, including the private sector. In terms of specific National Guard activities, DHS defers to DOD.

CYBER TEST BEDS/RANGES

Question. General Alexander testified that the services, departments, and agencies need to work together to ensure that they have adequate test bed and range space to safely organize, train, and equip the cyber warriors, operators, managers, researchers, and agents across the Federal Government.

What are the specific requirements that your departments and their various agencies have for test bed and range space? What specific outcome will those established requirements render in trained personnel and tactics?

Answer. The Department has a variety of requirements for test beds and range space, which DHS uses for internal employee training exercises, broader cybersecurity training for owners and operators within each of the 16 critical infrastructure sectors, and joint cyber exercises with partners. DHS likewise has longstanding requirements for a research-focused test bed that allows for the realistic and at-scale evaluation of innovative defensive technologies.

Improving cybersecurity is a global challenge and, as a critical piece of research infrastructure, the test bed needs to be accessible to international researchers. The Experimental Research Testbed project (formerly the Cyber Defense Technology Experiment Research Testbed Program or DETER) began in 2004 as a joint effort between the DHS Science and Technology Directorate (S&T) and the National Science Foundation (NSF) to address the need to research and understand new cybersecurity risks and threats in a safe environment. This international access requires that the test bed operate without classification restrictions or technology restricted by International Traffic in Arms Regulations (ITAR). The test bed must be securely accessible over the Internet so as to not require international researchers to have to travel to the physical location of the test bed. Additionally, since DHS S&T is focused on not only operating a research test bed, but also on conducting research to advance state-of-the-art test bed technology, it is critical that the software utilized is available as Open Source. Put simply, the availability of Open Source software allows researchers to transition technology advances to additional facilities. The software used in the test bed has been transitioned to four other facilities and is in the process of being deployed internationally. Test beds at those additional facilities can be connected together through "federation" techniques and experiments spanning multiple facilities can be conducted accordingly. This federation allows for greater capacity and access to unique resources, such as the power system test bed at the University of Illinois—Urbana Champaign.

Other agencies use the Experimental Research Testbed as a platform to develop and evaluate defensive mechanisms against cyber attacks on infrastructure. For example, the Defense Advanced Research Projects Agency (DARPA) currently uses the test bed as a consolidated evaluation platform for one of its programs—a leveraging of resources that saves DARPA the time and expense of constructing individual test beds for its six participants. In return, DARPA has provided both hardware and upgrades to the Experimental Research Testbed project.

Question. What is the current test bed and range capacity available to each of your departments? What is the wait time or backlog based on the access you currently have?

Answer. Currently, the Experimental Research Testbed has more than 3,500 active users from 29 different countries and is comprised of nearly 700 PC-based nodes spread between California and Virginia. It is a shared resource capable of running hundreds of concurrent experiments. The capacity of the test bed is enhanced by state-of-the-art virtualization techniques that intelligently assign resources to different components of an experiment based upon the level of fidelity needed. This capability is under active development and is allowing the test bed's capacity to continually grow without requiring additional hardware.

For smaller scale experiments, there is generally no wait time for researchers. For larger experiments that require the dedication of a large portion of the test bed, researchers may be required to wait several days until enough resources can be dedicated. The test bed is also used as a learning environment by over 70 college and university classes per semester. Test bed access therefore can become constrained during finals when large numbers of students attempt to access it to finish assignments.

Question. Have you identified additional test bed or range space that you would like to acquire, use, or lease?

Answer. DHS S&T is collaborating with NSF to conduct a comprehensive study across the cybersecurity research landscape to determine future requirements. This study is expected to be completed in mid-fiscal year 2014 and will be used to identify what additional test bed capabilities and capacity are required.

Question. What are the fiscal years 2013 and 2014 funding levels for testing and training space?

Answer. DHS S&T will be funding the Experimental Research Testbed project at $4.8 million in fiscal year 2013, and plans to fund it at $4.8 million in fiscal year 2014.

Question. What percentage of your required testing and training needs will you be able to meet in fiscal years 2013 and 2014?

Answer. DHS S&T's Experimental Research Testbed project currently fulfills the identified test bed requirements for cybersecurity research. The capabilities and capacity of the test bed will continue to improve in order to better address advancing threats and increasingly complex research challenges.

ROLE OF THE SECRET SERVICE IN CYBER INVESTIGATIONS

Question. On March 13, 2013, Jenny A. Durkan, United States Attorney, Western District of Washington, testified before the House of Representatives Committee on Judiciary, Subcommittee on Crime, Terrorism, Homeland Security, and Investigations, discussing "Investigating and Prosecuting 21st Century Cyber Threats." In her testimony she highlighted eight significant cyber investigations, four of which were Secret Service cases, a component of DHS.

We hear much about DHS's role in the securing of cyber space; what is DHS's role in investigating cyber crimes targeting our financial infrastructure?

Answer. DHS's law enforcement components are essential to securing the Nation from cyber criminals and cyber attacks. Investigating, arresting, and supporting the successful prosecution of criminal cyber actors is a critical element of the Department's strategy to safeguard and secure cyberspace. Effective investigations identify and lead to the arrest of the individuals and groups behind cyber attacks and otherwise disrupt the criminals responsible for such attacks. During the course of their investigations, DHS law enforcement components also develop criminal intelligence that can provide public and private sector entities with the knowledge and tools necessary to detect and disrupt future attacks.

Industry representatives such as Symantec estimate that cyber crime costs the U.S. taxpayer more than $110 billion annually.[1] While public discourse tends to center on the potential for national-level cyber attacks, cyber crime in the aggregate does serious damage to our Nation every day, and fighting cyber crime is an important part of keeping our Nation safe and our economy strong. DHS, through the investigative authority of the U.S. Secret Service, is focused on protecting the Nation's financial system from exploitation by cyber criminals. The U.S. Secret Service has adapted its investigative techniques over the years to address the emerging trends of cyber criminals. For example, since passage of the Comprehensive Crime Control Act of 1984, the U.S. Secret Service has arrested over 30,644 individuals for cybercrime violations with an attributed fraud loss of over $2.7 billion and potential fraud loss of over $33 billion.

In 2001, Congress likewise recognized the U.S. Secret Service for its expertise in preventing, detecting, and investigating potential attacks against critical infrastructure and financial payment systems and directed the agency to develop a national network of Electronic Crimes Task Forces based on the successful model of the New York Electronic Crimes Task Force. Today, the U.S. Secret Service operates 31 domestic and international Electronic Crimes Task Forces that merge the skills and knowledge of representatives from Federal, State, local, private industry, and academic partners in furtherance of protecting the Nation's critical infrastructure and financial payment systems from cyber crime. In fiscal year 2012, the U.S. Secret Service arrested 1,378 individuals for cyber crime violations responsible for over $355 million in fraud losses and over $1.2 billion in potential losses. These inves-

[1] Norton 2012 Cybercrime Report: http://www.norton.com/2012cybercrimereport Ponemon Cost of Cybercrime (if extrapolated): http://www8.hp.com/us/en/hp-news/press-release.html?id=1303754

tigations culminated with the Department of Justice attaining a 99.6-percent conviction rate for these cases.

We also work with a variety of international partners to combat cybercrime. For example, through the U.S.-EU Working Group on Cybersecurity and Cybercrime, which was established in 2010, we develop collaborative approaches to a wide range of cybersecurity and cybercrime issues. In 2011, DHS participated in the Cyber Atlantic tabletop exercise, a U.S.-EU effort to enhance international collaboration of incident management and response, and in 2012, DHS and the EU signed a joint statement that advances transatlantic efforts to enhance online safety for children. U.S. Immigration and Customs Enforcement (ICE) also works with international partners to seize and destroy counterfeit goods and disrupt Web sites that sell these goods. Since 2010, ICE and its partners have seized over 2,000 domain names associated with businesses selling counterfeit goods over the Internet. To further these efforts, the administration issued its Strategy on Mitigating the Theft of U.S. Trade Secrets last month. DHS will act vigorously to support the Strategy's efforts to combat the theft of U.S. trade secrets—especially in cases where trade secrets are targeted through illicit cyber activity by criminal hackers.

In addition, since opening in May of 2008, the National Computer Forensics Institute (NCFI) has held over 90 Cyber and Digital Forensics courses in 13 separate subjects. The NCFI has trained more than 2,000 State and local investigators, prosecutors, and judges. This institution serves as the Nation's only center dedicated to instructing State and local law enforcement in digital forensics and equips graduates to conduct network intrusion and electronic crimes investigations. Several hundred prosecutors and judges, as well as representatives from the private sector, have also received training on the impact of network intrusion incident response, electronic crimes investigations, and computer forensics examinations.

DHS is committed to working with its partners across government and the private sector to protect the Nation's critical financial infrastructure from cyber attack. To achieve this goal, DHS will bring to bear the tremendous investigative resources of its law enforcement components against those who attempt to do us harm.

Question. Would you characterize the recent $45 million ATM scheme, investigated by the Secret Service among others, as representative of a trend in global cybercrime?

Answer. The facts relayed in the recently unsealed indictments against eight of the individuals involved in the theft of over $45 million from various ATMs in New York City are an example of the highly sophisticated, organized, transnational cyber-criminal activity impacting the Nation's financial system. This case is just one example of a number of recently "unlimited cash-out" operations conducted in a highly coordinated fashion by transnational networks of cyber criminals.

The ATM case demonstrates, as numerous cybersecurity experts have confirmed in testimony before congressional committees, that the majority of network intrusions are carried out by criminal actors whose sole motivation is financial gain. The suspects distributed the stolen data to organized crews of street criminals in more than 20 countries who then encoded the information on magnetic-stripe plastic cards. While this particular case was conducted by a transnational network of highly technical hackers, other U.S. Secret Service investigations have demonstrated that many financial intrusions are successfully executed against networks because of weak or stolen credentials. DHS is committed to not only reducing this threat through effective investigations, but also working with financial institutions through the Financial Services Information Sharing and Analysis Center to help them better secure their computer systems.

Question. What additional resources might be needed by the investigative arms of DHS to properly combat this type of fraud?

Answer. Investigating cybercrime requires highly trained and experienced criminal investigators. ICE and the U.S. Secret Service are expanding participation in the existing Electronic Crimes Task Forces (ECTF), which will strengthen the Department's cybercrimes investigative capabilities and realize efficiencies in the procurement of computer forensic hardware, software licensing, and training. The U.S. Secret Service-led ECTF model has been in existence for over 20 years. Hiring and training additional law enforcement investigators in the U.S. Secret Service would enhance the Department's capacity to respond to and investigate cybercrime directed at the Nation's financial infrastructure. Additional resources would also allow DHS to increase the capacity of the Secret Service's network of ECTFs and further develop its international cyber investigative working groups to respond to transnational threats to critical infrastructure.

Improving cybersecurity requires public-private partnerships, and the vast scope of cybercrime directed at the United States means that our partners at the State, local, and tribal governmental levels are vital to the national effort. In order to develop State and local capacity to investigate cybercrimes, the U.S. Secret Service operates the NCFI in Hoover, Alabama. This facility is the Nation's only federally funded training center dedicated to instructing State and local law enforcement officials about the complexities associated with cybercrime investigations. The NCFI is capable of training over 2,000 State and local police investigators, prosecutors and judges in cybercrime investigations every year. Since 2008, the NCFI has been funded annually at $4 million. The current level of funding, for example, allowed NCFI to train and equip over 600 police investigators, prosecutors and judges in 2012. These officials have come from all 50 States and three U.S. territories.

Cyber criminals often operate outside the borders of the United States, and related investigations accordingly require extensive cooperation with international law enforcement agencies. Additionally, law enforcement agencies have long recognized that the most critical capability for transnational organized crime is to quickly and quietly move large quantities of money across borders. The anonymity of cyberspace affords a unique opportunity for criminal organizations to launder huge sums of money undetected. The cyber crime investigations of the U.S. Secret Service depend heavily on developing and maintaining effective international law enforcement partnerships. The Department of State and the Department of Justice are critical partners in developing these international relationships and in the execution of international law enforcement action through multilateral assistance treaties. Funding to support the international investigations of DHS law enforcement components, training for its international law enforcement foreign partners, and associated investigative travel costs would enhance DHS's investigative capabilities.

Question. What will be the impact of the dismantling of Liberty Reserve and their digital currency system by the Secret Service, its Electronic Crimes Task Forces, Immigration and Custom Enforcement investigators, and the IRS on illegal cyber money laundering operations?

Answer. Over the course of its 7-year existence, Liberty Reserve emerged as the principal means by which cyber criminals around the world distributed, stored, and laundered the proceeds of illegal activity. Liberty Reserve facilitated a broad range of online criminal activity, including narcotics trafficking, child pornography, computer hacking, investment fraud, credit card fraud, and identity theft. Annually, Liberty Reserve processed more than 12 million financial transactions with a combined value of $1.4 billion. Since its founding in 2006, Liberty Reserve processed an estimated 55 million separate financial transactions and is believed to have laundered more than $6 billion in criminal proceeds.

The dismantling of Liberty Reserve by the U.S. Secret Service and its partners in the Global Illicit Financial Team—IRS-CI and ICE-Homeland Security Investigations (HSI)—significantly impacted the cyber criminal community, forcing cyber criminals to seek alternative means to fund their illicit activities.

ROLE OF DHS IN CAPABILITY BUILDING FOR LAW ENFORCEMENT CYBER INVESTIGATIONS

Question. We are seeing more examples of cyber threats being encountered and responded to by State and local law enforcement officials. In many instances, however, these officials do not have the appropriate type of training to fully understand what they are investigating may go beyond the incident they have encountered.

Is DHS involved in developing the cyber law enforcement capabilities of State, local, and tribal entities for investigating these types of cyber crimes?

Is this an appropriate role for DHS agencies to fulfill?

Answer. DHS has a well-established role in developing and supporting State, local, tribal, and territorial (SLTT) capabilities. Included are the efforts of numerous components to develop SLTT capabilities and operational relationships to effectively investigate cyber crime. For example, the first U.S. Secret Service ECTF that was established in 1995 boosted cyber law enforcement capabilities in coordination with State and local authorities. Since 2001, when Congress directed that a nationwide network of ECTFs be established, the U.S. Secret Service has worked in partnership with SLTT authorities, the private sector, and academia to develop cyber capabilities for the common purpose of preventing, detecting, and investigating various forms of electronic crimes, including potential terrorist attacks against critical infrastructure and financial payment systems.

In partnership with the State of Alabama, the Secret Service established the NCFI in Hoover, Alabama, for the purposes of training SLTT law enforcement officials on cyber law enforcement methods and techniques. Since opening in 2008, the NCFI has trained over 2,000 State and police investigators, prosecutors, and judges in cybercrime investigations. These officials have come from all 50 States and three U.S. territories. The investigators trained by the NCFI are nominated by local Secret Service field offices where they can apply their skills as members of the ECTFs.

When it opened in 2008, the NCFI offered instruction in one of five cyber investigation curriculums. As of 2013, the NCFI offers 13 separate curriculums designed to address developing cyber trends. For example, the NCFI worked last year with DHS to develop cyber analytical training for State and local law enforcement members staffing the cyber intelligence fusion centers throughout the Nation. An intra-agency agreement between the Federal Emergency Management Agency and the Secret Service will allow the NCFI to fund three more cyber analyst courses for fusion center members this year. Additionally, in August 2012, the NCFI partnered with the Federal Bureau of Investigation to conduct two NCFI training courses to State and local law enforcement officials assigned to the FBI's National Domestic Communications Assistance Centers. Currently, the NCFI operates at 25 percent of its capacity on a $4 million annual budget. Additionally, the NCFI through its curriculum established a national standard of training in cybercrime investigations, network intrusion response, computer forensics, and electronic crime prosecution.

ICE-HSI has a workforce that is well-trained to deal with cybercrime. HSI has several hundred special agents that routinely deal with cyber crime, and we operate ICE's Cyber Crime Center, or C3, and routinely provide investigative expertise and assistance to State, local, and tribal entities when consulted for assistance concerning transnational cyber crime. These efforts are an appropriate role for HSI to fill and to ensure that transnational criminal organizations are fully identified and dismantled via successful prosecutions.

Questions Submitted by Senator Tom Udall

ROLE OF NATIONAL LABORATORIES IN PROMOTING CYBERSECURITY

Question. Secretary Beers, our National Labs—which are the crown jewels of our Nation's research system—are active in efforts to promote cybersecurity.

In my home State of New Mexico, Sandia National Laboratories is engaged in efforts to secure the national electrical grid from cyber attack. Los Alamos National Laboratories is a leader in quantum cryptography.

Sandia also has partnerships with universities and the private sector. They're helping computer science students become cyber professionals.

Could you discuss what role our National Labs should have in protecting our Nation from cyber attack?

Answer. The National Labs are essential for providing enduring and multi-disciplinary research and development capabilities to help solve complex national security problems, including cyber-related problems. Among other things, the Labs provide unique facilities and infrastructure in support of talented subject matter experts who work to develop technologies and other solutions that help the Nation protect against and recover from cyber attacks. The S&T Cyber Security Division (CSD) has had great success in working with the Labs on several key cybersecurity initiatives. For example:

—S&T CSD has frequently worked with Sandia National Labs to red-team developed cybersecurity solutions.

—The Pacific Northwest and Oak Ridge National Labs currently serve as principal investigator researchers for a number of S&T CSD's research and development contracts.

—The S&T CSD Transition to Practice Program is currently working with multiple National Labs (Sandia, Los Alamos, Lawrence Livermore, Oak Ridge, and Pacific Northwest) to transition numerous developed cybersecurity technologies into the government and private sectors.

NPPD also works with DHS S&T to ensure that cybersecurity research and development efforts are fully coordinated with ongoing programmatic requirements. With Pacific Northwest and Sandia National Labs, the Deputy Assistant Secretary for Cybersecurity Coordination participates in external review boards to review and shape research conducted at these Labs and to gain insight into research areas that may meet NPPD and S&T requirements in cybersecurity. S&T and the Homeland Security Enterprise should continue to leverage the strengths of the National Labs in cybersecurity to help respond to and mitigate the threats from cyber attacks.

In addition, the National Labs provide advanced modeling, simulation and analysis, and cyber training. This includes work with the National Infrastructure Simulation and Analysis Center, a joint partnership with Sandia and Los Alamos to identify and address potential impacts to the sectors from possible cyber-related incidents and consequence analysis with the DHS NPPD Homeland Infrastructure Threat and Risk Analysis Center (HITRAC). HITRAC also works on ascertaining impacts from cyber manipulation of industrial control systems including leveraging the expertise of Idaho National Labs as a partner. This analysis can inform partners, policymakers, and homeland security professionals about the potential consequences of a cyber-related incident and sector resilience to such events.

MOBILE PHONES AND CYBERSECURITY AWARENESS

Question. Secretary Beers, this year, there will be more mobile phones than people on the planet. Today, our wireless devices are not just phones, but pocket computers. We use them for sensitive transactions, including mobile banking and online purchases.

But GAO recently found that cyber threats are increasing for mobile devices and the information they store. GAO recommended that DHS and NIST work together to "establish a baseline measure of consumer awareness . . . related to mobile security." GAO also recommends the development of performance measures that use the baseline to assess the effectiveness of initiatives to educate the public about cybersecurity.

Could you share any thoughts on how best to raise public awareness for cyber security threats to mobile devices?

Answer. Public awareness is best developed in partnership with the mobile device communications service providers, which have a financial interest in the quality of their service. Part of that quality of service would include ensuring proper protection of their customers' mobile devices. Increased awareness and the capabilities sought can be developed through thoughtful engagement with standing advisory groups such as the National Security Telecommunications Advisory Committee.

Part of the engagement might focus on consumer and supplier adoption of the update practices similar to those used to protect desktop systems. Anti-malware protection and timely updates of applications and operating systems is just as important for mobile devices (phones and tablets) as for desktop computers. The same is true for other networked devices like multifunction printers that themselves host sophisticated operating systems and applications.

Mobile banking and third-party payment systems continue to increase in popularity due to the efficiencies they provide to the consumer and financial institutions. This has resulted in cybersecurity challenges that merit attention. As part of DHS's responsibilities to secure key conveyances in the global economy and the U.S. Secret Service's role to protect the financial system from criminal exploitation, the Department works closely with its partners across government and in the private sector to not only raise awareness of these risks, but establish effective ways to mitigate these growing risks. Recently the Federal Deposit Insurance Corporation (FDIC) published information about the current landscape of mobile banking. As a starting point for financial institutions seeking to adopt mobile banking services, the FDIC references risk management strategies outlined in the Federal Financial Institutions Examination Council IT Examination Handbook. That handbook, however, does not discuss mobile devices specifically. The FDIC's statements instead relate to mobile banking and not necessarily mobile payment systems.

While there accordingly may be some good cybersecurity work being done on the mobile banking side, the consumer likely does not make a distinction and may assume the same level of cybersecurity attaches whether they use mobile banking or mobile payment systems. For example, most users connect their mobile payment systems, such as PayPal, directly to their checking accounts or other bank accounts. Disparate levels of cybersecurity between the two could result in a systemic security risk, where a compromise to one (mobile payment systems) has the potential for causing loss in both. In essence, both become a single system with shared, lowest-denominator, vulnerability. More broadly, current third-party application security is primarily based on device/operating system policies regarding application signing and privileges. Unfortunately, the devices must rely on transmission protocols (like SMS) that were not designed with security in mind. For example, the U.S. Secret Service Cell Phone Forensic Facility at the University of Tulsa is working to show how SMS payment systems can be attacked using simple and widely available wireless devices. Further research is needed to assess all attack vectors to determine what further mitigation is necessary.

The Federal Government can raise public awareness about mobile device cyber risk by continuing to support fundamental research to identify vulnerabilities and to develop effective mitigation and protection measures. Both the U.S. Secret Service's Cell Phone Forensics Facility at the University of Tulsa and its ongoing partnership with Carnegie Mellon CERT serve as outstanding examples of how the Federal Government can effectively partner with academia for this purpose. S&T has launched a research program to improve the security of mobile devices and enable better detection of malicious applications. These research efforts not only serve to raise awareness of these sorts of vulnerabilities, but also to develop effective mitigation and protection measures.

Question. What is the proper role for government and industry to promote best practices for both companies and consumers?

Answer. Government and industry are well positioned to collaboratively promote best practices for companies and consumers. Government can measure awareness across a large consumer base and use this baseline measure to further assess its performance as it employs public cybersecurity awareness initiatives, such as the Stop.Think.Connect.™ campaign. In addition, as the developer, producer, and consumer of mobile device products, industry has an invaluable sense of which security practices are effective. Government can convene and organize collaborative processes that ensure the best practices from within Government and from across industry are brought together and made available to wide range of consumers, both technical and nontechnical. Where appropriate, Government can build these best practices into its outreach and awareness efforts.

Among its activities, DHS provides and promotes a trusted environment for exchange of information between industry mobile device communications service providers, manufacturers, and Government in order to identify and develop consensus on best practices in mitigating the ongoing emerging cyber threats being deployed to exploit privacy of their mobile devices. The best practices are pushed to the public through industry partners and Government outreach.

Currently, DHS promotes cybersecurity and resilience via enhanced processes and diagnostics in partnership with industry and academia. DHS enables public-private collaboration focused on reducing exploitable software weaknesses and addressing means to improve capabilities that routinely develop, acquire, and deploy resilient information technology (IT) products. Among its activities, DHS:

—Enables partners and citizens to secure their part of cyberspace by providing public-private collaboration in advancing security and resilience of IT throughout the lifecycle;

—Focuses on reducing exploitable weaknesses and addressing means to improve capabilities that routinely develop, acquire, and deploy resilient products;

—Enables security automation and measurement through the use of common indexing, reporting and scoring capabilities for malware, exploitable software weaknesses, counterfeit and tainted hardware, and common attacks on IT assets.

Questions Submitted by Senator Thad Cochran

Question. All witnesses, we have heard about the importance of cooperation and clearly defined lanes responsibility across the Federal Government for our cybersecurity efforts. What are your respective roles in receiving and sharing threat information with the private sector?

Answer. The success of DHS's cyber mission relies heavily on the response to dynamic cyber threats through the leveraging of homeland security, law enforcement, and military authorities and capabilities, which respectively promote domestic preparedness, criminal deterrence and investigation, and national defense. DHS, the Department of Justice (DOJ), and the Department of Defense (DOD) each play a key role in responding to cybersecurity incidents that pose a risk to the United States. While each agency operates within the parameters of its authorities, the Federal Government's response to cyber incidents of consequence is coordinated among these three agencies such that "a call to one is a call to all." Synchronization among DHS, DOJ, and DOD not only ensures that whole-of-government capabilities are brought to bear against cyber threats, but also improves the Federal Government's ability to share timely and actionable cybersecurity information among a variety of partners, including the private sector.

For its part, the DHS cyber mission relies on its ability to establish shared situational awareness of potentially harmful activity, events, or incidents across multiple constituencies to improve the ability of diverse and distributed partners to protect themselves. To do this, the DHS National Cybersecurity and Communications Integration Center (NCCIC) incorporates information and data received through its own analysis, Intelligence Community, and law enforcement reporting, along with data shared by private sector and international partners into a comprehensive series of actionable information products, which are shared with partners in easy to digest machine-readable formats.

Multidirectional sharing of alerts, warnings, analysis products, and mitigation recommendations among Federal, State, local, tribal, and territorial governments, private sector, information sharing and analysis centers, and international partners is a key element of the NCCIC's cyber and communications protection and prevention framework. The NCCIC continuously works with a broad range of partners to explore and innovate new ways to enhance information sharing and move closer to network speed communications.

In order to meet DHS's public-private cybersecurity data sharing and analytical collaboration mission, the Department has developed a critical infrastructure Cyber Information Sharing and Collaboration Program (CISCP) and the Enhanced Cybersecurity Services (ECS) program. The CISCP program mission is to improve the defensive posture of DHS's critical infrastructure partners by:

—Sharing a view of current threats and vulnerabilities affecting both critical infrastructure and Federal Government sources among Federal Government and industry cybersecurity analysts.

—Aligning those analysts in collaborative engagements regarding cyber threat detection, prevention, mitigation, and response efforts to reduce risks to critical infrastructure information technology and communications networks, systems, and data.

The goal of the CISCP program is an effective information sharing framework among the Federal Government, Information Sharing and Analysis Centers and related organizations, information and communications technology service providers, and their respective critical infrastructure owner/operator members and customers.

Within the CISCP program, Federal Government and industry partners contribute threat data, adding to the volume of information currently available for analysis by the DHS CISCP analytical team. Because the act of providing threat or attack data may harm competitive or other commercial interests of DHS's industry partners, significant steps are taken by the CISCP Team to both conceal the source of data provided and to protect Protected Critical Infrastructure Information (PCII). First, all data is anonymized so that analysis of submitted data is not carried out or based upon the identity of the submitter absent their express authorization. The CISCP program data is governed using the Traffic Light Protocol (TLP), which is a set of designations used to ensure that sensitive information is shared with the correct audience. It employs four data-sharing categories (red, amber, green, and white) to indicate different degrees of sensitivity and the corresponding sharing considerations to be applied by the recipients. Regular analyst-to-analyst technical threat exchanges (both classified and unclassified) involving Federal Government and industry partners are likewise held to share details of cyber threat activity and mitigation recommendations. To join CISCP, stakeholders sign a Collaborative Research and Development Agreement that provides them with opportunities to establish physical access to DHS's NCCIC watch floor and to receive clearances up to the TS/SCI level.

In addition to the CISCP program, DHS actively collaborates with public and private sector partners every day through the ECS program to respond to and coordinate mitigation efforts against attempted disruptions and adverse impacts to the Nation's critical cyber and communications networks and infrastructure. Expanded in February 2013 by EO 13636, the ECS program coordinates the protection, prevention, mitigation, and recovery from cyber incidents through information sharing initiatives with business owners and operators to strengthen their facilities and communities. ECS is a voluntary information sharing program that assists critical infrastructure owners and operators as they improve the protection of their systems from unauthorized access, exploitation, or data exfiltration. ECS augments, but does not replace, an entity's existing cybersecurity capabilities; rather it responds to high level malware threats that DHS, working with other experts, has determined pose the greatest threat to critical infrastructure.

DHS works with cybersecurity organizations from across the Federal Government to gain access to a broad range of sensitive and classified cyber threat information, and in responding to major cyber incidents also comes into possession of such information. It would ordinarily be difficult to share classified and sensitive information about high-level cyber threats with a broad range of private sector partners. Doing so could jeopardize intelligence sources and methods as well as law enforcement investigations. It likewise could undercut private sector partners who provide DHS with threat information under the categorical exclusion (confidentiality assurance) provided available under the PCII authorities.

DHS develops indicators based on threat information and shares it with a relatively small number of qualified CSPs, thus enabling them to better protect their customers who are critical infrastructure entities. In addition, the ECS program does not involve Government monitoring of private networks or communications; any monitoring is strictly voluntary, and solely occurs between the CSP and the protected critical infrastructure entity. Collection of communications content, and for that matter metadata, is not directed, or permitted under the ECS program. The information returned to the Federal Government by the CSPs is limited to anonymized, aggregated information about the threats detected, and the critical infrastructure sectors at which the threats were directed. Any information shared by a CSP customer is done so voluntarily, in an anonymized fashion, and for a limited tenure. CSPs or critical infrastructure entities may choose to be involved with the Federal Government in other ways—for instance reporting a cybercrime or seeking technical assistance in case of a major cyber incident—but such involvement is not related to the conduct of the ECS program and occurs independently of it.

The U.S. Secret Service also shares information that it derives through its cyber crime investigations, primarily through its 31 Electronic Crimes Task Forces (ECTF). The ECTFs hold quarterly meetings to share information with the U.S. Secret Service's public and private sector partners, in addition to providing a conduit for sharing information with organizations facing specific cyber risks. In addition to ECTFs, the U.S. Secret Service and U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) support research efforts that provide extensive and detailed data on cyber crime trends. These reports include the Verizon Data Breach Investigations Report, the Trust Wave Global Security Report, and the U.S. Secret Service Computer Emergency Response Team's (USSS–CERT) Insider Threat Report. In addition to these annual research reports, the U.S. Secret Service regularly sends special agents trained through the agency's Electronic Crimes Special Agent Program to speak at cybersecurity and law enforcement conferences. The agents provide information to improve awareness of cybercrime methods and trends.

Question. All witnesses, I think we all recognize the importance of defending our Nation's critical infrastructure against cyber attacks. A foreign or terrorist cyber attack on our electric grid, water systems, or financial systems could cause widespread damage and even have detrimental effects on our economy and consumer confidence. There has been much discussion about how involved the Federal Government should be in defending infrastructure owned by non-Federal entities. How would you define the threshold for what types of non-Federal infrastructure might qualify as "critical" for these purposes?

Answer. The term "critical infrastructure" is defined in section 1016(e) of the USA Patriot Act of 2001 (42 U.S.C. 5195c(e)), namely systems and assets, whether 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 or safety, or any combination of those matters. This definition is used to determine which infrastructure, whether it is owned by a Federal entity or not, qualifies as critical.

Question. Deputy Secretary Beers, I recognize the important role that cyber research and development plays in ensuring we maintain a technological edge against those who wish to harm our Nation's civilian computer systems. I note that your department requested fiscal year 2014 funding for such initiatives, including experimental research testbed projects. Your Department is still a relatively young one and you don't have the robust laboratory network that other Departments have. How are you collaborating with other Departments such as Defense and Energy to advance important research in cybersecurity and existing University capabilities? What are some of the technological challenges that we face?

Answer. DHS S&T conducts large parts of its cybersecurity research and development (R&D) program in collaboration with other organizations across the Federal Government. For example, the S&T Cyber Security Division (CSD) is an active part of the National Information Technology Research & Development organization (NITRD), which coordinates R&D planning across the Federal Government, chartered through the President's National Science & Technology Council and the Office of Science and Technology Policy. NITRD developed a National Cybersecurity R&D Plan, published in December 2011, and has carried forward and sustained this collaborative planning. CSD also leads the working group effort developing the National R&D Plan for Critical Infrastructure Security & Resiliency, which is a tasking from the EO 13636/PPD–21 guidance published this past February.

CSD's collaboration with other Federal agencies and organizations extends into specific R&D program efforts, including but not limited to the following:

—DHS S&T and the Department of Defense (DOD) collaborate in their Small Business Innovation Research (SBIR) program efforts, including a combined annual review.

—Department of Energy (DOE) Laboratories are conducting several elements of the DHS S&T Cyber Security research program.

—DHS S&T has accepted several research projects transitioned from the Defense Advanced Research Projects Agency

—The DHS S&T Trustworthy Cyber Infrastructure for the Power Grid program is conducted in partnership with DOE.

The DHS S&T Transition to Practice program is drawing promising cybersecurity technologies from the DOE National Laboratories to support its final development and transition into operational capability and use.

The December 2011 NITRD report, "Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program," describes in detail the technological challenges that DHS faces. Those challenges fall into four overall areas:

—Advancing a balance of both long-term science and near-term engineering improvements;

—Understanding and addressing the interconnections of technological and human systems;

—Understanding cyber complexity and addressing major risks and increasing resilience;

—Transitioning capabilities and improvements into operational use.

In 2000, the U.S. Secret Service instituted the USSS–CERT liaison program in partnership with Carnegie-Mellon University's Software Engineering Institute (SEI) in Pittsburgh, Pennsylvania—a federally funded research and development center (FFRDC) sponsored by the DOD. The USSS–CERT program sponsors the development and implementation of innovative, cost-effective solutions to meet emerging cyber threats across the full spectrum of operations. The Federal Government, through its collaborative model with the CMU–SEI, and the FFRDC, realizes significant cost savings by leveraging participating agencies' resources to accomplish shared objectives with the cost-effective benefits. The U.S. Secret Service's partnership and presence at SEI represents the U.S. Secret Service's long-standing commitment to developing mission critical systems; cybercrime applications; and malware analysis and applications that identify, assess, and mitigate threats to the Nation's financial systems, critical infrastructure, and persons and facilities protected by the U.S. Secret Service.

Question. All witnesses, we've often heard that there is a potential for a "Cyber Pearl Harbor," or an unexpected cyber attack on our Nation by a foreign entity that has dramatic and lengthy consequences. I think it may be difficult for most Americans, and even members of this Committee, to visualize how exactly such an attack would be carried out and what it would look like. Can you help us to better understand these things? Are the appropriations this Committee has been recommending sufficient to help prevent such an attack?

Answer. The Department currently sees malicious cyber activity attacks against critical infrastructure from foreign nations and nonstate actors. Their methods range from distributed denial of service attacks and social engineering to viruses and other malware introduced through remote access, thumb drives, supply chain exploitation, and leveraging trusted insiders' access. These attacks are becoming more frequent and more sophisticated, putting at risk the Nation's critical infrastructure, which underpins the economy, provides the public with basic day to day needs, and ensures the Nation's basic security and well-being. Ultimately, a significant cyber incident may come in many forms and the vulnerabilities that have yet to be identified may be the most important. Because of this increasing risk, DHS is working alongside interagency, private sector, and international partners to enhance resilience, harden systems, and prepare for a variety of national response scenarios.

We thank the Committee for its ongoing support for the Department's cybersecurity activities. However, DHS cybersecurity programs have been impacted by sequestration. For example, funding has been reduced for operations and maintenance and analytical contracts supporting the National Cybersecurity Protection System (NCPS). While this will not affect when NCPS E^3A will reach initial operating capability, full operating capability will be delayed beyond fiscal year 2015 if sequestration continues. Funding has also been reduced for licensing and installing sensors for continuous monitoring at Federal agencies and some features of the Federal dashboard will be delayed until fiscal year 2014. Finally, funding for other cybersecurity activities, such as the U.S. Computer Emergency Readiness Team, funding for the Software Engineering Institute, the GFIRST Conference, updates to the Cyber Security Evaluations Tool, and the number of onsite risk assessments to the Transportation sector have been impacted by sequestration.

QUESTIONS SUBMITTED TO HON. DR. PATRICK GALLAGHER, ACTING DEPUTY SECRETARY, DEPARTMENT OF COMMERCE DIRECTOR, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

QUESTIONS SUBMITTED BY SENATOR PATTY MURRAY

Question. The electricity subsector is already subject to mandatory and enforceable cybersecurity standards. As NIST works to comply with the Executive order on cybersecurity, how is NIST working to ensure the Framework will include these existing standards?

Answer. [A response was not provided by press time.]

Question. Understanding that cyber threats are constantly evolving and that owners and operators of critical infrastructure have to make decisions just like the Federal Government on what needs to be secured, how is NIST including risk management practices within the Framework activities?

Answer. [A response was not provided by press time.]

QUESTIONS SUBMITTED BY SENATOR RICHARD J. DURBIN

CYBER EXECUTIVE ORDER—ROLE OF THE EXECUTIVE ORDER VERSUS CYBER LEGISLATION

Question. President Obama issued Executive Order 13636 in February of this year. What is the effect of this Executive order? Is it improving your ability to share information with the private sector?

Answer. The Executive order directs the National Institute of Standards and Technology (NIST) to lead the development of a framework to reduce cyber risks to critical infrastructure. The framework is intended to be used on a voluntary basis throughout an entire organization—including by the most senior executives who oversee an organization to the officials and staff responsible for managing information technology-based resources. It is designed specifically for companies and other entities that are part of the critical infrastructure, especially owners and operators of critical infrastructure, to identify, assess, and manage cyber risk. However, other organizations—large and small and with varying business needs—will benefit by reducing risks and protecting their assets and mission-driven work by using the framework.

When he signed the Executive order, President Obama also underscored the need for comprehensive cybersecurity legislation, since the scope of the Executive order is limited. What are your legislative priorities in terms of items you believe should be included in cyber legislation?

We'd like to hear from all the witnesses on this issue.

Answer. The administration's legislative priorities for the 113th Congress build upon the President's 2011 Cybersecurity Legislative Proposal and take into account 2 years of public and congressional discourse about how best to improve the Nation's cybersecurity.

The administration is working toward legislation that:

—Facilitates cybersecurity information sharing between the government and the private sector as well as among private sector companies. We believe that such sharing can occur in ways that protect privacy, confidentiality, and civil liberties, reinforce the appropriate roles of civilian and intelligence agencies, and include targeted liability protections.

—Incentivizes the adoption of best practices and standards for critical infrastructure by complementing the process set forth under the Executive order;

—Gives law enforcement the tools to fight crime in the digital age while protecting privacy, confidentiality, and civil liberties;

—Updates Federal agency network security laws, and codifies DHS' cybersecurity responsibilities; and

—Creates a National Data Breach Reporting requirement.

In each of these legislative areas, the right privacy, confidentiality, and civil liberties safeguards must be incorporated. The administration wants to continue the dialogue with the Congress and stands ready to work with members of Congress to incorporate our core priorities to produce cybersecurity information sharing legislation that addresses these critical issues.

CYBER EXECUTIVE ORDER—PROTECTING PRIVACY AND CIVIL LIBERTIES

Question. The Executive order requires Federal agencies to develop cybersecurity efforts in accordance with the Fair Information Practice Principles, as well as other policies, principles, and frameworks to protect privacy and civil liberties. I worked with a number of other Senators to ensure that the Cybersecurity Act of 2012 included provisions to protect privacy and civil liberties.

What specific steps can government agencies take to ensure that privacy and civil liberties are protected as we enhance our Nation's cybersecurity?

Answer. In April 2013, NIST published the Security and Privacy Controls for Federal Information Systems and Organizations, Special Publication (SP) 800–53, Revision 4. Appendix J provides a structured set of privacy controls, based on best practices that help organizations comply with applicable Federal laws, Executive orders, directives, instructions, regulations, policies, standards, guidance, and organization-specific issuances. The privacy controls are based on the Fair Information Practice Principles (FIPPs) embodied in the Privacy Act of 1974, section 208 of the E-Government Act of 2002, and Office of Management and Budget (OMB) policies. There are eight privacy control families, each aligning with one of the FIPPs. They provide steps government agencies can take to ensure that privacy protected as we enhance our Nation's cybersecurity.

However, unlike the longstanding framework for evaluating privacy impacts under the FIPPs, there exists no similar, corresponding framework that supports general evaluations of the potential broad range of impacts that might occur within the collection of individual rights described as "civil liberties." Policies typically focus on the protection of individual rights, and civil liberties issues arise within government frameworks (or specific programs implementing those frameworks) where implementation of the framework fails to account for those rights. Consequently, in addition to the specific NIST guidance described above, the Department of Homeland Security has established an interagency Assessments Working Group, consisting of representatives of the privacy and civil liberties officials of agencies involved in implementing the Executive order. The purpose of this group is to provide a forum for assisting agencies in meeting their responsibilities under the Executive order, including identifying cybersecurity activities and how to apply both the Fair Information Practice Principles and other applicable policies, principles and frameworks that provide privacy and civil liberties protections in these activities. Due to the highly divergent nature of critical infrastructure entities (including State and local government, private sector, quasi-governmental) the exact bundle of rights which are applicable in any given workplace will be highly variable; we recognize this challenge. The Department of Commerce is an active participant in this Working Group.

As we noted above, the administration also supports legislation that would facilitate cybersecurity information sharing between the government and the private sector as well as among private sector companies. We believe that such sharing can—and must—occur in ways that protect privacy, confidentiality, and civil liberties, reinforce the appropriate roles of civilian and intelligence agencies, and include targeted liability protections.

QUESTIONS SUBMITTED BY SENATOR TOM UDALL

ROLE OF NATIONAL LABORATORIES IN PROMOTING CYBERSECURITY

Question. Dr. Gallagher, our National Labs—which are the crown jewels of our Nation's research system—are active in efforts to promote cybersecurity.

In my home State of New Mexico, Sandia National Laboratories is engaged in efforts to secure the national electrical grid from cyber attack. Los Alamos National Laboratories is a leader in quantum cryptography.

Sandia also has partnerships with universities and the private sector. They're helping computer science students become cyber professionals.

Could you discuss what role our National Labs should have in protecting our Nation from cyber attack?

Answer. NIST recognizes the value of Department of Energy's National Laboratories cutting-edge research in addressing national priorities including cybersecurity. The results from the laboratories cybersecurity research are instrumental in the development of next generation standards and best practices. Currently, we are working with Department of Energy's Laboratories on critical cybersecurity challenges such as security for the advanced metering infrastructure.

ENGAGEMENT WITH INDUSTRY GROUPS

Question. Dr. Gallagher, I would like to ask about NIST's work with industry partners. When it comes to developing guidelines and standards for cybersecurity, is NIST getting the level of cooperation it needs from industry stakeholders? Are there areas where more engagement is needed?

Answer. NIST employs collaborative partnerships with our customers and stakeholders in industry, government, academia, and consortia to leverage their technical and operational insights and the resources of a global community. These collaborative efforts and our private sector collaborations in particular, are constantly expanding through new initiatives, including in recent years through the National Initiative for Cybersecurity Education (NICE), National Strategy for Trusted Identities in Cyberspace (NSTIC), the National Cybersecurity Center of Excellence (NCCoE), and in implementation of Executive Order 13636, "Improving Critical Infrastructure Cybersecurity."

FEDERAL CYBERSECURITY STANDARDS AND NEW COMPUTING TRENDS

Question. Dr. Gallagher, last month NIST revised its Federal cybersecurity guidelines, which many agencies follow.

Could you discuss how new computing tools and trends, such as the move to "cloud computing" and mobile devices creates new potential cyber vulnerabilities?

Answer. Mobile devices and cloud computing have already significantly changed business capabilities, allowing employees access to information resources wherever and whenever they need it. These technologies offer both an opportunity and a challenge. Their unique capabilities—including their always-on, always-connected nature—can facilitate more efficient and effective business, but also create new challenges to ensure the confidentiality, integrity and availability of information accessed by these devices.

To address the security challenges and accelerate the Federal Government's secure adoption of cloud computing, NIST is playing a leading role in developing standards and guidelines, in close consultation and collaboration with standards bodies, the private sector, Federal departments and agencies, and other stakeholders. NIST's long-term goal is to provide thought leadership and guidance around the cloud computing paradigm to catalyze its use within industry and government.

NIST is working collaboratively with industry to bridge the security gaps in mobility. For example, NIST has ongoing work to identify properties and capabilities of roots of trust needed to secure next generation mobile devices. This work examines issues relating to boot firmware protections; integrity measurement and reporting of critical firmware and software; secure storage; device authentication; and application and data isolation.

What are the main takeaways from NIST's cybersecurity guidance to Federal agencies?

Answer. NIST cybersecurity guidance builds on the guiding principle of mission-focused, risk-based information security. NIST performs research and develops standards, best practices, testing and metrics in order to provide protections against threats to the confidentiality, integrity and availability of information and services. Through collaborations with industry and academia, NIST's programs in areas such as risk management, cryptography, identity management, authentication, key management, security automation, privacy, usability, biometrics, configuration baselines, vulnerability management, and trusted hardware are designed to give practical, affordable and innovative guidance and metrics for today's computing platforms and information management.

MOBILE PHONES AND CYBERSECURITY AWARENESS

Question. Dr. Gallagher, this year, there will be more mobile phones than people on the planet. Today, our wireless devices are not just phones, but pocket computers. We use them for sensitive transactions, including mobile banking and online purchases.

But GAO recently found that cyber threats are increasing for mobile devices and the information they store. GAO recommended that DHS and NIST work together to "establish a baseline measure of consumer awareness . . . related to mobile security." GAO also recommends the development of performance measures that use the baseline to assess the effectiveness of initiatives to educate the public about cybersecurity.

Could you share any thoughts on how best to raise public awareness for cybersecurity threats to mobile devices?

Answer. NIST is leading the National Initiative for Cybersecurity Education (NICE) initiative, involving more than 20 Federal departments and agencies, to ensure coordination, focus, public engagement, technology transfer and sustainability. DHS, FCC, and FTC are among the leads for the awareness components of NICE, including the development of baseline and progress information as part of their ongoing cybersecurity awareness campaigns. Interactions through this campaign suggest public awareness and practices with regard to mobile security are limited and this has led to the development of a "Safety Tips for Mobile Devices" resource by the STOP.THINK.CONNECT campaign and a recent blog post on "Being Smart with your Smartphone."

Question. What is the proper role for government and industry to promote best practices for both companies and consumers?

Answer. Government and industry must work together to promote best practices for companies and consumers. NIST works closely with industry on the research, development and outreach necessary to provide standards and guidelines, tools, metrics and best practices to protect our Nation's information technology infrastructure for business and industrial control systems. Through these collaborations, NIST continues to develop cybersecurity standards, security metrics, and product assurance programs to promote, measure, and validate the security attributes of information systems and services. As technology advances and security requirements evolve, NIST, with its industry partnerships, can critically evaluate existing standards, guidelines, and technologies to ensure that they adequately reflect the current state of the art.

QUESTIONS SUBMITTED BY SENATOR THAD COCHRAN

Question. All witnesses, we have heard about the importance of cooperation and clearly defined lanes responsibility across the Federal Government for our cybersecurity efforts. What are your respective roles in receiving and sharing threat information with the private sector?

Answer. NIST works with Federal agencies and private sector companies to develop underlying standards and best practices that are used to support a wide array of information sharing activities. These standards and best practices are a fundamental component of providing coordination between organizations, allowing for rapid and accurate sharing of information between government and industry, and industry to industry. The collaborative development approach ensures that the needs of all sectors are adequately addressed, leading to an information sharing ecosystem that benefits all organizations.

Question. All witnesses, I think we all recognize the importance of defending our Nation's critical infrastructure against cyber attacks. A foreign or terrorist cyber attack on our electric grid, water systems, or financial systems could cause widespread damage and even have detrimental effects on our economy and consumer confidence. There has been much discussion about how involved the Federal Government should be in defending infrastructure owned by non-Federal entities. How would you define the threshold for what types of non-Federal infrastructure might qualify as "critical" for these purposes?

Answer. Executive Order 13636 defines critical infrastructure as the systems and assets, whether 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 or safety, or any combination of those matters. NIST is working with critical infrastructure owners and operations and their partners to define a cybersecurity framework that reduces cyber risks to critical infrastructure. The Draft Cybersecurity Framework includes a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks.

Question. All witnesses, we've often heard that there is a potential for a "Cyber Pearl Harbor," or an unexpected cyber attack on our Nation by a foreign entity that has dramatic and lengthy consequences. I think it may be difficult for most Americans, and even members of this Committee, to visualize how exactly such an attack would be carried out and what it would look like. Can you help us to better understand these things? Are the appropriations this Committee has been recommending sufficient to help prevent such an attack?

Answer. NIST considers a cybersecurity threat to be any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. This includes threats that are immediate, have significant reach across the Internet and rapidly propagate. Ensuring we are able to develop solutions that can scale globally, protect technological innovation, and keep up with the threats are of utmost importance to NIST and the Department of Commerce as a whole.

Unlike a physical attack that has to conform to physical constraints, a cyberattack can have velocity, reach, and scale that does not have these limiting factors. A cyberattack can occur at the speed of a digital transmission, our interconnected systems can extend the reach beyond traditional kinetic limitations and with the intersections of cyber and physical systems, the scale of impacts can go beyond disruption or disclosure of sensitive information. A cyberattack can potentially have a physical impact, conducted at the speed, reach of the Internet and at the scale of our interconnected systems.

NIST appreciates the Committee's continued support and funding for the critical cybersecurity efforts at NIST.

QUESTIONS SUBMITTED TO RICHARD A. MCFEELY, EXECUTIVE ASSISTANT DIRECTOR, CRIMINAL, CYBER, RESPONSE, AND SERVICES BRANCH, FEDERAL BUREAU OF INVESTIGATION

QUESTIONS SUBMITTED BY SENATOR RICHARD J. DURBIN

CYBER EXECUTIVE ORDER—ROLE OF THE EXECUTIVE ORDER VERSUS CYBER LEGISLATION

Question. President Obama issued Executive Order (EO) 13636 in February of this year. What is the effect of this Executive order? Is it improving your ability to share information with the private sector?

Answer. Implementation of Executive Order (EO) 13636 is underway across the U.S. Government (USG). The Federal Bureau of Investigation (FBI) is optimistic that, once fully implemented, the Executive order will lead to better information sharing between the private sector and the government. Consistent with the USG policy (articulated in section 4 of EO 13636) "to increase the volume, timeliness, and quality of cyber threat information shared with U.S. private sector entities," the FBI has prioritized the efficient, effective, and appropriate sharing of cyber threat information with authorized entities and is working with the Department of Homeland Security (DHS) to ensure a consistent, whole-of-government solution to sharing cyber threat information with the private sector.

Among these changes, we have modified the means by which we share information with the private sector to prevent intrusion into companies' networks and the exfiltration of their data and intellectual property. For example, the FBI has increased the level of detail it provides to industry partners in briefings regarding cyber threats. The National Cyber Investigative Joint Task Force conducts these briefings for private sector, government, and critical infrastructure partners on a near-daily basis. In partnership with DHS and the Treasury Department, we also provided a detailed briefing on financial services industry threats to executives of more than 40 banks who participated in a secure video teleconference. Detailed briefings have also been provided to those in the energy sector, which is a key part of our Nation's infrastructure.

In addition, the FBI is working with DHS to release Joint Indicator Bulletins (JIBs) to anti-virus companies, Internet service providers, and foreign partners. These JIBs contain information regarding Internet Protocol (IP) addresses that are believed to be infected with malware. Since October 2012, the FBI has released approximately 170,000 IP addresses to more than 130 countries through DHS's U.S. Computer Emergency Response Team and our Legal Attaché. We have also released nine FBI Liaison Alert System notices to victims of intrusions and to trusted partners. These notices contain specific and technical actionable intelligence related to threats. Furthermore, as required by EO 13636, the Deputy Attorney General (DAG) has issued instructions regarding the timely production of unclassified reports of cyber threat information. The DAG instructions require the FBI to produce timely reports that contain sufficient technical and threat detail to facilitate cybersecurity defense and response activities. Furthermore, all components of the Department of Justice (DOJ) are required to update their systems to increase the volume, timeliness, and quality of cyber threat information that is shared with U.S. private sector entities so they can better protect and defend against cyber threats.

Question. When he signed the Executive order, President Obama also underscored the need for comprehensive cybersecurity legislation, since the scope of the Executive order is limited. What are your legislative priorities in terms of items you believe should be included in cyber legislation?

Answer. We would be pleased to work with DOJ, DHS, and others to identify legislative measures that may enhance cybersecurity, and we look forward to providing our views of any possible legislation pursuant to DOJ's role in assisting in the development of the administration's position.

CYBER EXECUTIVE ORDER—PROTECTING PRIVACY AND CIVIL LIBERTIES

Question. The Executive order requires Federal agencies to develop cybersecurity efforts in accordance with the Fair Information Practice Principles, as well as other policies, principles, and frameworks to protect privacy and civil liberties. I worked with a number of other Senators to ensure that the Cybersecurity Act of 2012 included provisions to protect privacy and civil liberties. What specific steps can government agencies take to ensure that privacy and civil liberties are protected as we enhance our Nation's cybersecurity?

Answer. Section 5 of EO 13636 is consistent with the work USG agencies have been doing to ensure that privacy and civil liberties are incorporated into our cyber activities and affirms the need to continue these efforts. Departments and agencies must also conduct regular assessments, with subsequent reporting, and include in these assessments an evaluation of their activities against the Fair Information Practice Principles and other applicable privacy and civil liberties policies, principles, and frameworks.

The FBI builds privacy and civil liberties protections into all investigative efforts, including cybersecurity. For example, the Domestic Investigations and Operations Guide (DIOG), which articulates FBI policy regarding our investigative and intelligence collection activities, outlines protections to be afforded at each step of an investigation. All FBI operational personnel are required to complete DIOG training and a specific privacy course, as well as yearly information security training (which includes a privacy component). The Privacy and Civil Liberties Unit (PCLU) in the FBI's Office of the General Counsel is devoted to privacy and civil liberties issues, including Bureau-wide compliance with the requirements of the Privacy Act and the eGovernment Act. PCLU is also actively involved in assessing the privacy and civil liberties aspects of FBI information systems and programs through Privacy Threshold Analyses and Privacy Impact Assessments. PCLU works closely with all FBI divisions, including the Cyber Division, to help ensure that appropriate protections are in place.

QUESTIONS SUBMITTED BY SENATOR MARY L. LANDRIEU

Question. General Alexander testified that the services, departments, and agencies need to work together to ensure that they have adequate test bed and range space to safely organize, train, and equip the cyber warriors, operators, managers, researchers, and agents across the Federal Government.

a. What are the specific requirements that your departments and their various agencies have for test bed and range space? What specific outcome will those established requirements render in trained personnel and tactics?

b. What is the current test bed and range capacity available to each of your departments? What is the wait time or backlog based on the access you currently have?

c. Have you identified additional test bed or range space that you would like to acquire, use, or lease?

d. What are the fiscal years 2013 and 2014 funding levels for testing and training space?

e. What percentage of your required testing and training needs will you be able to meet in fiscal years 2013 and 2014?

Answer to subparts a through e. As used in this inquiry, the concepts of "test-bed" and "range space" are not used by the FBI and we are not able to comment on them.

QUESTIONS SUBMITTED BY SENATOR TOM UDALL

ROLE OF NATIONAL LABORATORIES IN PROMOTING CYBERSECURITY

Question. Mr. McFeely, our National Labs—which are the crown jewels of our Nation's research system—are active in efforts to promote cybersecurity.

In my home State of New Mexico, Sandia National Laboratories is engaged in efforts to secure the national electrical grid from cyber attack. Los Alamos National Laboratories is a leader in quantum cryptography.

Sandia also has partnerships with universities and the private sector. They're helping computer science students become cyber professionals.

Could you discuss what role our National Labs should have in protecting our Nation from cyber attack?

Answer. The National Laboratories, which are Department of Energy (DOE) entities, are central to cybersecurity research and development and should continue to lead in these efforts. There are multiple areas in which opportunities exist for FBI-National Lab partnerships that leverage National Lab knowledge and resources to assist the FBI in meeting investigative challenges. For example, the FBI's Operational Technology Division and the Labs could partner to:

—Enlist the Labs' supercomputing resources to help solve the FBI's most computationally challenging problems;

—Study where to apply quantum cryptography research to protect against active cyber threats;

—Apply the Labs' vulnerability research to active FBI investigations; and

—Use unsolved investigative problems to motivate National Labs' vulnerability research.

Additionally, we continue to appreciate DOE's critical role as the sector specific agency for the energy sector in providing a cooperative environment to help the energy sector defend against cyber threats. Currently, the FBI collaborates with DOE and DHS to ensure the timely sharing of threat information with the energy sector. The FBI also works with DOE to support a voluntary program in which energy sector asset owners use government-developed tools to improve their situational awareness and better protect their own assets. Asset owners are free to share this information with the industry and government at their discretion.

Question. Mr. McFeely, your written testimony describes how the FBI is trying to help State and local law enforcement agencies pursue Internet crimes. I am disturbed by your comment that very few cases referred to State and local officials by the FBI are actually being worked.

Could you elaborate on the FBI's pilot program you mention in your testimony to help State and local law enforcement agencies pursue Internet fraud and cyber crimes?

Answer. Every year, there are thousands of individual and corporate victims of crimes facilitated through the use of computer networks or devices with targets that are independent of those networks or devices. These crimes are often referred to as Internet-facilitated crimes. Because these cases frequently involve victims spread across multiple jurisdictions and perpetrators living in foreign countries, local and State law enforcement agencies have often viewed these crimes as the province of Federal law enforcement agencies. Yet, while many local and State agencies have seen the problem as too broad for their jurisdictions, Federal agencies have not been able to prioritize these crimes in such a way that they receive significant investigative attention.

To properly address the threat of Internet-facilitated crimes against U.S. victims, the FBI is establishing a platform to assist in the development of these investigations by Federal, State, local, tribal, and international law enforcement agencies. This platform is being developed through the Internet Crime Complaint Center (IC3), which has received victims' reports of Internet crimes for the past 13 years and is currently receiving approximately 300,000 complaints annually. The FBI will leverage intelligence that has been consolidated at IC3 and package it in a way that facilitates investigations by appropriate law enforcement agencies, with assistance provided by the FBI's local Cyber Task Force.

In addition to this broad program, the FBI is seeking ways to work in cost-efficient and effective ways with State and local governments on cybersecurity matters. For example, we have begun a pilot project with the Utah Department of Public Safety to disseminate Internet fraud information to law enforcement authorities throughout the State. We will assess the results of this Utah pilot to determine whether it should be expanded to other jurisdictions.

Questions Submitted by Senator Thad Cochran

Question. All witnesses, we have heard about the importance of cooperation and clearly defined lanes responsibility across the Federal Government for our cybersecurity efforts. What are your respective roles in receiving and sharing threat information with the private sector?

Answer. The FBI, which is an intelligence-driven and threat-focused national security organization with both intelligence and law enforcement responsibilities, is charged with investigating, attributing, and disrupting cyber crimes. The FBI may receive information regarding a cyber threat or incident from a victim or third party, including those in the private sector. We are working toward making Guardian, which is our terrorist threat tracking and collaboration system, available to trusted industry partners to report cyber intrusions in real time. Known as iGuardian, this system will allow the FBI to more effectively understand and identify cyber threats, collaborate with our government partners through the sharing of information regarding cyber intrusions, and track pending investigations and operations. Each incident reported through this system will immediately be routed to CyWatch, the FBI's 24/7 cyber operations center, where it will be vetted and assigned to an FBI Cyber Task Force investigator.

In the course of the FBI's investigative process, we share information with USG partners in support of their roles in the incident response process. The information we share is used to help us and our Intelligence Community partners understand the actions, goals, methods, and capabilities of those posing threats, and to anticipate and prevent future attacks against our critical infrastructure and government systems. The FBI also notifies any additional actual or potential victims or targets revealed through investigation and, as part of the USG team, provides the information they need to protect their systems.

The FBI completes these activities in a manner that ensures protection of the digital crime scene and actions are taken consistent with preserving evidence for use in a later criminal proceeding, if it is determined that such a proceeding is warranted.

Question. All witnesses, I think we all recognize the importance of defending our Nation's critical infrastructure against cyber attacks. A foreign or terrorist cyber attack on our electric grid, water systems, or financial systems could cause widespread damage and even have detrimental effects on our economy and consumer confidence. There has been much discussion about how involved the Federal Government should be in defending infrastructure owned by non-Federal entities. How would you define the threshold for what types of non-Federal infrastructure might qualify as "critical" for these purposes?

Answer. Presidential Policy Directive 21, "Critical Infrastructure Security and Resilience" (2/12/13) (PPD–21) defines the term "critical infrastructure" as follows:

The term "critical infrastructure" has the meaning provided in section 1016(e) of the USA Patriot Act of 2001 (42 U.S.C. 5195c(e)), namely systems and assets, whether 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 or safety, or any combination of those matters.

PPD–21 identifies 16 critical infrastructure sectors. Based on the cyber threat to each of these sectors, the potential impact of a cyber attack on these sectors, and the extent to which other Federal agencies are responsible for their protection, the FBI has organized its efforts to address the threats to these 16 critical infrastructure sectors in the following order of priority:

—Financial Services, Chemical, Communications, Defense Industrial Base, Energy, Healthcare and Public Health, Information Technology, Nuclear, and Transportation;

—Food and Agriculture, Critical Manufacturing, Dams, and Water;

—Commercial Facilities, Emergency Services, and Government Facilities.

Question. All witnesses, we've often heard that there is a potential for a "Cyber Pearl Harbor," or an unexpected cyber attack on our Nation by a foreign entity that has dramatic and lengthy consequences. I think it may be difficult for most Americans, and even members of this Committee, to visualize how exactly such an attack would be carried out and what it would look like. Can you help us to better understand these things? Are the appropriations this Committee has been recommending sufficient to help prevent such an attack?

Answer. As the question recognizes, the events of Pearl Harbor represented an unexpected, surprise attack on our Nation by a foreign entity with devastating consequences. Under this analogy, in a "Cyber Pearl Harbor," the United States might one day face, without warning, the wide-scale disruption of a critical service that would result in damages, both economic and physical, to include the loss of life. Along with our law enforcement and Intelligence Community partners, the FBI works every day to prevent and address the threat of an attack of this scale.

Cyber-attacks are continually increasing in both frequency and sophistication. The U.S. economy is continually threatened by cyber activities that are difficult to detect and that deprive us of the full value of our intellectual property, threaten our economic prosperity, and erode our military advantages. Since 2008, appropriated funds have provided more than 500 new FBI support, intelligence, and special agent personnel to address cyber threats. Although these and other critical resources have helped us counter increasingly aggressive cyber threats, as the sophistication of malicious software increases and the demand that critical systems be globally available grows, these systems become ever more vulnerable to attack.

CONCLUSION OF HEARING

Chairwoman MIKULSKI. As previously announced and as part of our practice on security issues, we will now move to a closed briefing. Before we do, I would like to make some general closing comments.

First of all, I really do want to thank the witnesses for participating. The hearing has not been quite the way we originally thought, but it was a good hearing. People do have a right to know. People have a right to say their voices. That is why we responded.

But I think the big national debate that started after 9/11 is the inherent tension between security and privacy. It is time now for a new, fresh national debate. It is beginning in the usual committee structure.

The second thing is that many of us are concerned about what is the access to people and businesses' information. Now, there are those who, because of the Snowden revelation, wonder about Government's access to that information, whether it is through the NSA, whether it is through the IRS, or whatever. People are asking what is the Government doing.

The purpose of this hearing, however, is who is raiding the information that we have. So maybe people are concerned about what is NSA doing. But I am concerned about the people every single day that are trying to get access to somebody's Social Security number, their Medicare number, their checking account number, their smart phone information so they can either steal from them or lead to other access to their bank account, to their other kinds of assets. So we are worried about that.

I am concerned every day about the number of people out there, with the great intellectual entrepreneurship of our country, that are coming up with new ideas and new products to create the new jobs for the 21st century. And they are being stolen in the greatest cyber espionage heist. So why find a cure for cancer if you can try to steal it from FDA or the Patent Office? I am worried about that.

And then I worry about things like the grid and I worry about access to those who are trying to raid the grid. Tonight there is a gathering storm. We fear a derecho, another derecho maybe hitting the Maryland-Washington area. We know when the grid is shut down, it is a terrible consequence in terms of our society. I do not want ever to have a grid shut down here in the Greater Capital Region or anywhere in the United States.

So the purpose of this hearing was to go after those who have predatory intent—predatory, premeditated intent—against either an individual, our business, or our critical infrastructure.

There are those who are also concerned about is Government now passing beyond a red line on civil liberties. I think we ought to have that debate. I think we ought to have that discussion. It could be the subject of another hearing here. There will be the Feinstein hearing. There will be the Judiciary Committee hearing. But you know what? This is America. This is America and people have a right to know. They have a right to have their public officials explain this.

So I think it has been a great hearing.

So, therefore, though, this committee will now stand in recess after the closed briefing until the morning of Thursday, June 20, where we will vote on our spending allocations and also take up the very important legislation of Veterans Affairs and our agricultural appropriations. This committee now stands in recess.

[Whereupon, at 4:39 p.m., Wednesday, June 12, the hearing was concluded, and the committee was recessed, to reconvene subject to the call of the Chair.]

○