AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

ENHANCING CYBERSECURITY OF THIRD-PARTY CONTRACTORS AND VENDORS

HEARING

BEFORE THE

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTEENTH CONGRESS

FIRST SESSION

APRIL 22, 2015

Serial No. 114–47

Printed for the use of the Committee on Oversight and Government Reform

Available via the World Wide Web: http://www.fdsys.gov
http://www.house.gov/reform

U.S. GOVERNMENT PUBLISHING OFFICE

97–335 PDF WASHINGTON : 2015

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 OVERSIGHT AND GOVERNMENT REFORM

JASON CHAFFETZ, Utah, *Chairman*

JOHN L. MICA, Florida
MICHAEL R. TURNER, Ohio
JOHN J. DUNCAN, JR., Tennessee
JIM JORDAN, Ohio
TIM WALBERG, Michigan
JUSTIN AMASH, Michigan
PAUL A. GOSAR, Arizona
SCOTT DESJARLAIS, Tennessee
TREY GOWDY, South Carolina
BLAKE FARENTHOLD, Texas
CYNTHIA M. LUMMIS, Wyoming
THOMAS MASSIE, Kentucky
MARK MEADOWS, North Carolina
RON DESANTIS, Florida
MICK MULVANEY, South Carolina
KEN BUCK, Colorado
MARK WALKER, North Carolina
ROD BLUM, Iowa
JODY B. HICE, Georgia
STEVE RUSSELL, Oklahoma
EARL L. "BUDDY" CARTER, Georgia
GLENN GROTHMAN, Wisconsin
WILL HURD, Texas
GARY J. PALMER, Alabama

ELIJAH E. CUMMINGS, Maryland, *Ranking Minority Member*
CAROLYN B. MALONEY, New York
ELEANOR HOLMES NORTON, District of Columbia
WM. LACY CLAY, Missouri
STEPHEN F. LYNCH, Massachusetts
JIM COOPER, Tennessee
GERALD E. CONNOLLY, Virginia
MATT CARTWRIGHT, Pennsylvania
TAMMY DUCKWORTH, Illinois
ROBIN L. KELLY, Illinois
BRENDA L. LAWRENCE, Michigan
TED LIEU, California
BONNIE WATSON COLEMAN, New Jersey
STACEY E. PLASKETT, Virgin Islands
MARK DeSAULNIER, California
BRENDAN F. BOYLE, Pennsylvania
PETER WELCH, Vermont
MICHELLE LUJAN GRISHAM, New Mexico

SEAN MCLAUGHLIN, *Staff Director*
DAVID RAPALLO, *Minority Staff Director*
SARAH VANCE *Clerk*

CONTENTS

ENHANCING CYBERSECURITY OF THIRD–PARTY CONTRACTORS AND VENDORS

Wednesday, April 22, 2015,

HOUSE OF REPRESENTATIVES,
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM,
WASHINGTON, D.C.

The committee met, pursuant to call, at 9:35 a.m., in Room 2247, Rayburn House Office Building, the Honorable Jason Chaffetz [chairman of the committee] presiding.

Present: Representatives Chaffetz, Mica, Walberg, Amash, Massie, Meadows, DeSantis, Mulvaney, Buck, Walker, Hice, Russell, Carter, Grothman, Hurd, Palmer, Cummings, Maloney, Norton, Clay, Lynch, Connolly, Cartwright, Duckworth, Kelly, Lawrence, Lieu, Plaskett, DeSaulnier, and Lujan Grisham.

Chairman CHAFFETZ. The Committee on Government Reform will come to order.

Without objection, the chair is authorized to declare a recess at any time.

One of the most serious national security challenges we currently face as a Nation is the security of our Country's information and communications infrastructure. I am encouraged this committee is leading a bipartisan effort to address our Government's cybersecurity, and I want to thank Ranking Member Cummings for bringing this issue to the committee's attention and for his tenacity in insisting that we address this in an aggressive way and, thus, we are here today.

The stakes are high. Hackers are targeting extremely sensitive information related to our national security. Hackers recently hit the White House, State Department networks. They are accessing a range of sensitive information. But these are not isolated incidents. Cyber attacks against government assets are becoming more frequent and they are more sophisticated then ever. Over the past eight years, the number of information security incidents has risen by more than 1,000 percent, if not more, and they are happening at the private sector at an increasing and alarming rate.

One of the members of our team that knows a lot about this we are proud to have as the subcommittee chairman on our IT Subcommittee is the general from Texas, Mr. Hurd. I would like to give him time at this point.

Mr. HURD. Thank you, Mr. Chairman. I join you in thanking Ranking Member Cummings for bringing this important issue to the committee's attention.

This is not a new problem. The Government Accountability Office has identified the security of Federal information systems and crit-

ical infrastructure as a government-wide high-risk issue every year since 1997. Congress recently took action to address the cybersecurity threat. Last year we passed an update to the Federal Information Security Management Act, or FISMA, of 2014. This committee, and particularly the IT Subcommittee, which I chair, intends to closely monitor the implementation of FISMA 2014 because FISMA is the backbone of the Federal response to the cybersecurity threat.

A key aspect of these reforms was increased accountability and transparency for OMB and DHS and all Federal agencies with regard to cybersecurity, and Federal agencies are now required to report to Congress when their networks are hacked. This increased transparency will allow Congress to better understand how our Government is protecting some of our most sensitive information.

Concerns about cybersecurity are not limited to government networks. Hackers have successfully breached the networks of government contractors like USIS and KeyPoint. Their computer networks contain extremely sensitive information about thousands of Federal employees cleared to access classified information. In fact, almost one-third of all personnel who provide security services at the 24 major Federal agencies are contractors. So we have to make sure government contractors are protecting the information we entrust them to protect.

After all, as the chairman said, if one of our Nation's most secure networks, the White House, is vulnerable and susceptible to these attacks, then how do we know to what extent other agencies and contractors are preparing themselves?

Mr. Chairman, I look forward to working with you and the ranking members and members on both sides of the aisle in this process. I yield back.

Chairman CHAFFETZ. I thank the gentleman.

We will now recognize the ranking member of the full committee, Mr. Cummings, for five minutes.

Mr. CUMMINGS. Thank you very much, Mr. Chairman. I thank you for agreeing to my request to hold today's hearing on the cybersecurity challenges posed by contractors and third-party vendors.

Over the past several years we have seen an alarming increase in the number of major data breaches that originated with contractors and vendors. Just last year, Target and Home Depot were breached by hackers who gained access to the retailers' networks by using credentials stolen from the computer systems of vendors that did business with these companies.

Federal agencies are not immune. The breach of the Postal Service last year originated from a phishing attack on a contractor for the agency. Last year, contractors with the Office of Personnel Management were subjected to a sophisticated cyber attack and tens of thousands of sensitive personnel records were compromised. One of those contractors was a company called USIS. At the time, it was the largest provider of background information investigative services to the Federal Government.

USIS is currently at the center of a billion dollar civil fraud suit brought by the Justice Department for allegedly dumping incomplete background investigation reports to OPM over a four and a half year time period. According to the Justice Department, USIS deliberately took this action to increase profits. Apparently, the

company's desire to increase profits also may have been to blame for its failure to make cyber investments necessary to secure the large amounts of sensitive personal information it should have been protecting on its networks.

On September 3rd, 2014, committee staff received a briefing from security experts at the Department of Homeland Security, the Office of Director of National Intelligence, and OPM, all of whom analyzed the cyber attack against USIS. While much of that briefing was sensitive, one point may be discussed publicly. Press accounts had initially reported that the attack may have compromised the personal information of up to 27,000 Federal employees.

However, government cybersecurity experts believe this number is a floor and not a ceiling. The actual number of individuals affected by USIS's data breach is still not yet known, but these experts believe that the personal information of many more Federal employees may have been compromised.

Unfortunately, investigating the USIS data breach has been particularly challenging. That is because neither USIS nor its parent company, Altegrity, have fully complied with this committee's request for answers.

Today's hearing is a recognition that the Federal Government faces increased cyber risks from contractors. But as I mentioned earlier, this is a challenge the private sector faces as well.

I have repeatedly pressed for more rigorous oversight of cybersecurity in both private and public sectors. Although we had little success in the previous Congress, I am encouraged by the bipartisan approach we have taken on this very critical issue and I hope it continues.

So, Mr. Chairman, I want to thank you again for agreeing to hold today's hearing. In addition, I understand that our staffs are meeting tomorrow to discuss a possible follow-on hearing with some of these private sector entities. And I want to thank you for continuing to work with me.

While our ranking member is not here yet, I would yield a minute to my colleague, Mr. Connolly, who has worked very hard on these issues over the years. He might have a brief statement.

Mr. CONNOLLY. I thank the ranking member for his generosity.

Obviously, cybersecurity is a sophisticated and evolving national challenge. Meeting the daunting threat requires a broad whole-Government and industry approach that simultaneously enhances what I believe are the three pillars of an effective approach to cybersecurity: people, policy, and practices.

No better demonstration of this importance of individuals in securing information systems than the truism that the number one cybersecurity threat or vulnerability facing any company is the behavior of its own employees. Indeed, the best cybersecurity policies in the world won't amount to a hill of beans if an organization's culture does not translate good policy into better practice.

So I really look forward to hearing the testimony today. I look forward to working with you, Mr. Chairman, and you, Mr. Cummings, as we move forward with some legislative remedies to what I think is a vexing and growing problem that affects both the domestic and, frankly, defense and intelligence sides of the Federal Government. Thank you.

Chairman CHAFFETZ. Thank you. The gentleman yields back.

I will hold the record open for five legislative days for any members who would like to submit a written statement.

We will now recognize our first panel of witnesses.

Pleased to welcome Mr. Tony Scott, Chief Information Officer and Administrator of the Office of Electronic Government and Information Technology at the Office of Management and Budget. My understanding is, Mr. Scott, this is your first time testifying before Congress in your new role as the Federal CIO, and we appreciate you being here. It will be an interesting experience. You have done a lot of important work here. You have a very impressive resume and background, and we look forward to working with you in your new role, and appreciate you being here today.

Ms. Donna Seymour is the Chief Information Officer at the Office of Personnel Management. Again, we welcome you.

Mr. Gregory Wilshusen is the Director of Information Security Issues at the Government Accountability Office, otherwise known as the GAO.

And Dr. Eric Fischer is the Senior Specialist in Science and Technology at the Congressional Research Service. We appreciate you, doctor, for being here today. We very much value what the CRS does for all members, both sides of the aisle, and we appreciate the organization and the good work that is done there. We rely heavily on it and we look forward to your testimony today.

Pursuant to committee rules, all witnesses are to be sworn before they testify, so if you will please rise and raise your right hands.

Do you solemnly swear or affirm that the testimony you are about to give will be the truth, the whole truth, and nothing but the truth?

[Witnesses respond in the affirmative.]

Chairman CHAFFETZ. Let the record reflect that all witnesses have answered in the affirmative.

In order to allow time for discussion, we would appreciate it if you would hold your verbal comments to five minutes. We have a little generosity on that, but please be assured that your entire written statement will be entered into and made part of the record.

So, with that, Mr. Scott, we will now recognize you for five minutes.

WITNESS STATEMENTS

STATEMENT OF TONY SCOTT

Mr. SCOTT. Thank you, Chairman Chaffetz and Ranking Member Cummings and members of the committee. Thank you for the opportunity to appear before you today.

I started as the Federal Chief Information Officer just over two months ago, and I am excited for the opportunity to speak with you today about OMB's role in Federal cybersecurity. I am also pleased to join the panel, as everyone here has an important role to play in strengthening cybersecurity.

Federal cybersecurity oversight is one of my responsibilities as Federal CIO and head of the OMB Office of E–Government and Information Technology. My office is responsible for two things: first, developing and overseeing the implementation of Federal IT policy

and, second, through the United States Digital Service, providing onsite expertise to agencies with high impact facing IT programs. My team is also leading the government-wide implementation of the Federal Information Technology Acquisition Reform Act, known as FITARA, and the Federal Information Security Modernization Act of 2014, FISMA, both of which passed last year.

Strengthening Federal cybersecurity is one of the Administration's top priorities and a duty that I take very seriously. Having recently left a private sector CIO role, I can attest to the fact that having a strong cybersecurity program is critical to ensuring mission success. This is no different in the Federal Government. Given the evolving threat landscape, it is imperative that we do everything we can and everything in our power to ensure the security of Government information and networks. In this interconnected world, we have to ensure that agencies, the contractors that support them, and the citizens we serve are all protected.

I would like to start by providing an overview of OMB's role in Federal cybersecurity, discuss some recent incidents related to third-party contractors and vendors, and some of the steps OMB is taking to strengthen Federal cybersecurity practices.

OMB and my office recently announced the creation of a dedicated unit called the E–Gov Cyber Unit. This unit will conduct oversight through initiatives, such as CyberStat reviews and will drive FISMA implementation. We will continue to work closely with DHS, who is our operational partner, and with agencies who directly lead their own cybersecurity efforts. These efforts are critical in confronting today's cyber threats and improving our ability to deal with threats in the future.

In 2014 alone, several high-profile cyber incidents across our Nation made headlines for their scope, their scale, and their impact. The Federal Government and those acting on its behalf are not immune from this threat activity, as has been noted. Specifically and related to today's discussion, cyber incidents have involved vendors responsible for conducting background investigations on behalf of the Federal Government. In close partnership with DHS and other appropriate agencies, OMB responded quickly and oversaw the government-wide response to mitigate these incidents.

DHS worked closely with vendors that conduct background investigations to mitigate this incident, and OMB, in its policy and oversight role, took immediate action to address identified challenges. First, through the President's Management Council, OMB conducted a review of agencies' cyber security programs to identify risks and implementation gaps. During this response to these incidents and our subsequent review, two things became clear: first, third-party contractors and vendors were inconsistently implementing protections over sensitive data and, second, Federal agencies did not have adequate contractual language and policy direction to guide how contractors and agencies should respond to incidents.

Based on this review, agencies were directed to identify and review relevant contracts to ensure compliance with current laws and OMB guidance and, second, OMB directed an interagency effort to collect and disseminate contracting best practices relative to cybersecurity.

In closing, I think it is obvious that securing our information is a great challenge, and this will remain a core focus of this Administration. We look forward to working with Congress on legislative actions that may further protect our Nation's critical networks and systems, and I thank the committee for holding this hearing and for your commitment to improving Federal cybersecurity. When it is time, I would be pleased to answer any questions you may have.

[Prepared statement of Mr. Scott follows:]

Embargoed until Delivered

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503
www.whitehouse.gov/omb

TESTIMONY OF TONY SCOTT

UNITED STATES CHIEF INFORMATION OFFICER
OFFICE OF MANAGEMENT AND BUDGET
BEFORE THE COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
UNITED STATES HOUSE OF REPRESENTATIVES

April 22, 2015

Chairman Chaffetz, Ranking Member Cummings, members of the Committee, thank you for the opportunity to appear before you today. As some of you may know, I started my Office of Management and Budget (OMB) career just over two months ago, and I'm excited for the opportunity to speak with you today about OMB's role in Federal cybersecurity.

Before I begin, I would like to say that Federal cybersecurity oversight is one of my responsibilities as the Federal Chief Information Officer (CIO). As Federal CIO, I lead OMB's Office of E-Government & Information Technology (IT) (E-Gov). This office is responsible for: (1) developing and overseeing the implementation of Federal IT policy and (2) through the United States Digital Service, providing on-site expertise to agencies with high-impact public facing IT programs. During this Administration, E-Gov has been responsible for developing successful initiatives, like TechStat and PortfolioStat, which are focused on ensuring agency programs deliver value to customers. This is also the team responsible for leading the government-wide implementation of the Federal Information Technology Acquisition Reform Act (FITARA).[1] Although the objective of this law is to improve management of IT through strengthened CIO authorities, the law's impact on cybersecurity cannot be understated. CIOs with the proper authorities to manage IT will help ensure agencies are consistently applying cybersecurity policies and practices. Even though my team has a variety of responsibilities, I will focus my remarks on the team's work in Federal cybersecurity.

Strengthening Federal cybersecurity is one of the Administration's top priorities and a duty that I take very seriously. Having recently left a private sector CIO role, I can attest to the fact that having a strong cybersecurity program is critical to ensuring mission success. This is no different in the Federal government. Given the evolving threat landscape, it is imperative that we do everything in our power to ensure the security of government information and networks. In this interconnected world, we have to ensure that agencies, third-party contractors and vendors, and the citizens we serve all are protected from these threats. In my remarks today, I will provide you with an overview of OMB's role in Federal cybersecurity, a description of

[1] https://www.congress.gov/bill/113th-congress/house-bill/3979

recent events related to the cybersecurity of third-party contractors and vendors, and the steps OMB is taking to strengthen Federal cybersecurity practices.

OMB's Role in Federal Cybersecurity

To better understand OMB's role, I think it is important to provide a brief overview of the Federal cybersecurity landscape and the various offices involved. Under the Federal Information Security Modernization Act of 2014 (FISMA), the Director of OMB is responsible for Federal information security oversight and policy issuance for non-national security systems.[2] For national security systems, oversight and policy authority is delegated under FISMA to the Secretary of Defense for Department of Defense (DoD) systems and to the Director of National Intelligence for Intelligence Community systems. My testimony today will focus on OMB's role overseeing non-national security systems.

OMB executes its responsibilities in close coordination with its Federal cybersecurity partners, including the Department of Homeland Security (DHS) and the Department of Commerce's National Institute of Standards and Technology (NIST). FISMA clarifies DHS's role as the operational lead for cybersecurity of Federal civilian government systems. Specifically, the law gives DHS the authority to issue binding operational directives and to provide technical assistance to agencies. The law also states that Federal agencies are responsible for "providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of: (1) information collected or maintained by or on behalf of the agency and (2) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency."

Understanding the importance of this responsibility, OMB recently announced the creation of the first ever dedicated cybersecurity unit within the Office of E-Government & IT: the E-Gov Cyber and National Security Unit (E-Gov Cyber). The creation of the E-Gov Cyber Unit reflects OMB's focus on conducting robust, data-driven oversight of agencies' cybersecurity programs and on issuing Federal guidance consistent with emerging technologies and risks. This is the team behind the work articulated in the Fiscal Year (FY) 2014 FISMA report which highlighted both successes and challenges affecting Federal agencies' cyber programs. In FY 2015, the E-Gov Cyber Unit is targeting oversight through CyberStat reviews, prioritizing agencies with high risk factors as determined by cybersecurity performance and incident data. Additionally, the Unit is driving FISMA implementation by providing agencies with the guidance they need in this dynamic environment. The top FY 2015 policy priority of the team is updating Circular A-130, which is the central government-wide policy document that establishes agency guidelines on how to manage information resources. The E-Gov Cyber Unit is actively engaging with various stakeholders within the IT community to ensure the updated Circular provides agencies with guidance consistent with the latest technologies and best practices.

[2] https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf

Cybersecurity and Third-Party Contractors and Vendors

In 2014, several high profile cyber incidents across our nation made headlines for their scope, scale, and impact on victims. The Federal government was not immune to this threat activity. In 2014, cyber incidents impacted vendors responsible for conducting background investigations on behalf of the Federal government. In close partnership with DHS and appropriate agencies, OMB responded quickly and oversaw the government-wide response to mitigate the incidents, to include ensuring that relevant agencies notified potential victims in accordance with OMB guidance. During the response to these incidents, two things became clear: (1) third-party contractors and vendors were inconsistently implementing protections to prevent the unauthorized access, use, disclosure, disruption, modification, or destruction of government information and (2) Federal agencies did not have adequate contractual language, policy direction, or awareness of best practices to guide how contractors and agencies should respond to intrusions and/or actual breaches.

Steps Taken to Address Challenges

As part of the immediate response efforts, DHS worked closely with vendors that conduct background investigations, at their request, to ensure they had comprehensive controls in place to protect against future incidents. At the same time, OMB, in its policy and oversight role, took immediate action to address identified challenges. First, through the President's Management Council (PMC), OMB conducted a review of agencies' cybersecurity programs to identify risks and implementation gaps. Second, OMB directed an inter-agency effort to collect and disseminate contracting best practices to help agencies ensure the protection of sensitive government information.

The review conducted through the PMC allowed agencies and OMB to assess a broad range of cybersecurity risks ranging from how agencies identify and detect threats to agency policies and procedures for responding to incidents. As part of this review, agencies were directed to establish and initiate a process for identifying and reviewing relevant contracts to ensure compliance with Federal cybersecurity and privacy laws, OMB guidance, and NIST standards. The results of these reviews provided important context for both OMB and agencies and are being used to inform ongoing efforts to strengthen agency cybersecurity programs.

The inter-agency effort to collect and disseminate contracting best practices included direction from OMB to the Federal CIO Council and Chief Acquisition Officers (CAO) Council to provide recommendations to OMB for next steps to bolster cyber protections in Federal contracts. As part of this effort, OMB will address the need for:

- Formal guidance to agencies to implement new policy requirements;
- Updates to existing guidance or recommended inclusions in annual guidance documents; and
- Facilitation of best practices sharing through existing interagency forums.

In closing, I would like to say that securing our information in cyber space is the next great challenge for our country, but it is a challenge that I welcome. Ensuring the security of

information on the Federal government's networks and systems will remain a core focus of the Administration as we move aggressively to implement innovative protections and respond quickly to new challenges as they arise. In addition to our current strategy, we look forward to working with Congress on legislative actions that may further protect our nation's critical networks and systems.

I thank the Committee for holding this hearing, and for your commitment to improving Federal cybersecurity. I would be pleased to answer any questions you may have.

Mr. HURD. [Presiding] Thank you, Mr. Scott.
Ms. Seymour, you are now recognized for five minutes.

STATEMENT OF DONNA K. SEYMOUR

Ms. SEYMOUR. Chairman Chaffetz, Ranking Member Cummings, and members of the committee, thank you for inviting me to participate in today's hearing to examine the cybersecurity of third-party contractors. I am happy to be here with you today to share OPM's experiences in the important area of cybersecurity.

As the Chief Information Office of the Office of Personnel Management, I am responsible for the information technology that supports OPM's mission to recruit, retain, and honor a world-class workforce. Director Archuleta tasked me with conducting a thorough assessment of the state of IT at OPM, including cybersecurity. Director Archuleta's goal, as laid out in the OPM Strategic Plan, is to innovate IT infrastructure at OPM in a way that protects sensitive information entrusted to us by the Federal workforce and the American people.

OPM and its contractors are under constant attack by advanced persistent threats and criminal actors. These adversaries are sophisticated, well funded, and focused. In an average month, OPM thwarts almost 2.5 billion confirmed attempts to hack its network. These attacks will not stop. If anything, they will increase.

While we need to focus on how to prevent attacks, we know from the NIST cybersecurity framework it is equally important that we focus on how to detect, investigate, and mitigate attacks. In the past year, OPM and some of its contractors became the victims of cyber attacks. Throughout the process of analyzing the breaches, OPM worked closely with the US–CERT at DHS, the FBI, and other agencies. We also worked with the Office of Management and Budget, the CIO Council, and the Privacy Council. OPM followed OMB protocols, informing the agency response team investigating the incidents, and making notifications.

We learned there were significant differences in our ability to understand and respond to these attacks because of the way sensitive information is exchanged, because of technical architecture, and because of the contractual relationship with the company.

The way in which the Government shares sensitive information with the company is important to understand. In one case, company-owned laptops connected directly to the OPM network; in another case, company-owned laptops connected to the company's network and then to OPM network. If laptops connect directly to the Government network, it is easier to assess their security posture and limit the exposure of the sensitive information.

The architecture of the network is important because it provides a framework for how sensitive information is stored, accessed, and exchanged, and it defines the boundaries for protecting the network. If the network is well defined and the data is segregated, it is easier to protect. A well architected network also makes it easier to investigate incidents. And, of course, network logs help us understand what might have happened during an incident.

When the Government has a well-defined relationship with a contractor that specifically addresses information security and incident management, it is easier to work with the company to obtain

information and plan remediation efforts. As a result of lessons learned this past year, the agencies have collaborated with the help of OMB and the Office of Federal Procurement Policy and the CIO Council to share lessons learned. This includes contracting clauses that strengthen our relationship with contractors.

For example, at the onset of the contract, a security assessment serves as a method to review the security features in place to protect sensitive information. This assessment should be validated by an independent assessment organization. But this only provides a prospective of the security posture at a point in time. An information security continuous monitoring program is essential to enabling insight into the security posture of a system on a recurring basis.

Director Archuleta recognizes cybersecurity as an agency priority. OPM's 2016 budget request included $21 million to complete the modernization of our IT infrastructure. This funding is critical to continue the progress we have made so far in protecting data from relentless adversaries. For example, OPM is implementing information security continuous monitoring both in our own network and systems, as well as our contractor systems.

We look at security controls on a rotating, more frequent basis, identifying vulnerabilities in real time given the changing nature of threats. Plans of actions and milestones are created and tracked to remediate concerns. OPM has also grown its cybersecurity capability, which will allow us to do onsite technical inspections of contractor networks in the future.

Thank you for this opportunity to testify today. I am happy to address any questions you may have.

[Prepared statement of Ms. Seymour follows:]

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

STATEMENT OF
DONNA SEYMOUR
CHIEF INFORMATION OFFICER
U.S. OFFICE OF PERSONNEL MANAGEMENT

before the

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
UNITED STATES HOUSE OF REPRESENTATIVES

on

"Enhancing Cyber Security of Third-Party Contractors and Vendors"

April 22, 2015

Chairman Chaffetz, Ranking Member Cummings and Members of the committee:

Thank you for inviting me to participate in today's hearing to examine the cyber security of third party contractors. I am happy to be here with you today to share OPM's experiences in the important area of cybersecurity.

As Chief Information Officer (CIO) for the Office of Personnel Management (OPM), I am responsible for the information technology (IT) security that supports OPM's mission to recruit, retain, and honor a world class workforce. Director Katherine Archuleta tasked me with conducting a thorough assessment of the state of IT at OPM – including cybersecurity. Director Archuleta's goal, as laid out in OPM's Strategic IT Plan, is to innovate IT infrastructure at OPM in a way that protects the sensitive information entrusted to us by the Federal workforce and the American people.

OPM and its contractors are under constant attack by advanced persistent threats and criminal actors. These adversaries are sophisticated, well-funded, and focused. In an average month, OPM thwarts almost two and a half billion confirmed attempts to hack its network. These attacks will not stop – if anything, they will increase. While we need to focus on how to prevent attacks, we know from the National Institute of Standards and Technology (NIST) Cybersecurity Framework

it is equally important that we focus on how to detect, investigate, and mitigate attacks.

In the past year, OPM and some of its contractors became the victims of cyber-attacks. Throughout the process of analyzing the breaches, OPM worked closely with the US Computer Emergency Readiness Team (CERT) at the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), and other agencies. We also worked with the Office of Management and Budget (OMB), the CIO Council, and the Privacy Council. OPM followed OMB protocols in forming the Agency Response Team, investigating the incidents, and making notifications. We learned there were significant differences in our ability to understand and respond to these attacks because of the way sensitive information is exchanged, because of technical architecture, and because of the contractual relationship with the company.

The way in which the government shares sensitive information with the company is important to understand. In one case, company-owned laptops connected directly to the OPM network. In another case, company-owned laptops connected to the company's network and then to the OPM network. If laptops connect directly to the government network, it is easier to assess their security posture and limits exposure of the sensitive information.

The architecture of the network is important because it provides a framework for how sensitive information is accessed and exchanged, and it defines the boundaries for protecting the network. If the network is well defined and data is segregated, it is easier to protect. A well architected network also makes it easier to investigate incidents. And, of course, network logs help us understand what might have happened during an incident. When the government has a well-defined relationship with the contractor that specifically addresses information security and incident management, it is easier to work with the company to obtain information and plan remediation efforts. As a result of lessons learned this past year the agencies have collaborated, with the help of OMB Office of Federal Procurement Policy and the CIO Council, to share lessons learned. This includes contracting clauses that strengthen our relationship with contractors.

For example, at the onset of the contract a security assessment serves as a method to review the security features in place to protect sensitive information. This assessment should be validated by an independent assessment organization. But this only provides a perspective of the security posture at a point in time. A

continuous monitoring program is essential to enabling insight into the security posture of a system on a recurring basis.

Director Archuleta recognizes cyber-security as an agency priority. OPM's 2016 budget request included $21 million to complete the modernization of our IT infrastructure. This funding is critical to continue the progress we have made so far in protecting data from relentless adversaries. For example, OPM is implementing continuous monitoring, in a lawful manner, both for its own network and systems as well as its contractor systems. We look at security controls on a rotating, more frequent basis, identifying vulnerabilities in real time given the changing nature of threats. Plans of action and milestones are created and tracked to remediate any concerns. OPM has also grown its cybersecurity capability which will allow us to do onsite technical inspections of contractor networks.

Thank you for this opportunity to testify today and I am happy to address any questions you may have.

Mr. HURD. Thank you, Ms. Seymour.

Mr. Wilshusen, you are recognized for five minutes.

STATEMENT OF GREGORY C. WILSHUSEN

Mr. WILSHUSEN. Chairman Hurd, Ranking Member Cummings, and members of the committee, thank you for the opportunity to testify at today's hearing.

As you know, Federal agencies and their contractors depend on interconnected networks and computer systems to carry out mission-related functions. The security of these networks and systems is vital to maintaining public confidence and preserving our Nation's security, prosperity, and well-being.

Safeguarding Federal computer systems and information, however, is a continuing concern. The number of information security incidents, both cyber and non-cyber, reported by Federal agencies continues to rise, increasing from about 5,500 in fiscal year 2006 to over 67,000 in fiscal year 2014. Similarly, the number of incidents involving personal information more than doubled in recent years, to over 27,600 in 2014.

As discussed with your staff, my testimony today will describe cyber threats affecting Federal and contractor systems, and the challenges in securing them.

Before I begin, Mr. Chairman, if I may, I would like to recognize my esteemed colleagues who were instrumental in developing my written statement. With me today is Larry Crossland, an Assistant Director of Information Security, who led this issue. In addition, Rosanna Guerrero, Lee McCracken, Fatima Jahan, Chris Bazinsky, and Bill Cook, who are all back at the office, also made significant contributions.

Mr. Chairman, the Federal Government and its contractors face an evolving array of cyber threats. These threats can be intentional or unintentional. Unintentional threats can be caused by defective computer equipment, careless or poorly trained employees, or natural disasters that inadvertently disrupt systems.

Intentional threats can be both targeted and untargeted attacks from a variety of sources, including criminal groups, hackers, disgruntled insiders, nations, and terrorists. These sources vary in terms of their capabilities, willingness to act, and motives, which can include seeking monetary gain or pursing an economic, political, or military advantage. In particular, adversaries possessing sophisticated levels of expertise and abundant resources, sometimes referred to as advanced persistent threats, pose increasing risks.

Cyber adversaries have a variety of tools and techniques to perpetuate and perpetrate attacks. These include malicious software, social engineering, phishing, denial of service, zero day exploits, and, in sophisticated attacks, may use a combination of these and other techniques.

The number of cyber attacks vastly increases the reach and impact due to the fact that attackers do not need to be physically close to the victims and can more easily remain anonymous. The risks posed by cyber attacks is heightened by the vulnerabilities in Federal networks and systems.

Specifically, weaknesses in security controls continue to threaten the confidentiality, integrity, and availability of the systems supporting Federal operations. Most major Federal agencies have deficient information security. For fiscal year 2014, 19 of the 24 major agencies reported inadequate information system controls for financial reporting purposes, and inspectors general at 23 of these agencies cited it as a major management challenge.

Federal agencies face several challenges in protecting their systems. These include designing and implementing risk-based information security systems and programs, addressing cybersecurity for building and access control systems, enhancing oversight of contractors providing IT services, improving security incident response activities, responding to breaches of personally identifiable information, and implementing security privacy programs at small agencies.

Underscoring the importance of these matters, we once again designated Federal information security as a government-wide, high-risk area in this year's update to the high-risk report, a designation that has remained in place since 1997. This year we also expanded the area to include protecting the privacy of personally identifiable information.

Until Federal agencies successfully address these challenges, including implementing the hundreds of outstanding recommendations made by GAO and agencies' inspectors general, Federal systems and information will remain at increased and unnecessary risk of unauthorized disclosure, modification, and loss.

Mr. Chairman, Ranking Member Cummings, members of the committee, this concludes my statement. I would be happy to answer your questions.

[Prepared statement of Mr. Wilshusen follows:]

United States Government Accountability Office
Testimony
Before the Committee on Oversight and Government Reform, House of Representatives

For Release on Delivery
Expected at 2:00 p.m. ET
Wednesday, April 22, 2015

CYBERSECURITY

Actions Needed to Address Challenges Facing Federal Systems

Statement of Gregory C. Wilshusen,
Director, Information Security Issues

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

April 22, 2015

GAO Highlights

CYBERSECURITY

Actions Needed to Address Challenges Facing Federal Systems

Highlights of GAO-15-573T, a testimony before the Committee on Oversight and Government Reform, House of Representatives

Why GAO Did This Study

Federal agencies, as well as their contractors, depend on interconnected computer systems and electronic data to carry out essential mission-related functions. Thus, the security of these systems and networks is vital to protecting national and economic security, public health and safety, and the flow of commerce. If information security controls are ineffective, resources may be lost, information—including sensitive personal information—may be compromised, and the operations of government and critical infrastructure could be disrupted, with potentially catastrophic effects. Federal law sets forth various requirements, roles, and responsibilities for securing federal agencies' systems and information. In addition, GAO has designated federal information security as a high-risk area since 1997.

GAO was asked to provide a statement summarizing cyber threats facing federal agency and contractor systems, and challenges in securing these systems. In preparing this statement, GAO relied on its previously published work in this area.

What GAO Recommends

In its previous work, GAO has made numerous recommendations to agencies to assist in addressing the identified cybersecurity challenges.

View GAO-15-573T. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

Federal and contractor systems face an evolving array of cyber-based threats. These threats can be unintentional—for example, from equipment failure, careless or poorly trained employees; or intentional—targeted or untargeted attacks from criminals, hackers, adversarial nations, or terrorists, among others. Threat actors use a variety of attack techniques that can adversely affect federal information, computers, software, networks, or operations, potentially resulting in the disclosure, alteration, or loss of sensitive information; destruction or disruption of critical systems; or damage to economic and national security. These concerns are further highlighted by the sharp increase in cyber incidents reported by federal agencies over the last several years, as well as the reported impact of such incidents on government and contractor systems.

Because of the risk posed by these threats, it is crucial that the federal government take appropriate steps to secure its information and information systems. However, GAO has identified a number of challenges facing the government's approach to cybersecurity, including the following:

- **Implementing risk-based cybersecurity programs at federal agencies:** For fiscal year 2014, 19 of 24 major federal agencies reported that deficiencies in information security controls constituted either a material weakness or significant deficiency in internal controls over their financial reporting. In addition, inspectors general at 23 of these agencies cited information security as a major management challenge for their agency.
- **Securing building and access control systems:** GAO previously reported that the Department of Homeland Security lacked a strategy for addressing cyber risks to agencies' building and access control systems—computers that monitor and control building operations—and that the General Services Administration had not fully assessed the risk of cyber attacks to such systems.
- **Overseeing contractors:** The agencies GAO reviewed were inconsistent in overseeing contractors' implementation of security controls for systems they operate on behalf of agencies.
- **Improving incident response:** The agencies GAO reviewed did not always effectively respond to cybersecurity incidents or develop comprehensive policies, plans, and procedures to guide incident-response activities.
- **Responding to breaches of personally identifiable information:** The agencies GAO reviewed have inconsistently implemented policies and procedures for responding to data breaches involving sensitive personal information.
- **Implementing security programs at small agencies:** Smaller federal agencies (generally those with 6,000 or fewer employees) have not always fully implemented comprehensive agency-wide information security programs.

Until agencies take actions to address these challenges—including the hundreds of recommendations made by GAO and inspectors general—their systems and information will be at increased risk of compromise from cyber-based attacks and other threats.

Chairman Chaffetz, Ranking Member Cummings, and Members of the Committee:

Thank you for inviting me to testify about cyber threats facing federal information systems at today's hearing. As you know, federal agencies and their contractors are dependent on computerized (cyber) information systems and electronic data to carry out operations and to process, maintain, and report essential information. The security of these systems and data is vital to public confidence and the nation's safety, prosperity, and well-being. Safeguarding federal computer systems and the systems that support critical infrastructures—referred to as cyber critical infrastructure protection—is a continuing concern. In February 2015, the Director of National Intelligence testified that cyber threats to U.S. national and economic security are increasing in frequency, scale, sophistication, and severity of impact.[1]

Underscoring the importance of this issue, we have designated federal information security as a high-risk area since 1997 and in 2003 expanded this area to include computerized systems supporting the nation's critical infrastructure. In the 2015 update to our high-risk list, we further expanded this area to include protecting the privacy of personally identifiable information (PII)—that is, personal information that is collected, maintained, and shared by both federal and nonfederal entities.[2]

As discussed with your staff, my testimony today will describe (1) cyber threats facing federal and contractor systems and (2) challenges in securing them, as well as actions needed to address these challenges. In preparing this statement in April 2015 we relied on our previous work in these areas.[3] The reports presenting this work contain detailed overviews of its scope and the methodology we used to carry it out. The work on which this statement is based was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform audits to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions

[1]James R. Clapper, Director of National Intelligence, Statement for the Record on the Worldwide Threat Assessment of the US Intelligence Community for the Senate Armed Services Committee (February 26, 2015).

[2]See GAO, *High-Risk Series: An Update*, GAO-15-290 (Washington, D.C.: Feb. 11, 2015).

[3]See the list of related GAO products at the end of this statement.

based on our audit objectives. We believe that the evidence obtained provided a reasonable basis for our findings and conclusions based on our audit objectives.

Background

As computer technology has advanced, both government and private entities have become increasingly dependent on computerized information systems to carry out operations and to process, maintain, and report essential information. Public and private organizations rely on computer systems to transmit sensitive and proprietary information, develop and maintain intellectual capital, conduct operations, process business transactions, transfer funds, and deliver services. In addition, the Internet has grown increasingly important to American business and consumers, serving as a medium for hundreds of billions of dollars of commerce each year, as well as developing into an extended information and communications infrastructure supporting vital services such as power distribution, health care, law enforcement, and national defense.

Consequently, the security of these systems and networks is essential to protecting national and economic security, public health and safety, and the flow of commerce. Conversely, ineffective information security controls can result in significant risks, including

- loss or theft of computer resources, assets, and funds;
- inappropriate access to and disclosure, modification, or destruction of sensitive information, such as national security information, personally identifiable information (PII),[4] or proprietary business information;
- disruption of critical operations supporting critical infrastructure, national defense, or emergency services;
- undermining of agency missions due to embarrassing incidents that erode the public's confidence in government;
- use of computer resources for unauthorized purposes or to launch attacks on other systems;
- damage to networks and equipment; and
- high costs for remediation.

[4]Personally identifiable information is information about an individual maintained by an agency, including information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, mother's maiden name, biometric records, and any other personal information that is linked or linkable to an individual.

Recognizing the importance of these issues, Congress recently enacted laws intended to improve federal cybersecurity. These include the Federal Information Security Modernization Act of 2014 (FISMA), which revised the Federal Information Security Management Act of 2002 to, among other things, clarify and strengthen information security roles and responsibilities for the Office of Management and Budget (OMB) and the Department of Homeland Security (DHS). The act also reiterated the requirement for federal agencies to develop, document, and implement an agency-wide information security program. The program is to provide security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

In addition, the Cybersecurity Workforce Assessment Act and the Homeland Security Cybersecurity Workforce Assessment Act aim to help DHS address its cybersecurity workforce challenges. Another law, the National Cybersecurity Protection Act of 2014, codifies the role of DHS's National Cybersecurity and Communications Integration Center as the federal civilian interface for sharing information between federal and nonfederal entities regarding cyber risk, incidents, analysis, and warnings. The Cybersecurity Enhancement Act of 2014, among other things, authorizes the National Institute of Standards and Technology (NIST) to facilitate and support the development of voluntary standards to reduce cyber risks to critical infrastructure and to develop and encourage the implementation of a strategy for the use and adoption of cloud computing services by the federal government.

The Federal Government and Its Contractors Face an Evolving Array of Cyber-Based Threats

Risks to cyber-based assets can originate from unintentional and intentional threats. Unintentional threats can be caused by, among other things, defective computer or network equipment, and careless or poorly trained employees. Intentional threats include both targeted and untargeted attacks from a variety of sources, including criminal groups, hackers, disgruntled employees, foreign nations engaged in espionage and information warfare, and terrorists.

Threat sources vary in terms of the capabilities of the actors, their willingness to act, and their motives, which can include monetary gain or political advantage, among others. For example, adversaries possessing sophisticated levels of expertise and significant resources to pursue their

objectives—sometimes referred to as "advanced persistent threats"—pose increasing risks. Table 1 describes common sources of cyber threats.

Table 1: Sources of Cybersecurity Threats

Threat source	Description
Bot-network operators	Bot-net operators use a network, or bot-net, of compromised, remotely controlled systems to coordinate attacks and to distribute phishing schemes, spam, and malware attacks. The services of these networks are sometimes made available on underground markets (e.g., purchasing a denial-of-service attack or services to relay spam or phishing attacks).
Criminal groups	Criminal groups seek to attack systems for monetary gain. Specifically, organized criminal groups use cyber exploits to commit identity theft, online fraud, and computer extortion. International corporate spies and criminal organizations also pose a threat to the United States through their ability to conduct industrial espionage and large-scale monetary theft and to hire or develop hacker talent.
Hackers/hacktivists	Hackers break into networks for the challenge, revenge, stalking, or monetary gain, among other reasons. Hacktivists are ideologically motivated actors who use cyber exploits to further political goals. While gaining unauthorized access once required a fair amount of skill or computer knowledge, hackers can now download attack scripts and protocols from the Internet and launch them against victim sites. Thus, while attack tools have become more sophisticated, they have also become easier to use. According to the Central Intelligence Agency, the large majority of hackers do not have the requisite expertise to threaten difficult targets such as critical U.S. networks. Nevertheless, the worldwide population of hackers poses a relatively high threat of an isolated or brief disruption causing serious damage.
Insiders	The disgruntled organization insider is a principal source of computer crime. Insiders may not need a great deal of knowledge about computer intrusions because their position within the organization often allows them to gain unrestricted access and cause damage to the targeted system or to steal system data. The insider threat includes contractors hired by the organization, as well as careless or poorly trained employees who may inadvertently introduce malware into systems.
Nations	Nations use cyber tools as part of their information-gathering and espionage activities. In addition, several nations are aggressively working to develop information warfare doctrine, programs, and capabilities. Such capabilities enable a single entity to potentially have a significant and serious impact by disrupting the supply, communications, and economic infrastructures that support military power—impacts that could affect the daily lives of citizens across the country. In his February 2015 testimony, the Director of National Intelligence stated that, among state actors, China, and Russia have highly sophisticated cyber programs, while Iran and North Korea have lesser technical capabilities but possibly more disruptive intent.
Terrorists	Terrorists seek to destroy, incapacitate, or exploit critical infrastructures in order to threaten national security, cause mass casualties, weaken the economy, and damage public morale and confidence. Terrorists may use phishing schemes or spyware/malware in order to generate funds or gather sensitive information.

Source: GAO analysis based on data from the Director of National Intelligence, Department of Justice, Central Intelligence Agency, and the Software Engineering Institute's CERT® Coordination Center. | GAO-15-573T

These threat sources make use of various techniques— or exploits—that may adversely affect federal information, computers, software, networks, and operations. Table 2 describes common types of cyber exploits.

Table 2: Types of Cyber Exploits

Type of exploit	Description
Cross-site scripting	An attack that uses third-party web resources to run script within the victim's web browser or scriptable application. This occurs when a browser visits a malicious website or clicks a malicious link. The most dangerous consequences occur when this method is used to exploit additional vulnerabilities that may permit an attacker to steal cookies (data exchanged between a web server and a browser), log key strokes, capture screen shots, discover and collect network information, and remotely access and control the victim's machine.
Denial-of-service/distributed denial-of-service	An attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources. A distributed denial-of-service attack is a variant of the denial-of-service attack that uses numerous hosts to perform the attack.
Malware	Malware, also known as malicious code and malicious software, refers to a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or otherwise annoying or disrupting the victim. Examples of malware include logic bombs, Trojan Horses, ransomware, viruses, and worms.
Phishing/spear phishing	A digital form of social engineering that uses authentic-looking, but fake, e-mails to request information from users or direct them to a fake website that requests information. Spear phishing is a phishing exploit that is targeted to a specific individual or group.
Passive wiretapping	The monitoring or recording of data, such as passwords transmitted in clear text, while they are being transmitted over a communications link. This is done without altering or affecting the data.
Spamming	Sending unsolicited commercial e-mail advertising for products, services, and websites. Spam can also be used as a delivery mechanism for malware and other cyber threats.
Spoofing	Creating a fraudulent website to mimic an actual, well-known website run by another party. E-mail spoofing occurs when the sender address and other parts of an e-mail header are altered to appear as though the e-mail originated from a different source.
Structured Query Language (SQL) injection	An attack that involves the alteration of a database search in a web-based application, which can be used to obtain unauthorized access to sensitive information in a database.
War driving	The method of driving through cities and neighborhoods with a wireless-equipped computer–sometimes with a powerful antenna–searching for unsecured wireless networks.
Zero-day exploit	An exploit that takes advantage of a security vulnerability previously unknown to the general public. In many cases, the exploit code is written by the same person who discovered the vulnerability. By writing an exploit for the previously unknown vulnerability, the attacker creates a potent threat since the compressed timeframe between public discoveries of both makes it difficult to defend against.

Source: GAO analysis of data from the National Institute of Standards and Technology, United States Computer Emergency Readiness Team, and industry reports; and GAO. | GAO-15-573T

An adversarial threat source may employ multiple tactics, techniques, and exploits to conduct a cyber attack. NIST has identified several representative events that may constitute a cyber attack:[5]

- **Perform reconnaissance and gather information:** An adversary may gather information on a target by, for example, scanning its network perimeters or using publicly available information.
- **Craft or create attack tools:** An adversary prepares its means of attack by, for example, crafting a phishing attack or creating a counterfeit ("spoof") website.
- **Deliver, insert, or install malicious capabilities:** An adversary can use common delivery mechanisms, such as e-mail or downloadable software, to insert or install malware into its target's systems.
- **Exploit and compromise:** An adversary may exploit poorly configured, unauthorized, or otherwise vulnerable information systems to gain access.
- **Conduct an attack:** Attacks can include efforts to intercept information or disrupt operations (e.g., denial of service or physical attacks).
- **Achieve results:** Desired results include obtaining sensitive information via network "sniffing" or exfiltration, causing degradation or destruction of the target's capabilities; damaging the integrity of information through creating, deleting, or modifying data; or causing unauthorized disclosure of sensitive information.
- **Maintain a presence or set of capabilities:** An adversary may try to maintain an undetected presence on its target's systems by inhibiting the effectiveness of intrusion-detection capabilities or adapting behavior in response to the organization's surveillance and security measures.

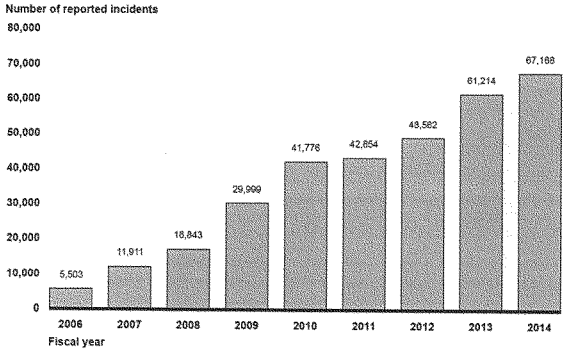
More generally, the nature of cyber-based attacks can vastly enhance their reach and impact. For example, cyber attacks do not require physical proximity to their victims, can be carried out at high speeds and directed at multiple victims simultaneously, and can more easily allow attackers to remain anonymous. These inherent advantages, combined with the increasing sophistication of cyber tools and techniques, allow threat actors to target government agencies and their contractors, potentially resulting in the disclosure, alteration, or loss of sensitive information, including PII; theft of intellectual property; destruction or

[5]NIST, *Guide for Conducting Risk Assessments*, Special Publication 800-30, Revision 1 (Gaithersburg, Md.: September 2012).

disruption of critical systems; and damage to economic and national security.

The number of information security incidents affecting systems supporting the federal government is increasing. Specifically, the number of information security incidents reported by federal agencies to the U.S. Computer Emergency Readiness Team (US-CERT) increased from 5,503 in fiscal year 2006 to 67,168 in fiscal year 2014, an increase of 1,121 percent (see fig. 1).

Figure 1: Incidents Reported to the U.S. Computer Emergency Readiness Team by Federal Agencies, Fiscal Years 2006 through 2014

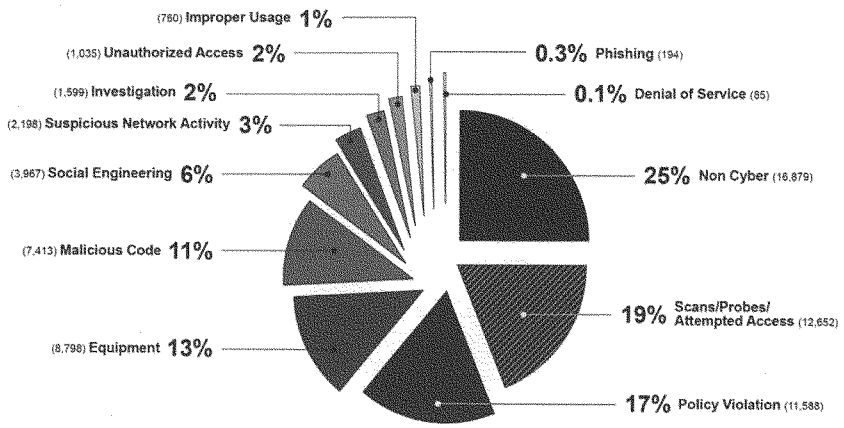


Source: GAO analysis of United States Computer Emergency Readiness Team data for fiscal years 2006-2014. | GAO-15-573T

Similarly, the number of information security incidents involving PII reported by federal agencies has more than doubled in recent years, from 10,481 in 2009 to 27,624 in 2014.

Figure 2 shows the different types of incidents reported in fiscal year 2014.

Figure 2: Information Security Incidents by Category, Fiscal Year 2014



Source: GAO analysis of United States Computer Emergency Readiness Team data for fiscal year 2014. | GAO-15-573T

These incidents and others like them could adversely affect national security; damage public health and safety; and lead to inappropriate access to and disclosure, modification, or destruction of sensitive information. Recent examples highlight the potential impact of such incidents:

- In April 2015, the Department of Veterans Affairs (VA) Office of Inspector General reported that two VA contractors had improperly accessed the VA network from foreign countries using personally owned equipment.
- In September 2014, a cyber intrusion into the United States Postal Service's information systems may have compromised PII for more than 800,000 of its employees.
- According to the Director of National Intelligence, unauthorized computer intrusions were detected in 2014 on the networks of the Office of Personnel Management and two of its contractors. The two contractors were involved in processing sensitive PII related to national security clearances for federal employees.
- In 2011, according to a media report, the Deputy Secretary of Defense acknowledged a significant cyber attack in which a large number of files was taken by foreign intruders from a defense contractor. The deputy secretary was quoted as saying "it is a significant concern that over the past decade, terabytes of data have been extracted by foreign intruders from corporate networks of defense companies" and that some of the data concerned "our most sensitive systems."

The Federal Government Faces Ongoing Challenges in Its Approach to Cybersecurity

Given the risk posed by cyber threats and the increasing number of incidents, it is crucial that the federal government take appropriate steps to secure its systems and information. However, both we and agency inspectors general have identified challenges in the government's approach to cybersecurity, including those related to protecting the government's information and systems. In particular, challenges remain in the following key areas:

- **Designing and implementing risk-based cybersecurity programs at federal agencies.** Agencies continue to have shortcomings in assessing risks, developing and implementing security controls, and

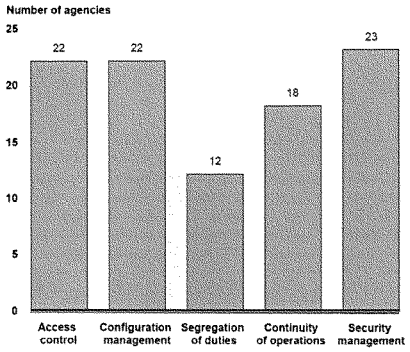
monitoring results. Specifically, for fiscal year 2014, 19 of the 24 federal agencies covered by the Chief Financial Officers Act[6] reported that information security control deficiencies were either a material weakness or a significant deficiency in internal controls over their financial reporting.[7] Moreover, inspectors general at 23 of the 24 agencies cited information security as a major management challenge for their agency. For fiscal year 2014, most of the agencies had weaknesses in five key security control categories.[8] Figure 3 shows the number of the 24 agencies reviewed with weaknesses in each of the five control categories for fiscal year 2014.

[6]The 24 CFO Act agencies are the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; the Environmental Protection Agency; General Services Administration; National Aeronautics and Space Administration; National Science Foundation; Nuclear Regulatory Commission; Office of Personnel Management; Small Business Administration; Social Security Administration; and the U.S. Agency for International Development.

[7]A material weakness is a deficiency, or combination of deficiencies, that results in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected. A significant deficiency is a control deficiency, or combination of control deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance. A control deficiency exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect and correct misstatements on a timely basis.

[8]These control categories are (1) limiting, preventing, and detecting inappropriate access to computer resources; (2) managing the configuration of software and hardware; (3) segregating duties to ensure that a single individual does not have control over all key aspects of a computer-related operation; (4) planning for continuity of operations in the event of a disaster or disruption; and (5) implementing agency-wide information security management programs that are critical to identifying control deficiencies, resolving problems, and managing risks regularly.

Figure 3: Information Security Weaknesses at 24 Federal Agencies Reviewed for Fiscal Year 2014



Source: GAO analysis of agencies, Inspector General and GAO reports as of April 17, 2015. | GAO-15-573T

Over the last several years, GAO and agency inspectors general have made hundreds of recommendations to agencies aimed at improving their implementation of information security controls. For example:

- **Addressing cybersecurity for building and access control systems.** In December 2014 we reported that DHS lacked a strategy for addressing cyber risk to building and access control systems[9] and that its Interagency Security Committee had not included cyber threats to such systems in its threat report to federal agencies.[10] Further, the General Services Administration (GSA) had not fully assessed the risk of cyber attacks aimed at building control systems. We recommended that DHS and GSA take steps to address these weaknesses. DHS and GSA agreed with our recommendations.

[9]Building and access control systems are computers that monitor and control building operations such as elevators; electrical power; and heating, ventilation, and air conditioning.

[10]GAO, *Federal Facility Cybersecurity: DHS and GSA Should Address Cyber Risk to Building and Access Control Systems*, GAO-15-6 (Washington, D.C.: Dec. 12, 2014).

- **Enhancing oversight of contractors providing IT services.** In August 2014 we reported that five of six agencies reviewed were inconsistent in overseeing assessments of contractors' implementation of security controls.[11] This was partly because agencies had not documented IT security procedures for effectively overseeing contractor performance. In addition, according to OMB, 16 of 24 agency inspectors general found that their agency's program for managing contractor systems lacked at least one required element. We recommended that OMB, in conjunction with DHS, develop and clarify guidance to agencies for annually reporting the number of contractor-operated systems and that the reviewed agencies establish and implement IT security oversight procedures for such systems. OMB did not comment on our report, but the agencies generally concurred with our recommendations.
- **Improving security incident response activities.** In April 2014 we reported that the 24 major agencies did not consistently demonstrate that they had been effectively responding to cyber incidents.[12] Specifically, we estimated that agencies did not completely document actions taken in response to detected incidents reported in fiscal year 2012 in about 65 percent of cases.[13] In addition, six agencies we reviewed had not fully developed comprehensive policies, plans, and procedures to guide their incident-response activities. We recommended that DHS and OMB address agency incident-response practices government-wide and that the six agencies in our review improve the effectiveness of their cyber incident response programs. The agencies generally agreed with these recommendations.
- **Responding to breaches of PII.** In December 2013 we reported that eight federal agencies had inconsistently implemented policies and procedures for responding to data breaches involving PII.[14] In addition, OMB requirements for reporting PII-related data breaches were not always feasible or necessary. Thus, we concluded that agencies may not be consistently taking actions to limit the risk to

[11]GAO, *Information Security: Agencies Need to Improve Oversight of Contractor Controls*, GAO-14-612 (Washington, D.C.: Aug. 8, 2014).

[12]GAO, *Information Security: Agencies Need to Improve Cyber Incident Response Practices*, GAO-14-354 (Washington, D.C.: Apr. 30, 2014).

[13]This estimate was based on a statistical sample of cyber incidents reported in fiscal year 2012, with 95 percent confidence that the estimate falls between 58 and 72 percent.

[14]GAO, *Information Security: Agency Responses to Breaches of Personally Identifiable Information Need to Be More Consistent*, GAO-14-34 (Washington, D.C.: Dec. 9, 2013).

individuals from PII-related data breaches and may be expending resources to meet OMB reporting requirements that provide little value. We recommended that OMB revise its guidance on federal agencies' responses to a PII-related data breach and that the reviewed agencies take specific actions to improve their response to PII-related data breaches. OMB neither agreed nor disagreed with our recommendation; four of the reviewed agencies agreed, two partially agreed, and two neither agreed nor disagreed.

- **Implementing security programs at small agencies.** In June 2014 we reported that six small agencies (i.e., agencies with 6,000 or fewer employees) had not fully implemented their information security programs.[15] For example, key elements of their plans, policies, and procedures were outdated, incomplete, or did not exist, and two of the agencies had not developed an information security program with the required elements. We recommended that OMB include a list of agencies that did not report on the implementation of their information security programs in its annual report to Congress on compliance with the requirements of FISMA, as well as including information on small agencies' programs. We also recommended that DHS develop guidance and services targeted at small agencies. OMB and DHS generally concurred with our recommendations.

Until federal agencies take actions to address these challenges—including implementing the hundreds of recommendations made by us and inspectors general—federal systems and information, as well as sensitive personal information about members of the public, will be at an increased risk of compromise from cyber-based attacks and other threats.

In summary, the cyber threats facing the nation are evolving and growing, with a wide array of threat actors having access to increasingly sophisticated techniques for exploiting system vulnerabilities. The danger posed by these threats is heightened by weaknesses in the federal government's approach to protecting federal systems and information, including personally identifiable information entrusted to the government by members of the public. Implementing GAO's many outstanding recommendations will assist agencies in better protecting their systems and information, which will in turn reduce the risk of the potentially devastating impacts of cyber attacks.

[15]GAO, *Information Security: Additional Oversight Needed to Improve Programs as Small Agencies*, GAO-14-344 (Washington, D.C.: June 25, 2014).

Chairman Chaffetz, Ranking Member Cummings, and Members of the Committee, this concludes my statement. I would be happy to answer any questions you may have.

Contact and Acknowledgments

If you have any questions regarding this statement, please contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov. Other key contributors to this statement include Larry Crosland (Assistant Director), Rosanna Guerrero, Fatima Jahan, and Lee McCracken.

Related GAO Products

Information Security: IRS Needs to Continue Improving Controls over Financial and Taxpayer Data. GAO-15-337. March 19, 2015.

Information Security: FAA Needs to Address Weaknesses in Air Traffic Control Systems. GAO-15-221. January 29, 2015.

Information Security: Additional Actions Needed to Address Vulnerabilities That Put VA Data at Risk. GAO-15-220T. November 18, 2014.

Information Security: VA Needs to Address Identified Vulnerabilities. GAO-15-117. November 13, 2014.

Federal Facility Cybersecurity: DHS and GSA Should Address Cyber Risk to Building and Access Control Systems. GAO-15-6. December 12, 2014.

Consumer Financial Protection Bureau: Privacy and Security Controls for Data Collections Should Be Enhanced. GAO-14-758. September 22, 2014.

Healthcare.Gov: Information Security and Privacy Controls Should Be Enhanced to Address Weaknesses. GAO-14-871T. September 18, 2014.

Healthcare.Gov: Actions Needed to Address Weaknesses in Information Security and Privacy Controls. GAO-14-730. September 16, 2014.

Information Security: Agencies Need to Improve Oversight of Contractor Controls. GAO-14-612. August 8, 2014.

Information Security: FDIC Made Progress in Securing Key Financial Systems, but Weaknesses Remain. GAO-14-674. July 17, 2014.

Information Security: Additional Oversight Needed to Improve Programs at Small Agencies. GAO-14-344. June 25, 2014.

Maritime Critical Infrastructure Protection: DHS Needs to Better Address Port Cybersecurity. GAO-14-459. June 5, 2014.

Information Security: Agencies Need to Improve Cyber Incident Response Practices. GAO-14-354. April 30, 2014.

Information Security: SEC Needs to Improve Controls over Financial Systems and Data. GAO-14-419. April 17, 2014.

Information Security: IRS Needs to Address Control Weaknesses That Place Financial and Taxpayer Data at Risk. GAO-14-405. April 8, 2014.

Information Security: Federal Agencies Need to Enhance Responses to Data Breaches. GAO-14-487T. April 2, 2014.

Critical Infrastructure Protection: Observations on Key Factors in DHS's Implementation of Its Partnership Model. GAO-14-464T. March 26, 2014.

Information Security: VA Needs to Address Long-Standing Challenges. GAO-14-469T. March 25, 2014.

Critical Infrastructure Protection: More Comprehensive Planning Would Enhance the Cybersecurity of Public Safety Entities' Emerging Technology. GAO-14-125. January 28, 2014.

Computer Matching Act: OMB and Selected Agencies Need to Ensure Consistent Implementation. GAO-14-44. January 13, 2014.

Information Security: Agency Responses to Breaches of Personally Identifiable Information Need to Be More Consistent. GAO-14-34. December 9, 2013.

Federal Information Security: Mixed Progress in Implementing Program Components; Improved Metrics Needed to Measure Effectiveness. GAO-13-776. September 26, 2013.

Communications Networks: Outcome-Based Measures Would Assist DHS in Assessing Effectiveness of Cybersecurity Efforts. GAO-13-275. April 10, 2013.

Information Security: IRS Has Improved Controls but Needs to Resolve Weaknesses. GAO-13-350. March 15, 2013.

Cybersecurity: A Better Defined and Implemented National Strategy is Needed to Address Persistent Challenges. GAO-13-462T. March 7, 2013.

Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented. GAO-13-187. February 14, 2013.

Information Security: Federal Communications Commission Needs to Strengthen Controls over Enhanced Secured Network Project. GAO-13-155. January 25, 2013.

Information Security: Actions Needed by Census Bureau to Address Weaknesses. GAO-13-63. January 22, 2013.

Information Security: Better Implementation of Controls for Mobile Devices Should Be Encouraged. GAO-12-757. September 18, 2012.

Mobile Device Location Data: Additional Federal Actions Could Help Protect Consumer Privacy. GAO-12-903. September 11, 2012.

Medical Devices: FDA Should Expand Its Consideration of Information Security for Certain Types of Devices. GAO-12-816. August 31, 2012.

Privacy: Federal Law Should Be Updated to Address Changing Technology Landscape. GAO-12-961T. July 31, 2012.

Information Security: Environmental Protection Agency Needs to Resolve Weaknesses. GAO-12-696. July 19, 2012.

Cybersecurity: Challenges in Securing the Electricity Grid. GAO-12-926T. July 17, 2012.

Electronic Warfare: DOD Actions Needed to Strengthen Management and Oversight. GAO-12-479. July 9, 2012.

Information Security: Cyber Threats Facilitate Ability to Commit Economic Espionage. GAO-12-876T. June 28, 2012.

Prescription Drug Data: HHS Has Issued Health Privacy and Security Regulations but Needs to Improve Guidance and Oversight. GAO-12-605. June 22, 2012.

Cybersecurity: Threats Impacting the Nation. GAO-12-666T. April 24, 2012.

Management Report: Improvements Needed in SEC's Internal Control and Accounting Procedure. GAO-12-424R. April 13, 2012.

IT Supply Chain: National Security-Related Agencies Need to Better Address Risks. GAO-12-361. March 23, 2012.

Information Security: IRS Needs to Further Enhance Internal Control over Financial Reporting and Taxpayer Data. GAO-12-393. March 16, 2012.

Cybersecurity: Challenges in Securing the Modernized Electricity Grid. GAO-12-507T. February 28, 2012.

Critical Infrastructure Protection: Cybersecurity Guidance is Available, but More Can Be Done to Promote Its Use. GAO-12-92. December 9, 2011.

Cybersecurity Human Capital: Initiatives Need Better Planning and Coordination. GAO-12-8. November 29, 2011.

Information Security: Additional Guidance Needed to Address Cloud Computing Concerns. GAO-12-130T. October 6, 2011.

Information Security: Weaknesses Continue Amid New Federal Efforts to Implement Requirements. GAO-12-137. October 3, 2011.

Mr. HURD. Thank you, sir.

Dr. Fischer, you are recognized for five minutes.

STATEMENT OF ERIC A. FISCHER

Mr. FISCHER. Good afternoon, Chairman Hurd, Ranking Member Cummings, and distinguished members of the committee. On behalf of the Congressional Research Service, thank you for the opportunity to testify today.

I will try to put what you have heard from prior witnesses in context with respect to both long-term challenges and near-term needs in cybersecurity and the Federal roles in addressing them.

The technologies that process and communicate information have become ubiquitous and are increasingly integral to almost every facet of modern life. These technologies and the information they manage are collectively known as cyberspace, which may well be the most rapidly evolving technology space in human history. This growth refers to not only how big cyberspace is, but also to what it is: social media, mobile devices, cloud computing big data, and the Internet of things. These are all recent developments and all are increasingly important facets of cyberspace. It is difficult to predict how cyberspace will continue to evolve, but it is probably safe to expect the evolution to continue for many years.

That is not to say that all of cyberspace has changed. Basic aspects of how the Internet works are decades old, and obsolete hardware and software may persist for many years. These characteristics of the cyberspace environment present a daunting challenge for cybersecurity, whether for Federal agencies, third-party contractors and vendors, or even the general public.

But design incentives and consensus are also major long-term challenges for cybersecurity. Building security into the design of cyberspace has proven to be difficult. The incentive structure within cyberspace does not particularly favor cybersecurity, and significant barriers persist for developing consensus on what cybersecurity involves and how to implement it effectively.

Furthermore, no matter how important those four challenges are, they do not diminish the need to secure cyberspace in the short-term. That includes reducing risk by removing threats, hardening vulnerabilities, and taking steps to lessen the impacts of cyber attacks. It also includes addressing needs such as reducing barriers to information sharing, building a capable cybersecurity workforce, and fighting cybercrime.

Federal agencies play significant roles in addressing both near-term needs and long-term challenges. Under FISMA, all Federal agencies are responsible for securing their own systems. Private sector contractors acting on behalf of Federal agencies must also meet FISMA requirements. In fiscal year 2014, Federal agencies spent $12.7 billion on those activities, equivalent to about 13 percent of agency information technology budgets.

Now, Federal agencies also have responsibilities for other cybersecurity functions, as summarized in my written testimony. Research and development, along with education, are the two probably most focused on addressing long-term challenges. Others, such as technical standards and support, law enforcement, and regulation focus more on meeting immediate needs.

The Department of Defense, as an example, is responsible for military operations and protection of its own systems, in addition to some other cybersecurity activities. DOD includes the National Security Agency, which is also a member of the intelligence community. DOD has the largest annual investment of any Federal agency both in information technology and in cybersecurity.

The Department of Homeland Security fulfills several cybersecurity functions, developing, for example, new cybersecurity technologies and other tools. It coordinates the operational security of Federal systems under FISMA, including information sharing and technical support. It also plays a significant role in law enforcement related to cybercrime, with DOJ, of course, being the lead agency in that regard.

But perhaps it is best known as coordinating Federal efforts to improve the security of critical infrastructure, most of which is controlled by the private sector. Those activities include information sharing incident response and technical support. Most private sector department activities are voluntary, but DHS also has some regulatory authority for the transportation and chemical sectors.

Now, the role of Federal regulation in cybersecurity has been a significant source of controversy, along with how to remove barriers to information sharing while protecting proprietary and personal information, and the proper roles of different Federal agencies in various cybersecurity activities, including regulation.

With respect to specifically the third-party vendors and contractors, it may be useful to note that a large proportion, roughly half, of recent Federal investment in information technology has been for procurement and acquisition of products and services. In addition, of course, vendors and contractors who provide other kinds of products and services increasingly rely on information technology in their businesses.

Also, I should mention that NIST is in the process of developing guidance for agencies to apply to other non-Federal systems that contain or process controlled, but unclassified, Federal information.

That concludes my testimony. Once again, thank you for asking me to appear before you today.

[Prepared statement of Mr. Fischer follows:]

Statement of Eric A. Fischer
Senior Specialist in Science and Technology
Congressional Research Service

Before

Committee on Oversight and Government Reform
U.S. House of Representatives

April 22, 2015

on

"Enhancing Cybersecurity of Third-Party Contractors and Vendors"

Chairman Chaffetz, Ranking Member Cummings, and distinguished Members of the Committee:

Thank you for the opportunity to discuss issues related to cybersecurity with you today. As the Committee requested, my testimony will provide an overview of the federal role in cybersecurity, current issues and needs, and long-term challenges the federal government faces in this area, including with respect to the roles of third parties.

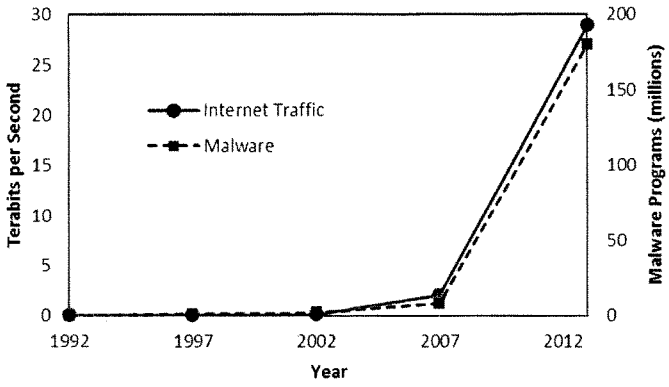
Both the responsibilities and the needs of the federal government with respect to cybersecurity have changed over the last several decades in response to the rapid expansion and evolution of the information technology (IT) industry over that period. The era of mainframe computers began in the 1950s. It was not until the mid-1970s, more than 25 years later, that personal computers began to see widespread use. Internet browser programs and the world-wide web did not appear until the 1990s. Since then, continued, exponential progress in processing power and memory capacity has made IT hardware not only faster, but also smaller, lighter, cheaper, and easier to use. As a result of that and other factors, the last 15 years has seen the rise of cloud computing, big-data analytics, social media, mobile computing, and the Internet of Things.

The original IT industry has also increasingly converged with the communications industry into what is commonly called information and communications technology (ICT). This technology is ubiquitous and increasingly integral to almost every facet of modern society. ICT devices and components are generally interdependent, and disruption of one may affect many others.

Over the past several years, experts and policy makers have expressed increasing concerns about protecting ICT systems from *cyberattacks*—deliberate, unauthorized attempts to access the systems, usually with the goal of theft, disruption, damage, or other unlawful actions. Many experts expect the number and severity of cyberattacks to increase over the next several years. In

fact, over the past ten years, both the amount of global Internet traffic and the number of malicious software programs have grown exponentially (**Figure 1**).

Figure 1. Internet Traffic and Malware



Sources: Internet traffic: Cisco, *The Zettabyte Era: Trends and Analysis*, June 10, 2014, http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/VNI_Hyperconnectivity_WP.pdf. Malware programs: AV-TEST, "Malware Statistics & Trends Report," April 9, 2015, http://www.av-test.org/en/statistics/malware/.

The act of protecting ICT systems and their contents has come to be known as *cybersecurity*. A broad and arguably somewhat fuzzy concept, cybersecurity can be a useful umbrella term but tends to defy precise consensus definition. Generally speaking, it refers to various measures intended to protect ICT components and content—collectively known as *cyberspace*[1]—from cyberattacks. Cyberspace includes computers and other ICT devices, related hardware and software, the networks that connect them, and the information they contain and communicate. Cybersecurity can also refer to the state or quality of being protected from such attacks, or to the broad field of endeavor aimed at implementing and improving protection.

Cybersecurity is also sometimes conflated in public discussion with other concepts such as privacy, information sharing, intelligence gathering, and surveillance. Privacy is associated with the ability of an individual person to control access by others to information about that person. Thus, good cybersecurity can help protect privacy in an electronic environment, but information that is shared to assist in cybersecurity efforts might sometimes contain personal data that at least some observers would regard as private. Cybersecurity can be a means of protecting against undesired surveillance of and gathering of intelligence from an information system. However,

[1] The term *cyberspace* usually refers to the worldwide collection of connected ICT components, the information that is stored in and flows through those components, and the ways that information is structured and processed (CRS Report RL32777, *Creating a National Framework for Cybersecurity: An Analysis of Issues and Options*, by Eric A. Fischer).

when aimed at potential sources of cyberattacks, such surveillance and information-gathering activities can also be useful to help effect cybersecurity. In addition, surveillance in the form of monitoring of information flow within a system can be an important component of cybersecurity.[2]

Overview of Federal Agency Cybersecurity Activities

The federal role in cybersecurity is complex. It involves both securing federal systems and assisting in the protection of nonfederal systems. No single overarching framework legislation is in place, but many enacted statutes—more than 50—address various aspects of cybersecurity.[3] Under the Federal Information Security Management Act (FISMA, 44 U.S.C. Chapter 35, Subchapter II, as amended by P.L. 113-256), all federal agencies have cybersecurity responsibilities relating to their own systems. Responsibility for other cybersecurity functions is distributed among several federal agencies under FISMA and other statutes. Among those functions[4] are the following:

- performing and supporting *research and development* (R&D);
- developing *technical standards*;
- providing *technical support* in cybersecurity to government and private-sector entities, especially critical infrastructure (CI) entities;
- engaging in electronic surveillance and other *intelligence-gathering* activities to detect cyberthreats;
- performing and coordinating *information sharing* to facilitate protection and mitigate the impacts of incidents;
- engaging in investigations of cybercrime and other *law enforcement* activities;
- developing and enforcing federal *cybersecurity* regulations; and
- preparing for and engaging in *cybercombat*.

Figure 2 provides a simplified schematic diagram of major agency responsibilities in cybersecurity. Below is a brief description of roles for selected agencies that may be of interest to the committee, especially agencies with activities that go beyond the requirements of each to secure its own systems. The description is a highly simplified overview of major roles, drawn from various sources. It is intended to provide a basic sketch of functions and responsibilities. Because of the increasing ubiquity of information technology and its merger with communications technology, the increasing complexity of cyberspace, the continuing evolution of agency roles, and the lack of consensus about what specifically constitutes cybersecurity,

---

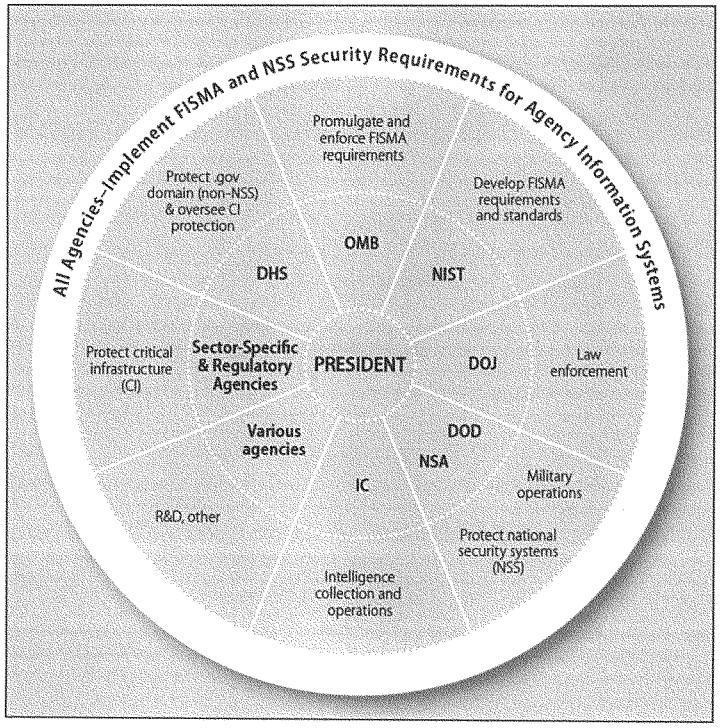
[2] See, for example, Department of Homeland Security, "Continuous Diagnostics and Mitigation (CDM)," June 24, 2014, http://www.dhs.gov/cdm.

[3] CRS Report R42114, *Federal Laws Relating to Cybersecurity: Overview of Major Issues, Current Laws, and Proposed Legislation*, by Eric A. Fischer.

[4] The functions are not necessarily mutually exclusive. For example, development of technical standards often involves R&D.

among other factors, the actual distribution of responsibilities is far more complex and in some ways may be more ambiguous than what is presented here.

Figure 2. Simplified Schematic Diagram of Federal Agency Cybersecurity Roles



Source: CRS

OMB — Office of Management and Budget. Under current law, in addition to its budgetary role in federal cybersecurity efforts, this White House office is responsible for promulgating and enforcing information security requirements under FISMA for federal information systems other than national security systems (NSS) and information systems in the Department of Defense (DOD) and Intelligence Community (IC) agencies that are crucial to their missions.

NIST — National Institute of Standards and Technology. This bureau within the Department of Commerce develops the standards that OMB promulgates under FISMA. It also performs research relating to cybersecurity, develops voluntary guidance, and works with government and private-sector entities to develop cybersecurity best practices.

DHS — Department of Homeland Security. While federal responsibilities for the cybersecurity of non-NSS systems are distributed among several agencies, FISMA, as amended by P.L. 113-256, provides DHS primary responsibility for coordinating the operational security of federal systems.[5] In addition, DHS oversees federal efforts to coordinate and improve the protection of U.S. critical infrastructure (CI), most of which is controlled by the private sector. Some notable DHS cybersecurity programs and activities include the following:

- The Cybersecurity Division of the Science and Technology Directorate,[6] established in 2011, focuses on developing and delivering new cybersecurity technologies and other tools in coordination with public- and private-sector partners.
- The National Cybersecurity and Communications Integration Center (NCCIC),[7] established administratively in 2009 under existing statutory authority to provide and facilitate information sharing and incident response among public and private-sector CI entities. It received specific statutory authorization in P.L. 113-282, the *National Cybersecurity Protection Act of 2014.*
- The National Cybersecurity Protection System (NCPS) and its EINSTEIN component, which provide capabilities for intrusion prevention and detection, analysis, and information sharing for cybersecurity of federal civilian systems.
- The Enhanced Cybersecurity Services (ECS) program, established pursuant to Executive Order 13636, *Improving Critical Infrastructure Cybersecurity,* and through which DHS provides private-sector CI entities with sensitive and classified cyberthreat information either directly or through providers of commercial Internet services.
- The Continuous Diagnostics and Mitigation (CDM) program, which provides products and services to agencies to implement CDM, including sensors, tools, dashboards, and other assistance.

DOD — Department of Defense. DOD is responsible for military operations in cyberspace. That includes both defensive and offensive operations, with the U.S. Cyber Command, under the U.S. Strategic Command, serving as the main focus for coordinating and conducting such activities.[8] DOD agencies such as the Defense Advanced Research Projects Agency (DARPA) and the National Security Agency (NSA) also engage in cybersecurity research and development (R&D). NSA and other DOD agencies also provide assistance upon request to DHS, other civilian

---

[5] The Obama administration had delegated such responsibilities to DHS in 2010 (Peter R. Orszag and Howard A. Schmidt, "Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security (DHS)," Office of Management and Budget, Memorandum for Heads of Executive Departments and Agencies M-10-28, July 6, 2010, http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-28.pdf).

[6] Department of Homeland Security, "Cyber Security Division," January 22, 2015, http://www.dhs.gov/science-and-technology/cyber-security-division.

[7] NCCIC is usually pronounced "En-kick."

[8] CRS Report R43848, *Cyber Operations in DOD Policy and Plans: Issues for Congress,* by Catherine A. Theohary and Anne I. Harrington.

agencies, and private sector entities under various agreements. DOD also offers scholarship opportunities in cybersecurity at selected institutions to recruit and retain qualified personnel.

IC — Intelligence Community. The IC consists of 17 federal agencies and other entities responsible for various forms of intelligence collection and operations, including those relating to cybersecurity.[9] The Director of National Intelligence sets standards for mission-crucial IC systems other than NSS.

NSA — National Security Agency.[10] While NSA is a major component of the IC, it also has a significant cybersecurity mission, serving as the designated manager of national security systems (NSS), which are information and telecommunications systems that are used in military, intelligence, and other national security activities or that handle classified information. This includes the development of security standards. NSA, along with DHS, is also involved in designation of academic centers of excellence in cybersecurity.

DOE—Department of Energy. DOE supports cybersecurity efforts in the energy sector, including electricity and nuclear, for example by assisting private-sector energy companies in developing cybersecurity capabilities for energy-delivery systems. It also provides some cybersecurity services to other agencies and private-sector entities through the DOE National Laboratories and other means. Several of DOE's 17 national laboratories also engage in cybersecurity R&D, education and training, and other activities. These include such things as modeling and simulation of systems and networks, forensic analyses, and providing test beds for investigating and improving the security of industrial control systems.

DOJ — Department of Justice. Most enforcement of federal criminal laws relating to cybersecurity, including investigation and prosecution, is carried out by DOJ. However, some entities within other departments also have enforcement responsibilities, such as the Secret Service in the Department of Homeland Security (DHS), and the Defense Criminal Investigative Organizations within DOD. The duties of law-enforcement agencies often involve computer forensics, electronic surveillance, and other technological activities. The Federal Bureau of Investigation (FBI) leads the multiagency National Cyber Investigative Joint Task Force (NCIJTF), which focuses on information sharing and analysis relating to cyberthreats for law enforcement purposes.

OSTP—Office of Science and Technology Policy. This White House office coordinates and facilitates interagency and multiagency cybersecurity activities, especially R&D.

NSF—National Science Foundation. This independent agency funds research and education in cybersecurity, largely through academic and nonprofit institutions. NSF also provides scholarships to train cybersecurity professionals through its Scholarship-for-Service program, established administratively in 2001 under existing statutory authority and receiving specific statutory authorization in P.L. 113-274.

---

[9] See CRS Report RL33539, *Intelligence Issues for Congress*, by John W. Rollins.

[10] Administratively, NSA is part of DOD but is listed separately because of its unique cybersecurity responsibilities.

SSAs — Sector-Specific Agencies. SSAs are those federal agencies responsible for leading public/private collaborative efforts to protect the 16 designated CI sectors.[11] A plan has been developed for each sector, and many of those plans include discussion of cybersecurity concerns and activities for the different sectors.[12]

Regulatory Agencies. The regulatory environment for cybersecurity is complex, involving both technical and nontechnical activities by various agencies.[13]

Agency Investment in Cybersecurity

As shown in **Table 1**, federal agencies invested a total of $66 billion in IT in FY 2006. That investment had grown to $80 billion in nominal dollars by FY 2014, for an average annual growth rate of 2.7%. The rate of growth in spending on cybersecurity has been several times higher, increasing from $8.3 billion in FY2006 to $12.7 billion in FY2014, for an annual growth rate of 11%.

Table 1. Federal FISMA and Information Technology (IT) Spending
Billions of Dollars, FY2006 to FY2014

Fiscal Year	2006	2007	2008	2009	2010	2011	2012	2013	2014
FISMA Spending	5.5	5.9	6.2	6.8	12.0	13.3	14.6	10.3	12.7
Total IT Spending	66.2	68.2	72.8	76.1	80.7	76.0	75.7	73.2	81.9
FISMA as a Proportion of Total IT Spending (%)	*8.3*	*8.7*	*8.5*	*8.9*	*14.9*	*17.5*	*19.3*	*13.8*	*12.7*

Source: Data on FISMA spending are from annual reports on implementation of FISMA from the Office of Management and Budget (OMB), many of which are available at http://www.whitehouse.gov/omb/e-gov/docs. Data on total IT spending are from OMB Exhibit 53 spreadsheets (see Office of Management and Budget, "Exhibit 53 Archive," *Federal IT Dashboard*, August 31, 2014, https://itdashboard.gov/exhibit53report for recent documents). The first year for which CRS has data on both FISMA spending and IT investment is FY2006, and the most recent is FY2014.

Note: As indicated by the vertical lines, FISMA data for FY2006-FY2009 are not comparable to later data, and data from 2013 are not comparable to earlier data, because of changes in how OMB collected the information (see text). Amounts for both FISMA and IT spending are reported in the documents as "actual" expenditures and therefore probably consist mostly of obligated funds.

---

[11] The White House, "Critical Infrastructure Security and Resilience," Presidential Policy Directive 21, (February 12, 2013), http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

[12] See Department of Homeland Security, "Sector-Specific Plans," 2012, http://www.dhs.gov/files/programs/gc_1179866197607.shtm.

[13] See, for example, Government Accountability Office, *Information Technology: Federal Laws, Regulations, and Mandatory Standards for Securing Private Sector Information Technology Systems and Data in Critical Infrastructure Sectors*, GAO-08-1075R, (September 16, 2008), http://www.gao.gov/assets/100/95747.pdf. The report identified legal cybersecurity requirements associated with specific federal agencies for nine CI sectors, pertaining specifically to securing privately owned information technology systems in those sectors.

The growth rate as shown in the table may be higher than the actual growth because of changes in how data were reported, but it is nevertheless likely that the actual rate of growth in cybersecurity spending has been substantially higher than that in IT investment overall. The large increase from FY2009 to FY2010 and the marked decrease from FY2012 to FY2013 do not appear to reflect actual changes in cybersecurity spending in those years. OMB changed the way it collected the data beginning with FY2010, when it introduced a separate form (Exhibit 53B) on which agencies were required to report detailed FISMA spending.[14] Before that, agencies reported the data as a simple percentage of their overall IT investment.[15] Therefore, data from FY2006 to FY2009 are not comparable to those from FY2010 to FY2013. The amplitude of the reported 75% increase in FISMA spending from FY2009 to FY2010 is almost certainly an artifact of the change in reporting method. It is possible that a real increase occurred, but the size and direction of any change during that period could not be determined. Similarly, the reported decrease of 30% in FISMA spending from FY2012 to FY2013 appears likely to be an artifact largely of additional changes in reporting requirements.[16] According to OMB,

> Prior to FY 2013, government-wide information security spending data was collected using a variety of methodologies, resulting in discrepancies in the figures. Based on conversations among the agencies and with the Hill, there was a decision made to streamline and coordinate the collection and presentation mechanisms to ensure uniformity in the final spending figures.[17]

OMB further stated that because of those changes, "comparisons cannot be drawn between the FY2012 and FY2013 information security spending figures" but that "the approach used in FY2013 will be used again for FY2014."[18] Presumably, out-year data can be meaningfully compared to FY2013 beginning with the FY2014 FISMA report.

Spending on cybersecurity varies greatly among agencies, from less than 5% as a proportion of the agency's total IT investment for nine of the 24 agencies reporting in FY2014 to more than 20% for three of them—DOD (24%), DHS (22%), and DOJ (22%). With DOD's mission responsibilities and its large IT budget, accounting for 46% of total federal IT investment, it is

---

[14] Office of Management and Budget, *Fiscal Year 2010 Report to Congress on Implementation of the Federal Information Security Management Act of 2002*, March 2011, http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/FY10_FISMA.pdf.

[15] Office of Management and Budget, *Fiscal Year 2009 Report to Congress on Implementation of the Federal Information Security Management Act of 2002*, March 2010, http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/FY09_FISMA.pdf.

[16] "Since publishing the FY 2012 FISMA report, OMB has worked internally and with agencies to streamline and improve reporting of this spending information" (Office of Management and Budget, *Annual Report to Congress: Federal Information Security Management Act*, May 1, 2014, 30, http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fy_2013_fisma_report_05.01.2014.pdf).

[17] Allie Neill, Legislative Affairs, OMB, email message to author, November 6, 2014.

[18] Ibid.

not surprising that DOD's spending on cybersecurity accounted for 70% of the federal total in FY2014, compared to 11% for DHS and 5% for DOJ.[19]

There appears to be widespread consensus that the U.S. government, as one of the largest procurers of IT products and services, can and should use its share of that market to leverage improvements not only in federal cybersecurity but across the broader market. A large proportion of federal IT spending is for procurement and acquisition of products and services. For example, in FY2008, from a total investment of $72.8 billion, procurement costs for IT products and services totaled $37.9 billion, about 7% of federal spending on all procurement ($537.8 billion). Half of federal IT products and services overall were procured by the Department of Defense (DOD), followed in order by the Department of Homeland Security (DHS) at 8%, and the General Services Administration (GSA) and the Department of Health and Human Services (DHHS) at about 6% each. About three-quarters of total IT procurement funding consisted of services rather than products.[20]

The 2013 cybersecurity executive order (E.O. 13636)[21] required the General Services Administration (GSA) and Department of Defense (DOD) to make recommendations on including cybersecurity standards in acquisition requirements. Those recommendations covered a range of topics, including acquisition strategies and practices, contract requirements, and training.[22] FISMA also gives agency heads responsibility for ensuring the cybersecurity of "information systems used or operated…by a contractor of an agency or other organization on behalf of an agency" (44 U.S.C. 2554). In addition to its FISMA standards and guidelines for such systems, NIST has also developed a draft publication with recommended requirements for agencies to use in ensuring the protection of controlled but unclassified information residing on nonfederal information systems.[23]

---

[19] The data for NSF is an anomaly, as the agency reported $163 million in FISMA spending for FY2014 but only $101 million in total IT investment. Presumably, this apparent discrepancy is a reporting artifact reflecting NSF expenditures in extramural research, given that the amounts reported for FY2012, before the reporting changes, were $14 million in FISMA spending and $103 million in IT investment.

[20] These figures are from analysis by CRS of data for 2009 from the Federal Procurement Data System (FPDS-NG), https://www.fpds.gov. The funding amounts are for procurement only—they do not include costs for agency personnel. More recent data were not available for this testimony.

[21] Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," *Federal Register* 78, no. 33 (February 19, 2013): 11737 – 11744, http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf. See also CRS Report R42984, *The 2013 Cybersecurity Executive Order: Overview and Considerations for Congress*, by Eric A. Fischer et al.

[22] Department of Defense and General Services Administration, *Improving Cybersecurity and Resilience Through Acquisition*, November 2013, http://www.gsa.gov/portal/mediaId/185367/fileName/IMPROVING_CYBERSECURITY_AND_RESILIENCE_THROUGH_ACQUISITION.action.

[23] Ron Ross et al., *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*, NIST Special Publication 800-171, Final Public Draft, (April 2015), http://csrc.nist.gov/publications/drafts/800-171/sp800_171_second_draft.pdf.

Cybersecurity Issues and Challenges

The risks associated with any cyberattack depend on three factors: *threats* (who is attacking), *vulnerabilities* (how they are attacking), and *impacts* (what the attack does). The management of risk to information systems is considered fundamental to effective cybersecurity.[24]

Threats. People who perform cyberattacks generally fall into one or more of five categories: *criminals* intent on monetary gain from crimes such as theft or extortion; *spies* intent on stealing classified or proprietary information used by government or private entities; *nation-state warriors* who develop capabilities and undertake cyberattacks in support of a country's strategic objectives; "*hacktivists*" who perform cyberattacks for nonmonetary reasons; and *terrorists* who engage in cyberattacks as a form of non-state or state-sponsored warfare.

Vulnerabilities. Cybersecurity is in many ways an arms race between attackers and defenders. ICT systems are very complex, and attackers are constantly probing for weaknesses, which can occur at many points. Defenders can often protect against weaknesses, but three are particularly challenging: inadvertent or intentional acts by *insiders* with access to a system; *supply chain* vulnerabilities, which can permit the insertion of malicious software or hardware during the acquisition process; and previously unknown, or *zero-day*, vulnerabilities with no established fix.

Impacts. A successful attack can compromise the confidentiality, integrity, and availability of an ICT system and the information it handles. *Cybertheft* or *cyberespionage* can result in exfiltration of financial, proprietary, or personal information from which the attacker can benefit, often without the knowledge of the victim. *Denial-of-service* attacks can slow or prevent legitimate users from accessing a system. *Botnet* malware can give an attacker command of a system for use in cyberattacks on other systems. *Destructive* attacks can damage computers and other ICT devices, and if directed at *industrial control systems,* can result in the destruction of the equipment they control, such as generators, pumps, and centrifuges.

Most cyberattacks have limited impacts, but a successful attack on some components of CI could have significant effects on national security, the economy, and the livelihood and safety of individual citizens. Thus, a rare successful attack with high impact can pose a larger risk than a common successful attack with low impact.

Reducing the risks from cyberattacks usually involves (1) removing the threat source (e.g., by closing down botnets[25] or reducing incentives for cybercriminals); (2) addressing vulnerabilities by hardening ICT assets (e.g., by patching software and training employees); and (3) lessening

---

[24] See, for example, National Institute of Standards and Technology, *Managing Information Security Risk: Organization, Mission, and Information System View*, March 2011, http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf.

[25] Botnets are basically a form of distributed computing, in which groups of computers or other Internet-enabled devices, called bots or zombies, perform automated tasks in a distributed manner over the Internet. Some bots are benign, but malicious botnets are a major cybersecurity problem. In such botnets, devices are infected with software that allows a controller, called a botmaster or bot herder, to use the devices in an Internet network for malicious purposes, usually without the knowledge or approval of the owner of the device.

impacts by mitigating damage and restoring functions (e.g., by having back-up resources available for continuity of operations in response to an attack).

Cybersecurity often involves highly technical measures, and the structure of ICT systems and of cyberspace is very complex. Therefore, identifying cybersecurity needs and the means to address them can be difficult. However, several near-term cybersecurity needs appear to be fairly well-established and straightforward. They include, for example,

- preventing cyber-based disasters and espionage by removing threats and hardening systems;
- reducing the impacts of successful attacks;
- improving inter- and intrasector collaboration to protect systems, particularly with respect to information sharing;
- clarifying federal agency roles and responsibilities;
- building and maintaining a capable cybersecurity workforce for both the public- and private sectors; and
- fighting cybercrime.

Many current cybersecurity activities are aimed at addressing these and related needs. More than 200 bills that would address such needs were introduced in the last three Congresses. The 113th Congress enacted five bills that arguably address aspects of several of those needs,[26] including

- amending FISMA to improve the cybersecurity of federal systems;
- updating of agency authorizations for cybersecurity R&D;
- providing for assessment of cybersecurity workforce needs at DHS and enhancing recruitment and retention capabilities; and
- providing statutory bases for a DHS information-sharing program, a NIST public/private partnership effort to develop best practices for CI cybersecurity, and an NSF program for educating cybersecurity professionals.

Bills not enacted included some that would have provided mechanisms to reduce legal and other barriers to information sharing, revised current federal cybercrime law, or provided a federal standard for notification of data breaches of data held by private-sector entities that contain the personal information of individuals.

The immediate and short-term needs discussed above exist in the context of more difficult long-term challenges. The existence of such challenges has been recognized by various observers over many years. For example, the 2008 Comprehensive National Cybersecurity Strategy recognized a need for the development of long-term strategic options and the need to identify "grand

---

[26] In addition to P.L. 113-256, P.L. 113-274, and P.L. 113-282 discussed above, Congress also enacted P.L. 113-246, the *Cybersecurity Workforce Assessment Act*, and P.L. 113-248, the *Border Patrol Agent Pay Reform Act of 2014*. The bills both provide for assessments of the DHS cybersecurity workforce, and the latter provides DHS with new authorities to establish cybersecurity positions and set compensation for them.

challenges" to address difficult cybersecurity problems.[27] The 2011 NSTC strategic plan for cybersecurity R&D recognized the need to develop cybersecurity principles that would endure changes in both technologies and threats.[28] Such challenges can be characterized in many different ways. One approach that may be useful is to characterize a particular set of difficult challenges that could be used to inform longer-term government and private-sector activities. One such set consists of four challenges: design, incentives, consensus, and environment (DICE).

Design. Experts often say that effective security needs to be an integral part of ICT design, not something that is added on toward the end of the development cycle. Yet, developers have traditionally focused more on features than security, largely for economic reasons. Also, many future security needs cannot be predicted with any certainty, posing a difficult challenge for designers.

Incentives. The structure of economic incentives for cybersecurity has been called distorted or even perverse. Cybercrime is regarded as cheap, profitable, and comparatively safe for the criminals. In contrast, cybersecurity can be expensive, is by its nature imperfect, and the economic returns on investments are often unsure. Economic incentives can be influenced by many factors, but one fundamental consideration is the degree to which users demand good cybersecurity as an essential feature of ICT systems and components.

Consensus. Cybersecurity means different things to different stakeholders, with little common agreement on meaning, implementation, and risks. Substantial cultural impediments to consensus also exist, not only between sectors but within sectors and even within organizations. Efforts such as the development of the NIST-led Cybersecurity Framework appear to be achieving some improvements in such consensus. However, one fundamental difficulty is that the increasing economic and societal prominence of cyberspace arises to a significant degree from the ability of ICT to connect things in unprecedented and useful ways. In contrast, security traditionally involves separation. Increasingly, cybersecurity experts and other observers are arguing that traditional approaches such as perimeter defense are insufficient, but consensus on a new conceptual framework has yet to emerge.

Environment. Cyberspace has been called the fastest evolving technology space in human history, both in scale and properties. This rapid evolution poses significant challenges for cybersecurity, exacerbating the speed of the "arms race" between attackers and defenders, and arguably providing a significant advantage to the former. New and emerging properties and applications—especially social media, mobile computing, big data, cloud computing, and the Internet of Things—further complicate the evolving threat environment, but they can also pose potential opportunities for improving cybersecurity, for example through the economies of scale provided by cloud computing and big data analytics. In a sense, such developments may provide

---

[27] The White House, "The Comprehensive National Cybersecurity Initiative," March 5, 2010, http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative.

[28] National Science and Technology Council, *Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program*, December 2011, http://www.whitehouse.gov/sites/default/files/microsites/ostp/fed_cybersecurity_rd_strategic_plan_2011.pdf.

defenders with opportunities to shape the evolution of cyberspace toward a state of greater security.

Legislation and executive actions in the 114th Congress could have significant impacts on those challenges. For example, cybersecurity R&D may affect the design of ICT, cybercrime penalties may influence the structure of incentives, the Cybersecurity Framework may improve consensus about cybersecurity, and federal initiatives in cloud computing and other new components of cyberspace may help shape the evolution of cybersecurity.

Debate about Federal Agency Roles in Improving Cybersecurity

Ongoing debate about the proper role of government in improving cybersecurity may have significant impacts on legislative developments. In general, that debate has mirrored the broader debate about the role of government. Two examples are described below.

Cybersecurity Regulations

For example, some observers have argued that more government regulation of at least some CI sectors is important for improving their cybersecurity, both to provide incentives for implementation of effective cybersecurity measures and guidance for what kinds of protection should be implemented. Proponents have also argued, among other things, that voluntary approaches have not worked well. They also state that CI sectors and subsectors that are already regulated, in particular financial services and electric power, have been largely successful at improving their cybersecurity as a result at least in part of regulatory requirements, and that opposition to such regulations within the sectors is minimal.

Opponents of increased regulation argue, in contrast, that expanding federal requirements would be costly and ineffective, that better mechanisms exist to enhance cybersecurity, and that given the rate of change in the cyber-technology space, increased regulation would in many cases be too inflexible to be useful and may impede innovation and economic growth and the international competitiveness of American companies. In addition, some have argued that the Cybersecurity Framework may provide sufficient incentives and guidance for CI entities to improve their cybersecurity.

Under Executive Order 13636, the Obama Administration required that certain regulatory agencies engage in consultative review of the framework, determine whether existing cybersecurity requirements are adequate, and report to the President whether the agencies have authority to establish requirements that sufficiently address the risks (it does not state that the agencies must establish such requirements, however), propose additional authority where required, and identify and recommend remedies for ineffective, conflicting, or excessively burdensome cybersecurity requirements.

The assessments of regulatory requirements and proposed actions under the order focused on three agencies: DHS, the Environmental Protection Agency (EPA), and the Department of Health and Human Services (HHS). The Administration concluded that "existing regulatory

requirements, when complemented with strong voluntary partnerships, are capable of mitigating cyber risks to our critical systems and information."[29]

Information Sharing

Barriers to the sharing of information on threats, attacks, vulnerabilities, and other aspects of cybersecurity—both within and across sectors—have long been considered by many to be a significant hindrance to effective protection of information systems, especially those associated with CI.[30] Examples have included legal barriers, concerns about liability and misuse, protection of trade secrets and other proprietary business information, and institutional and cultural factors—for example, the traditional approach to security tends to emphasize secrecy and confidentiality, which would necessarily impede sharing of information.

Proposals to reduce or remove such barriers, including provisions in legislative proposals in the last two Congresses, have raised concerns,[31] some of which are related to the purpose of barriers that currently impede sharing. Examples include

- risks to individual privacy and even free speech and other rights;
- use of information for purposes other than cybersecurity, such as unrelated government regulatory actions;
- commercial exploitation of personal information; and
- anticompetitive collusion among businesses that would currently violate federal law.

Research and Development

The need for improvements in fundamental knowledge of cybersecurity and new solutions and approaches has been recognized for well over a decade[32] and was a factor in the passage of the Cybersecurity Research and Development Act in 2002 (P.L. 107-305, H.Rept. 107-355). That

---

[29] Michael Daniel, "Assessing Cybersecurity Regulations," *The White House Blog*, May 22, 2014, http://www.whitehouse.gov/blog/2014/05/22/assessing-cybersecurity-regulations.The document notes that the executive order does not apply to independent regulatory agencies.

[30] See, for example, CSIS Commission on Cybersecurity for the 44th Presidency, *Cybersecurity Two Years Later*, January 2011, http://csis.org/files/publication/110128_Lewis_CybersecurityTwoYearsLater_Web.pdf.

[31] See, for example, Greg Nojeim, "WH Cybersecurity Proposal: Questioning the DHS Collection Center," *Center for Democracy & Technology*, May 24, 2011, http://cdt.org/blogs/greg-nojeim/wh-cybersecurity-proposal-questioning-dhs-collection-center; and Adriane Lapointe, *Oversight for Cybersecurity Activities* (Center for Strategic and International Studies, December 7, 2010), http://csis.org/files/publication/101202_Oversight_for_Cybersecurity_Activities.pdf. See also comments received by a Department of Commerce task force (available at http://www.nist.gov/itl/cybersecnoi.cfm) in conjunction with development of this report: Internet Policy Task Force, *Cybersecurity, Innovation, and the Internet Economy* (Department of Commerce, June 2011), http://www.nist.gov/itl/upload/Cybersecurity_Green-Paper_FinalVersion.pdf.

[32] See, for example, National Research Council, *Trust in Cyberspace* (Washington, DC: National Academies Press, 1999), http://www.nap.edu/catalog/6161.html.

law focuses on cybersecurity R&D by NSF and NIST. The Homeland Security Act of 2002, in contrast, does not specifically mention cybersecurity R&D. However, DHS and several other agencies make significant investments in it, and several of the cybersecurity bills considered by the last three Congresses would have addressed the role of DHS. About 60% of reported funding by agencies in cybersecurity and information assurance is defense-related (invested by DARPA, NSA, and other defense agencies), with NSF accounting for about 15%, and NIST, DHS, and DOE about 5%-10% each.[33]

R&D is generally regarded as one of the less contentious cybersecurity issues. Debate has generally focused on the roles of the agencies involved, priorities relating to specific R&D areas of inquiry, and what are the optimum levels of funding for federal programs.

Other Issues

Other cybersecurity issues that have been considered in recent Congresses include the following:

- **Cybercrime Laws**—updating criminal statutes and law-enforcement authorities relating to cybersecurity. *Controversies:* Adequacy of current penalties and authorities, impacts on privacy and civil liberties.
- **Data-Breach Notification**—requiring notification to victims and other responses after data breaches involving personal or financial information of individuals. *Controversies:* Federal vs. state roles and what responses should be required.
- **Workforce**—improving the size, skills, and preparation of the federal and private-sector cybersecurity workforce. *Controversies:* Hiring and retention authorities, occupational classification, recruitment priorities, and roles of DHS, NSA, NSF, and NIST.

Cybersecurity Bills Enacted in the 113th Congress

Until the 113th Congress, no major cybersecurity legislation had been enacted since 2002. Five bills were signed into law in December 2014 (**Table 2**) addressing aspects of several but not all of the issues discussed above.

They addressed the following issues:

- **Data-Breach Notification:**
  P.L. 113-283 requires OMB to establish procedures for notification and other responses to federal agency data breaches of personal information;
- **FISMA Reform:**
  P.L. 113-283 retains, with some amendments, most provisions of FISMA; also provides statutory authority to DHS for overseeing operational cybersecurity of federal civilian information systems; requires agencies to implement DHS

[33] The percentages were calculated from data in R&D budget crosscuts available at the Networking And Information Technology Research And Development (NITRD) Program, "Supplements to the President's Budget," *NITRD Publications*, 2014, https://www.nitrd.gov/publications/supplementsall.aspx.

directives; requires OMB to establish procedures for notification and other responses to data breaches of personal information;

Table 2. Cybersecurity Bills Enacted in the 113th Congress

Public Law	Bill No.	Title
113-246	H.R. 2952	Cybersecurity Workforce Assessment Act
113-274	S. 1353	Cybersecurity Enhancement Act of 2014
113-277	S. 1691	Border Patrol Agent Pay Reform Act of 2014
113-282	S. 2519	National Cybersecurity and Communications Integration Center Act of 2014
113-283	S. 2521	Federal Information Security Modernization Act of 2014

Source: CRS.

- **Privately Held CI:**
  P.L. 113-274 establishes a process led by NIST similar to that created in Executive Order 13636 to develop a common set of practices for protection of CI;
  P.L. 113-282 provides statutory authority and stipulates responsibilities for the NCCIC, which was established by DHS in 2009 under existing statutory authority to provide and facilitate information sharing and incident response among public and private-sector CI entities; also requires DHS to develop and exercise incident-response plans for cybersecurity risks to CI;
- **Information Sharing:**
  P.L. 113-282 establishes the NCCIC to provide and facilitate information sharing;
- **R&D:**
  P.L. 113-274 requires a multiagency strategic plan for cybersecurity R&D and specifies areas of research for NSF;
- **Workforce:**
  P.L. 113-246 requires an assessment by DHS of its cybersecurity workforce and development of a workforce strategy;
  P.L. 113-274 provides statutory authority for an existing NSF scholarship and recruitment program to build the federal cybersecurity workforce, as well as competitions and a study of existing education and certification programs;
  P.L. 113-277 provides additional DHS hiring and compensation authorities and requires a DHS assessment of workforce needs.

Legislation in the 114th Congress

In the 114th Congress, more than 30 bills have been introduced in the House and the Senate that would address several issues, including data-breach notification, incidents involving other nation-states, information sharing, law enforcement and cybercrime, protection of CI, workforce development, and education. The Obama Administration has released proposals for three bills—on information sharing, data-breach notification, and revision of cybercrime laws. Several bills have received or are expected to receive committee or floor action.

Mr. HURD. Thank you, Dr. Fischer, and thanks to everyone on the panel for your opening remarks.

We will begin questioning with my colleague from Florida, Mr. Mica.

Mr. MICA. Well, thank you, Mr. Chairman.

Let me ask, first, a general question. It appears that there is a fairly significant increase. The information I have is just since 2014 a 15 percent increase in incidents of some of the security risks or incidences. Is that correct, Mr. Scott? So we are seeing a fairly significant increase? Maybe each one of you could tell me what we are seeing overall or what you anticipate we are facing. Is this something that was just the last year or are we now expecting this to continue to increase?

Mr. SCOTT. First of all, I would say my experience in both the private sector and everything I have seen in the public sector would suggest that there has been a steady increase in attacks and incidents over a period of time.

Mr. MICA. But this is fairly accurate, the 15 percent increase just in 2014?

Mr. SCOTT. That sounds reasonable.

Mr. MICA. Security incidents?

Mr. SCOTT. Yes.

Mr. MICA. Ms. Seymour, are you seeing the same thing?

Ms. SEYMOUR. We are seeing an increase, sir, and I would say some of that is due to the fact that we are moving from paper into IT, and as we do that, more of that sensitive information——

Mr. MICA. You have more activity. So you expect more incidents.

Mr. Wilshusen?

Mr. WILSHUSEN. Yes, I would say that is probably reasonable to say 15 percent in fiscal year 2014. The numbers I have on incidents that were reported by Federal agencies to the US–CERT showed about a 10 percent increase.

Mr. MICA. And that is up?

Mr. WILSHUSEN. That is up, yes, for fiscal year 2014 over fiscal year 2013.

Mr. MICA. And Ms. Seymour just said that some of it is because we are shifting from paper to computer and cloud and a whole host of other things.

Mr. WILSHUSEN. Right. I would say over the last nine years or so it has increased over 1,100 percent. It is basically like a stairway, if you will.

Mr. MICA. It is going up.

Mr. WILSHUSEN. Going up and up. And I think there are several reasons for that, one of which might be just agencies are better in terms of detecting and reporting incidents. But I think it also reflects that there is a very active threat environment that is growing, as well as the continued vulnerabilities of Federal systems.

Mr. MICA. And that is going to be the second part of my question, where the risk comes from. You are a little bit ahead of me.

Dr. Fischer, you are also seeing the increase and the basis for the increase. Some they mentioned is that there is more activity, going again to the computer base——

Mr. FISCHER. I guess what I would like to add to what the other witnesses said is that there is certainly consensus that there is a

general increase. Now, with respect to a specific, also, there is a lot of evidence that the rate of increase is actually accelerating; it is not just a certain number per year, but each year those numbers go up. And a number of different measures would reflect that. So basically we can expect continued increase.

Mr. MICA. Continued increase.

Okay, the other thing, too, is the risk, where is the risk coming from. Some risk is State-based. You know, these incidents are being initiated by other States, rogue or whatever, and then rogue, say, individuals who can penetrate the system. Where is the risk coming from that you all see? Let's just go down the line real quick. Mr. Scott?

Mr. SCOTT. It comes from a number of different factors. You mentioned one, State-based.

Mr. MICA. Is that most of it?

Mr. SCOTT. It depends on who the target is.

Mr. MICA. And then most of the risk that we should fear, is it from that, or should it be from rogue operators?

Mr. SCOTT. There are people who want to get PII for monetary gain; there are people who are looking for intellectual property for industrial espionage. There is a wide variety of motivations for this.

Mr. MICA. Again, what poses the biggest risk, the State or the rogue?

Mr. SCOTT. It depends on your area of interest.

Mr. MICA. National security and economy.

Mr. SCOTT. Security and economy I think both industrial espionage and PII and government information are the high risk areas.

Mr. MICA. And the other thing, too, is we are seeing more of the contracts for some of these services go to the private sector, as opposed to in-house Government. Does that pose more of a risk? And are we putting in place means to require that they have in place protections that are adequate when they contract this work out?

Mr. SCOTT. I don't think it, out of necessity, increases the risk as long as good practice and procedures are followed; and that is true whether it is an in-house-run operation or something that is contracted out. So the answer is it will depend on the regime that is going it.

Mr. MICA. Thank you, Mr. Chair.

Mr. HURD. Thank you, sir.

I would like to now recognize Mr. Lynch from Massachusetts for five minutes.

Mr. LYNCH. Thank you, Mr. Chairman.

I also want to just commend my colleague, Mr. Cummings, the gentleman from Maryland. I remember over the past couple of years we had the breaches at JPMorgan and Home Depot and Target, where the gentleman from Maryland asked to have a hearing like this in the face of that breach, and he was denied by the previous chairman.

I know when we had the 800,000 workers that were affected in the U.S. Postal Service breach and the State Department breach, again the ranking member asked to have a hearing on the breaches and cybersecurity then and again we were denied by the previous chairman.

I just want to say that it probably reflects the new leadership, the new chairman, the gentleman from Utah, Mr. Chaffetz, that we are finally addressing this problem, and I think it bodes well not just for the committee and the work we are doing, but also I think for the American people, the people that we are supposed to be protecting. But again I want to thank Mr. Cummings for his leadership on this issue.

I happened to run across a report that was done by the New York State Department of Financial Services, and I would ask unanimous consent that we might enter this into the record, Mr. Chairman.

Mr. HURD. Without objection, so moved.

Mr. LYNCH. Thank you.

[The information follows:]

[This report can be found at: *http://www.dfs.ny.gov/about/press2014/pr140505—cyber—security.pdf]*

Mr. LYNCH. What they did is they went through and they looked at what the banks in New York were doing in the face of a lot of these breaches. This was obviously on the private sector side. And while I understand we are looking at the Federal side, I think that there are some lessons learned here.

I think that the importance of a meaningful sort of public-private partnership on protecting cybersecurity is necessary because so many times the Government is actually relying on third parties in the private sector to protect their information. I think the President pointed out that we have to have a very tight collaboration between banks and financial services companies and third-party vendors.

To this end, I was a little bit shocked by the report of the New York State Department of Financial Services. They examined 40 regulated banking organizations and the report reveals that the Wall Street efforts to mitigate security risks of outside firms leaves great room for improvement, to say the least. While 90 percent of the banking organizations surveyed reported that they have information security requirements in place, the requirements are across a broad spectrum. There were some banks that required data encryption that was in communication, but not data encryption when the information was at rest. So people could hack into the system and get the information that was not encrypted.

Others had access controls, data classification, and disaster recovery plans. In addition, nearly all of the surveyed banking organizations report they have implemented policies that require both initial and periodic review of third-party vendors.

However, less than half of those banks, and there is great reputational risk as well as financial risk for these firms to allow a breach, so they should be motivated, less than 50 percent of these institutions conduct any type of onsite assessments like Ms. Seymour mentioned in her testimony and only 46 percent are required to conduct onsite assessments of so-called high-risk third-party vendors such as check payment processors and trading settlement operations and data processing companies. Only about a third of them are required to conduct periodic onsite assessments of high-risk third-party stakeholders during the life of their entire contract, and those respondents included 50 percent of large institu-

tions reported that they use encryption, again, for data that is in communication, but not when it is at rest.

I suspect that with the motivation that these banks have, they have a larger compliance rate than we do in the Federal Government, and I want to know from you collectively—and I appreciate that you all do great work. Mr. Fischer, CRS is one of our favorite groups; they help Congress enormously. But if the private sector is failing so miserably, what lessons are there for us and what are we doing to try to step up our game to protect the information that the Federal Government has within its custody?

Mr. SCOTT. Thank you. Let me, for context, also describe a little bit of the fact that this is also a moving target. What was satisfactory even two or three years ago is no sort of table steaks in terms of, you know, where you just get started. So I think it is important to recognize that that will likely also continue to be the case.

What we are doing in OMB is we are conducting CyberStat reviews with each of the agencies that asks them to report and, in consultation with us, look at their maturity level across a number of different dimensions, many of which you mentioned; and then we will ask each of the agencies to set goals and we will measure progress against those goals. And each of these have to be a risk-based assessment to start with. So some agencies have different kinds of risks than other ones do. So that is an important part of the work that our unit is doing.

Then the second thing is, through our CIO Council and our CIO counsel, disseminating information and sharing best practices, as well as the guidance that we provide during the normal course of our work.

Mr. HURD. Thank you, Mr. Scott.

I would now like to recognize Mr. Russell from Oklahoma for five minutes.

Mr. RUSSELL. Thank you, Mr. Chairman.

Mr. Scott, in your role as FED CIO, you will have a great deal of influence over IT policies and practices that Federal agencies must implement. Given your role as a technologist and an IT specialist with years of private sector experience, can you give us a general sense of your impression of the State and Federal information security?

Mr. SCOTT. Thank you for the question. So, nine weeks in, it is a little difficult for me to give you a sort of comprehensive answer to that, but what I have observed so far is that there is a range, and that range is dependent on the agency that we are talking about here. It is why we are doing the CyberStat reviews and why we are going through the processes that we are going through. So at the end of that process I hope to have a more comprehensive view across the Federal agency.

That said, I would tell you there is no agency, even the ones that we have looked at so far, who we believe are doing a really good job who would say we are done or we have done enough and it is the end of job. Everyone believes there is more that we can and should do.

Mr. RUSSELL. Thank you for that.

Mr. Wilshusen, the Partnership for Public Service released a report last week that concluded the Federal Government is not well

positioned to recruit a capable cybersecurity workforce. How does recruitment and retention of cyber talent factor in the Government's operational ability to maintain effective cybersecurity?

Mr. WILSHUSEN. Well, clearly, it is one of the underlying causes, to make sure that the Federal Government and Federal agencies have technically competent individuals that help to secure their systems. We did a report a couple years ago to talk to human capital cybersecurity challenges within the Federal Government. What many agencies indicated to us, at least the ones we reviewed, stated that identifying those individuals and retaining them that had the technical security competencies is one of their biggest challenges. They are able to fill many of the other information security type of activities and positions, but those that had the technical capabilities has been a challenge because they are competing against a number of different organizations outside of Government, and those individuals are in somewhat short supply.

Mr. RUSSELL. Ms. Seymour, the Sony hack featured an infrastructure attack, meaning hackers not only stole data, but they also destroyed the network itself. What do you think the motivations of this type of attack are, and do you see that there will be more of this in the future? And, if so, what can we do to protect against it?

Ms. SEYMOUR. Thank you for the question, sir. I think that as we look at the motivations of these adversaries, I think we have to keep in mind that there is a holistic state of protection that we have to put in place. Some of our adversaries are just interested in the data and, in fact, they don't want to destroy the network because they want to set themselves up a way to come back in and get data in the future. Some of them it is just malicious, not for financial gain on themselves, but for denying access and causing the company or the agency a great deal of expense.

So we have to look at security from infrastructure perspective all the way through to our applications and we have to look at it from a user-based perspective as well as to the advanced persistent threats that we have.

Mr. RUSSELL. Thank you.

Dr. Fischer, your knowledge and breadth of so many of these issues, where do you see the threat going as we try to put up these defenses? I mean, they are obviously going to anticipate that. What do you see is the attitude of the attacks and those that will perpetrate them? If we could think forward, where would that go so that we can get ahead of the curve instead of always reacting behind it?

Mr. FISCHER. Well, sir, part of that I think depends on the whole question of the incentive structure that I mentioned. So now often people will talk about, well, who are the threat actors? You have State actors, hacktivists, cyber criminals, maybe some terrorists and a few other sort of classic hackers involved. So they have different motivations and different incentives.

So it seems that it depends, once again, on what the sector is specifically that is being attacked, or the particular agency or entity, what the motivation of the particular attacker is.

I think that one way to think about this is to realize that once the public recognizes that cybersecurity is a critical part of the

value proposition for anything they do, that is going to help greatly ameliorate the situation. And the other challenges I mentioned in my testimony are also important.

Mr. RUSSELL. Thank you for that.

And thank you, Mr. Chairman.

Mr. HURD. Again, I would like to now yield five minutes to Mrs. Maloney, from New York.

Mrs. MALONEY. Thank you, Mr. Chairman and Ranking Member, and all of the panelists today for focusing on this important issue. As we speak, they are debating cybersecurity on the floor. It is one of the few areas where there is a joint cause, a joint goal, and joint cooperation because it is so serious, such a threat to the economy and to privacy and really to our technology and security of our Country.

We, unfortunately, had in 2014 several high-profile data breaches of Federal agencies, breaches really that happened because of the contractors in the case of the Postal Service data breach, where over 800,000 current and former employees had their personal information compromised; and the loss of sensitive personal information of tens of thousands of Federal employees occurred because of data breaches of USIS and KeyPoint, two very large Federal contractors.

So I would like to hear what lessons were learned from these experiences and how it plans to apply those lessons to minimize the risk of these breaches in the future, and we will start with you, Ms. Seymour, from OPM. What are the chief lessons that you learned and how are the contractors cooperating? And anyone else who would like to jump in and add to the chief lessons that we have learned from these unfortunate situations.

Ms. SEYMOUR. Thank you for the question, ma'am. What we learned from those breaches is it is important to have a contractual relationship that is well defined with those contractors. At OPM we had very well defined contract clauses in our contracts, and that helped us have a better conversation with the contractor when the breaches occurred.

Mrs. MALONEY. Well, did you make any changes after these two breaches to make them better with your contracts, with your requirements? Have you made any specific changes?

Ms. SEYMOUR. Yes, ma'am. We have done two things. One is we have reviewed our contract clauses to strengthen them, and the second thing that we are doing is we are reviewing all of our contracts to make sure that we have the appropriate clauses across the board in our OPM contracts.

Mrs. MALONEY. So what are the appropriate clauses? What do you have to get in there to protect the Government in your contracts?

Ms. SEYMOUR. Clauses that require segregation of data. One of the lessons that we learned is that if you have a network where all the data is commingled, then it is very difficult to protect the data, to segregate the data, understand what the adversaries are about and, therefore, protect that information. If the data is well architected and segregated, you have a better chance of understanding what the adversaries are after and putting better protections around it in a very quick manner.

Mrs. MALONEY. Now, who got this information? When USIS and KeyPoint deal, who were the hackers? What was the breakdown?

Ms. SEYMOUR. At OPM, ma'am, we don't assign attribution. So I would have to defer to other agencies who do that kind of work.

Mrs. MALONEY. Okay. But could it happen now? Could it happen again? Or have the changes you made protected information?

Ms. SEYMOUR. First of all, KeyPoint has made numerous changes in their network and we are assessing those changes. OPM, as well, has made tremendous strides in its security and changing the architect of its nature.

Mrs. MALONEY. So you have reduced the risk, right?

Ms. SEYMOUR. Yes, ma'am.

Mrs. MALONEY. But how did you do it? How did you reduce the risk? You separated data. What else did you do?

Ms. SEYMOUR. You put firewalls between your systems so that you can better separate and better protect the information so that when you understand what the adversaries are after, you can strengthen your controls. We also have worked very hard on training for our users. Regardless of the security controls that you have in your network, one phishing attempt and a user clicks on a bad link and contracts malware is very dangerous.

Mrs. MALONEY. Mr. Scott, in your written testimony you indicated that one of the lessons learned from the USIS and KeyPoint data breaches was third-party contractors and vendors were inconsistently implementing protections. Can you explain what cybersecurity protections contractors had been inconsistently implementing?

Mr. SCOTT. It really falls into a couple of areas. One is what we require of the—and I am speaking broadly across a number of contracts across the Federal Government. So what we require in terms of initially our rights to look at and inspect their information security measures, number one.

Also, what they are supposed to do in terms of responding to an incident, the time frames that we allow and who they are supposed to notify. We were inconsistent on some of those activities. And then, thirdly, sorry, I have to look at my notes here. And also who they notify. We were inconsistent on. So when and who they notify.

Mrs. MALONEY. Okay, thank you. Any additional information will have to be sent to me because I am well over my time. Thank you so much.

I yield back.

Mr. HURD. Thank you.

I would now like to recognize the gentleman from Georgia, Mr. Hice.

Mr. HICE. Thank you, Mr. Chairman.

Dr. Fischer, let me begin with you. Just from a general guess or estimation, how often are Federal agencies attacked by nation states?

Mr. FISCHER. Well, that is probably a question that could be more effectively answered by an agency such as NSA because, obviously, a lot of the attacks that happen are not going to be made public once they are discovered. But, obviously, attacks by nation states are considered a very serious concern, particularly for agencies involved in——

Mr. HICE. Well, of course they are, but you wouldn't have any guess? Just generally speaking, I am curious what percentage are we looking at.

Mr. FISCHER. I wouldn't want to give you a number that was inaccurate, but we would be happy to get back to you with that.

Mr. HICE. Okay, if you would, please get back with me on that. Would you have any idea which nation states have been most active in attacking Federal agencies?

Mr. FISCHER. Well, generally speaking, the ones that are identified publicly are nation states like China, and Russia to some extent, and also Iran. You know, the sort of usual players in that regard.

Mr. HICE. Okay. Would those same nation states be responsible for attacking companies as well as Federal agencies?

Mr. FISCHER. Well, there is certainly some evidence to that, at least in some cases. It really depends on what the nation state's motivation is and what they are looking for. So in the case of China, for example, there is an interest in obtaining intellectual property, so there is some evidence that they have, in fact, attacked some private companies.

Mr. HICE. Okay. Would you try to get some more information back to us on that?

Mr. FISCHER. Sure. I would be happy to do that.

Mr. HICE. Mr. Wilshusen, what recommendations has GAO made to various agencies as it relates to management, oversight of contractors in regard to cybersecurity?

Mr. WILSHUSEN. We issued a report last year that addressed this very same issue in terms of overseeing the security controls implemented by contractors of Federal agencies, and we noted that many of the agencies did not have adequate policies and procedures documented in order to provide that level of oversight that was needed and, consequently, particularly with respect of independently assessing the effectiveness of the security controls that are implemented by those contractors, so we made a number of recommendations to agencies that we reviewed to take such actions.

Mr. HICE. Have they been responsive to those recommendations?

Mr. WILSHUSEN. They generally agreed with our recommendations, and that is something that we do follow up on.

Mr. HICE. You do follow up?

Mr. WILSHUSEN. Yes, we do.

Mr. HICE. Okay.

Ms. Seymour, OPM was one of the agencies reviewed by GAO. What steps has OPM taken to improve?

Ms. SEYMOUR. Thank you for the question, sir. Again, we are doing a holistic review of our contracts to make sure we have the appropriate security clauses in them. We have also strengthened those clauses. We have also enhanced our technical capability to do onsite inspections with contractors, and that is a program that is evolving in OPM, and we plan to start that this year.

Mr. HICE. All right, so it is evolving. But is there accountability? You are staying on top of that issue?

Ms. SEYMOUR. Yes, sir, there absolutely is. We have a very well articulated process that we are moving to for continuous monitoring, as opposed to taking an every three year look at security

controls on both our Government networks, as well as the contractor networks.

Mr. HICE. Okay, thank you.

Mr. Scott, let me come to you. The report by GAO last year reported the need for these controls on contractors and oversight thereof, and it was mentioned a while ago you were answering the six Federal agencies were evaluated, five of the six came back being inconsistent in all of this. As a result, there evidently is some confusion, as was brought up. What is being done to resolve the confusion?

Mr. SCOTT. So we will use our regular process to issue guidance for consistent application of the best practices that I talked about earlier. That is probably the main thing that we will do to clarify. And there are requirements even in FISMA that actually help us from a law perspective as well.

Mr. HICE. When can we expect a timetable for implementing all of this?

Mr. SCOTT. I think you should expect in the next few months would be the expectation there.

Mr. HICE. Okay. Thank you.

Thank you, Mr. Chairman.

Mr. HURD. Thank you.

Now I would like to recognize Mr. Cartwright, from Pennsylvania, for five minutes.

Mr. CARTWRIGHT. Thank you, Mr. Chairman.

Over the last few years a number of high-profile network compromises have left the private personal information on literally millions of people exposed, often taken from supposedly secure private sector and Government computer networks. Some of the attacks appear to come from foreign governments, as Mr. Hice was just exploring; some of them simply from criminals.

The highly publicized compromise of JPMorgan Chase's network let the personal information of 76 million households and 7 million small business customers flow out of company servers. Over the past eight years, the private records of nearly 30 million New Yorkers were exposed by data breaches. The USIS and KeyPoint compromises resulted in the theft of sensitive information from the background investigations of nearly 70,000 employees of the Federal Government.

Now, in a lot of compromises like this, what mitigates some of the damage done is data encryption. While it is obviously unfortunate if a company or agency is hacked, employees or customers can take some solace in the fact that, if their data was encrypted, their personal information is not at risk, even though it was exposed. If you can't read it, you can't use it.

Mr. Wilshusen, my question is for you. Over the years, GAO has conducted a number of assessments of cyber issues related to the Federal Government. When agencies do not have encryption policies in place, how does that affect what you are finding in your investigations?

Mr. WILSHUSEN. We would certainly report on that because, indeed, encryption is one of those key controls to help protect the confidentiality and even the integrity of sensitive information. What we often find, too, is even when agencies may encrypt certain

data like credentials and user IDs and that, they may use a lesser form or less secure form of encryption that can still be broken. Even though the information may be encrypted, the algorisms are such that they can be readily broken by competent individuals with the techniques and technologies to do that, so we also make recommendations for agencies to implement encryption in accordance with the current NIST standards.

Mr. CARTWRIGHT. Very good. So it is the quality of the encryption that matters very much.

Mr. WILSHUSEN. It is another factor; first, having encryption, and then making sure it is strong.

Mr. CARTWRIGHT. But then also the consistency of using encryption all the time. My understanding is that private companies and even some Federal agencies are under no pressure to use encryption at all times, even when that data has been determined to be considered sensitive. My question is, again, Mr. Wilshusen, is that true? And what concerns does that create? And is it something Congress should be looking into further?

Mr. WILSHUSEN. Well, it is maybe true with regard to like private sector companies. Unless they are regulated and are required to use encryption, like perhaps certain banks might be required to if they are regulated, but other companies, it would be generally up to their own determination whether or not and their business risk if they deem it appropriate. But they run the risk, as some of the recent incidents have shown, of having sensitive information being compromised and placed at risk.

Mr. CARTWRIGHT. Well, it is not just a question of what is, but it is also what should be. What do you think, does Congress have a role in enforcing and requiring encryption?

Mr. WILSHUSEN. I think Congress has a role in considering those issues and making the determination on whether that is in the best interest given all the potential implications of that. Certainly, it is your prerogative to make that determination and to consider it. Encrypting sensitive data is a basic fundamental security control, and I would certainly recommend that most companies use it to the extent that they have sensitive information that needs protection.

Mr. CARTWRIGHT. How about you, Dr. Fischer? Weigh in on that for us.

Mr. FISCHER. Well, the only thing I would like to add in addition is that it is also important to consider the kind of costs associated with encryption, because why is it that we don't all use encryption at home? Because it can be difficult for us to implement. The same thing can apply in the context of a company or even a Federal agency.

So if the use of encryption seems to basically, while it may help to meet the cybersecurity part of the mission, actually interferes with or perceives to interfere with the operational part of the mission, then often organizations may choose the operational part of the mission. So this raises the whole question about how does one make sure that security is usable. Because if security is not usable, basically people find a workaround.

Mr. CARTWRIGHT. Well, this is a fascinating topic, but I am out of time, so thank you, gentlemen.

I yield back.

Mr. HURD. Thank you.

I would like to now recognize Mr. DeSantis, from Florida, for five minutes.

Mr. DESANTIS. Thank you, Mr. Chairman.

Thank you to the witnesses.

When we have victims of cyber attacks, one of the issues is attribution. Where did this come from? I know that they emanate in Eastern Europe, Russia, China, whatever. So how do the agencies work with Homeland Security, the FBI, and other law enforcement in order to trace attacks back to the source when they happen?

Mr. Scott, do you want to give that a shot?

Mr. SCOTT. Sure. So let me just go through the process. So when an agency discovers there is something going on that they are suspicious about, DHS becomes the agency for the Federal Government that is the first response and deals with that. Then, depending on what they find, they may call in other agencies if there are suspicious of, you know, backers outside the Country or criminals or whatever. So who is called then would depend on what is found after the initial call is made.

Mr. DESANTIS. So that would be the type of thing if it was an attack on someone's bank account, they would inform the Secret Service, let's say?

Mr. SCOTT. Yes, potentially.

Mr. DESANTIS. How are the agencies managing mobile device security? I know that when I was active duty in the military and you put in your CAC card, there are all these encryption certificates, everything. But if someone just has a mobile device and they want to conduct business on that, how do you ensure that that is something that has integrity?

Ms. SEYMOUR. I can tell you from OPM's perspective, sir, what we have done is implemented security appliances so that we don't allow random mobile devices to connect to our network. So all of our mobile devices, my mobile device, is controlled, and there is encryption on the phone so that, if I lose it, my network operation center and security operation center can invalidate that device, wipe the data from it, and it is encrypted while it is on the phone. So those types of appliances and tool sets that we can install on our network are very important; they track every device that is on our network.

Mr. DESANTIS. And if that is not used, then there is more vulnerability to a cyber attack?

Ms. SEYMOUR. Yes, sir. It is very important to understand what is connected to your network, how it is connected to your network, and what the security controls are on those devices that are connected to your network.

Mr. DESANTIS. So there are policies? Are employees limited in what they can download onto the mobile device?

Ms. SEYMOUR. Yes, sir. That is one of the issues that we work through. If it is a Government-issued phone, then we have much more control over that. If it is a privately owned phone and bring-your-own-device type of environment, then we have to work through other issues about we may confiscate that phone or that mobile device for a security incident response, as a for instance.

Mr. DESANTIS. What about are employees are allowed to kind of just do their own email, apart from the Federal Government?

Ms. SEYMOUR. I don't know if I would couch it that way. There are controls that we put in our networks that prevent the bulk download of email, like to a private account. But clearly because of the way we communicate with the private sector and others, if I wanted to forward an email from my work account to my personal account, I may be able to do that in certain networks. But we also have ways of white-listing or black-listing certain addresses that you can't forward things to.

Mr. DESANTIS. Would an employee, if they just had their own email server, could they just use that, or would you make them use the Government system with the protections?

Ms. SEYMOUR. We would make them use the Government system, absolutely.

Mr. DESANTIS. Thanks.

I yield back the balance of my time.

Mr. HURD. The gentleman yields back.

I would like to now recognize the ranking member of the Information Technology Subcommittee, Ms. Kelly, from Illinois, for five minutes.

Ms. KELLY. Thank you, Mr. Chair.

Welcome. Some of the recent major data breaches at Government agencies and Government contractors have specifically targeted personally identifying information, or PII. For example, the U.S. Postal Service data breach, over 800,000 of its current and former employees' personal information was compromised. USIS and KeyPoint contractors that perform background checks for the Federal Government suffered breaches last year also, potentially exposing tens of thousands of Federal employees' personal information.

Mr. Wilshusen, what are some of the challenges agencies face in working with contractors?

Mr. WILSHUSEN. I think there are several challenges. One is, of course, just making sure that contractors and the Federal agencies clearly delineate the roles and responsibilities of each party, one, with respect to implementing security, but also, two, with respect to detecting and reporting on incidents that may occur.

Another challenge is just making sure that the security requirements that contractors are required to follow are in fact clearly communicated. One of the things that is important to know is that the contractors have full knowledge of what the type of security controls they are to implement to protect Federal information, and then, secondly, is to assure that Federal agencies have some assurance that the contractors are effectively implementing those security requirements either through an independent assessment or some sort of assessment that the agency does, because the agency is still responsible for the security of its information even though it may be operated or maintained by a third party.

Ms. KELLY. Thank you.

Mr. Scott, what guidance is provided to agencies on ensuring the security and privacy of personally identifiable information?

Mr. SCOTT. Well, in our guidance, we would require agencies to make sure they are following FISMA, number one. We also, for ex-

ample, are proposing an update to our Web policy requiring encrypted Web traffic, https, it is called, as an example, for Federal public-facing Web sites, and so on. So there are a variety of things that we would do over time, including what I shared earlier, which is best practices in terms of contract language and requirements in contracts to make sure that we have broadly disseminated that across the Federal Government.

Ms. KELLY. Does OMB guidance provide flexibility to agencies depending on the risk assessment of the PII it maintains?

Mr. SCOTT. I think that is a core principle that every agency has to go through, is where are there risks, and clearly that will differ from agency to agency.

When it comes to core PII, though, I don't think there is a lot of difference among the agencies; PII is PII in most cases.

Ms. KELLY. Do you think it is difficult for the Federal Government to recruit and retain qualified cybersecurity personnel?

Mr. SCOTT. I think it is not just a problem for the Federal Government. In my last role, it took nearly six months to find the chief information security officer that we wanted. It was the most exhausting, time-consuming search I think I have done in my professional career. So I would say it is a challenge more broadly than just the Federal Government.

Ms. KELLY. Well, is OMB doing anything special to help agencies find qualified candidates?

Mr. SCOTT. Absolutely. So part of the Digital Services team that I talked about is recruiting people out of the private sector to come spend some time in the Federal Government and, in essence, serve their Country and help us solve some of these big challenges not just in security, but in modernizing our whole IT environment.

Ms. KELLY. I yield back my time.

Mr. HURD. Votes have been called and the intention is to allow Ms. Norton to get through her questions, then we will in recess and pick up the questioning after votes. So, with that, I would like to recognize Ms. Norton, from the District of Columbia, for five minutes.

Ms. NORTON. Thank you very much, Mr. Chairman. I just have a few brief questions.

I am trying to find an industry standard, if you will, because it seems as if both the public and private sector are having the same kinds of problems. Daily news. Both sectors have it. States have it. Everybody has it. In part it is because, whether we face it or not, this technology is relatively new and we still are working our way through it.

I am wondering, don't we contract out most of this work, most of our work to contractors and vendors, as opposed to doing work in-house? I mean, I assume that NASA does work in-house, or maybe they even contract some out. But is most of this work contracted out?

Mr. SCOTT. I think it will vary by agency to the degree to which the work is contracted out, but there are certain kinds of work that lend themselves to contracting out, where there is a broad need and private industry has figured out that they can offer a service that Government can consume.

Ms. NORTON. Now, we in the Federal Government always use competitive bidding, do we not, for this work, as with other work?

Mr. SCOTT. I think that is generally the practice, yes.

Ms. NORTON. Is that the practice in the private sector as well?

Mr. SCOTT. I would say, in my experience, yes, it is very similar to what the Federal Government does in terms of competing, yes.

Ms. NORTON. We often look to the private sector; we say there is real money there, there is real people here. Somebody keeps shareholders by real people, unfortunately. Is there an industry standard beginning to develop anywhere? Is there an industry standard in the private sector which could be useful to the public sector, or are both sectors simply feeling their way through these problems? Yes, sir.

Mr. WILSHUSEN. You mean with respect to cybersecurity controls?

Ms. NORTON. Yes, of course.

Mr. WILSHUSEN. There are several standard-setting organizations that do create standards for information security. One is ISO, International Standards Organization, I believe, or International Organization for Standards. In addition, of course, within the Federal Government, NIST, the National Institutes of Standards and Technology, out of the Department of Commerce, implements or develops and promulgates information security standards, information processing standards for the Federal Government, as well as guidelines that agencies should be following.

Just recently, NIST developed a cybersecurity framework for improving cybersecurity within the critical infrastructure, and this framework identifies a number of different standards or sets of standards that are available to private sector owners and operators of critical infrastructure that they can use to secure their systems.

Ms. NORTON. We have always assumed that the Federal Government had the most secure level of assets and the rest of it have to make sure they are impenetrable. Can any of that cross over to other agencies and help them be more secure in their work?

Mr. WILSHUSEN. Well, I think with regard to the NIST standards and guidelines that it publishes, it often has a public announcement period and it is coordinated with some of the other standards organizations, so there is, I believe, cross-pollination, if you will, among the different standards at some level.

Ms. NORTON. Finally, the Affordable Health Care Act had a lot of glitches, but I haven't heard a lot about a lot of hacking there. Has that been shored up so, kind of information that is there, that that is fairly secure?

Mr. WILSHUSEN. Well, we issued a report last September on the security and privacy of the Healthcare.gov Federal facilitated marketplace and we identified a number of vulnerabilities within that particular system or module of that system. We presently have work ongoing looking at both the security and privacy of some of the State-based health insurance marketplaces, as well as looking at the incidents that have been identified for Healthcare.gov by CMS.

Ms. NORTON. Have they been fairly rare?

Mr. WILSHUSEN. We are still in the process of trying to obtain and collect the information from CMS and review it. We just re-

cently received a listing of the incidents that they have identified and reported to us, and we are in the process of analyzing that. We will be issuing a report later this year.

Ms. NORTON. Thank you.

Mr. HURD. Thank you. Votes have been called on the House floor. The committee will stand in recess to allow members to vote and come back. We anticipate reconvening at the end of the last vote, and we will advise member offices regarding the exact time.

The committee will stand in recess.

[Recess.]

Mr. HURD. I would like to thank you all for being patient. The committee will now reconvene and I would like to recognize the ranking member, Mr. Cummings, for five minutes.

Mr. CUMMINGS. Thank you very much, Mr. Chairman.

Ms. Seymour, I want to thank you for testifying today. I want to thank all of you for testifying.

Every day Government agencies and contractors are the targets of cyber attacks. I wanted to ask you about an attack that happened in 2014. In March of last year, OPM's networks were attacked by a sophisticated cyber threat. At about the same time, USIS, a contractor for OPM that conducts background checks, was also attacked. As I understand it, the attack against OPM did not result in any breaches of personal information, but the attack against USIS did. Is that right?

Ms. SEYMOUR. Yes, sir, that is correct.

Mr. CUMMINGS. So the attack on OPM, the Government agency, was thwarted, but the attack on USIS, the contractor, resulted in the theft of thousands of personal records. Ms. Seymour, we want to learn from this. What protections did OPM have in place that USIS did not?

Ms. SEYMOUR. Thank you for the question, sir. Some of the protections had to do with the architecture that the Government is using versus the architecture that USIS was using. Most of the Government's data is in a mainframe, and in USIS they were in a distributed more modern environment. The adversaries in today's environment are typically use to more modern technologies, and so in this case, potentially, our antiquated technologies may have helped us a little bit.

But I think also it comes down to culture and leadership, and one of the things that we were able to do immediately at OPM was to recognize the problem. We were able to react to it by partnering with DHS and our agencies, their partnering agencies to be able to put mitigations in place to better protect the information.

Mr. CUMMINGS. So those kinds of cyber protections that you had in place at OPM, they are expensive?

Ms. SEYMOUR. Yes, sir, some of them can be expensive. Some of the appliances that you put on a network, firewalls and different software to separate data and to protect it so that it recognizes good traffic in the network from potentially erroneous traffic in the network, those can be expensive. They are expensive sometimes to implement and then sometimes expensive to operate and maintain.

Mr. CUMMINGS. So USIS could have saved money by not investing in those cyber protections, is that right?

Ms. SEYMOUR. What I would offer, sir, is, yes, you can save money by not implementing security, but it is a temporary savings because these vulnerabilities and the breaches that we suffer are expensive to remediate.

Mr. CUMMINGS. Right. Right. So USIS is a subsidiary of a company called Altegrity, and Altegrity owns other subsidiaries that also do business with the Federal Government. On February 11th, 2014, the committee held a hearing with the head of USIS. I asked him about whether Altegrity oversaw these subsidiaries and I also asked him about bonuses Altegrity paid to USIS executives during a four-and-a-half year period when USIS allegedly perpetrated a massive fraud against the Government. In response, he confirmed that Altegrity, in fact, oversaw these subsidiaries and that Altegrity determined those million dollar bonuses. Since then, neither USIS nor Altegrity has answered one single question we have asked them.

So, Ms. Seymour, after you discovered the breach at USIS, was the company fully cooperative in responding to the Government's request for information about the cyber attack? Did they allow Federal cyber officials to investigate the breach of other Altegrity subsidiaries?

Ms. SEYMOUR. The Government was able to negotiate with USIS to allow US–CERT to scan their network and uncover some of the vulnerabilities and propose remediation steps for USIS. We were limited somewhat in our ability to scan the network, or US–CERT was limited in its ability to scan the network, again, because of the architecture of the USIS network, so US–CERT was given permission to scan two of the subnets of that network that they identified.

Mr. CUMMINGS. Chairman's indulgence. I just have one more question.

Ms. Seymour, after the breach and the discovery of the alleged—let me go back to what you just said. Were you able to accomplish everything you wanted to accomplish with regard to USIS? I take it that you didn't get everything that you wanted.

Ms. SEYMOUR. It is difficult. Again, the way the network was architected. I can give you an example, if I might. If you ask me to physically secure an apartment building, but you only allow me to go into two apartments, I can't tell you what is in those other apartments. Clearly, they are part of the building that you have asked me to secure.

Mr. CUMMINGS. Yes, I got it.

Ms. SEYMOUR. Okay.

Mr. CUMMINGS. So, in answer to my question, you didn't get everything you wanted.

Ms. SEYMOUR. We were not able to go to the boundaries of the network, sir.

Mr. CUMMINGS. And, Ms. Seymour, after the breach and the discovery of the alleged fraud, OPM decided not to renew its contract with USIS. But I recently learned that the company may be planning legal action. Have you seen any signs that Altegrity or USIS might bring a lawsuit against OPM?

Ms. SEYMOUR. I am not privy to any of that information, sir. I have no knowledge.

Mr. CUMMINGS. So after failing to protect the personal data of tens of thousands of people, after not fully cooperating with the Government after the breach, after refusing to answer Congress's questions, now Altegrity may be planning to sue. There are serious questions about how Altegrity has been conducting business with over $2 billion in taxpayer funds it has received. I think we should pursue answers directly from Altegrity, and I will bring that up with the chairman.

Mr. Chairman, thank you very much.

Mr. HURD. Thank you, Ranking Member Cummings.

I would like to recognize myself for five minutes.

The first question I have is to you, Mr. Scott. One, thank you for being here today. Like you, I think I have been here for four weeks longer than you have in this position, and having come out of the private sector most recently, trying to get our hands around what is really going on, and one of the interesting things that I find is that some very basic questions, the Federal Government, we haven't answered them.

If North Korea launched a missile at San Francisco, we know how we would respond; the North Koreans know how we would respond. That is a physical-on-physical attack. A digital-on-physical attack, we have a little bit example of that, that Stuxnet from a couple years ago. But what is a digital-on-digital attack? What reaches the level of a digital act of war?

Who is having these conversations? How are we going to go about answering some of these questions? I would really just like your insight on those issues and how we are going to come to some resolution as a whole of Government.

Mr. SCOTT. Well, I think those kinds of questions actually are, frankly, outside the purview of OMB; they are really National Security questions and DOD kinds of questions, so in the few weeks that I have been here, I just haven't been engaged in sort of that conversation, although, like you, I am curious about the answers to those and I do think policy things are going to have to be worked out over some time. It is pretty clear to me that there are somewhat fuzzy lines in that space.

Mr. HURD. Thank you. One of the things that this committee as a whole and my Subcommittee on Information Technology specifically is going to be looking at the continued implementation of FISMA from 2014, and I am interested on your thoughts on where the guidance to all the agencies and departments on implementation of FISMA is and when can we expect some of that guidance.

Mr. SCOTT. Thank you for that question. As you know, the FISMA law passed in the 2014 year and, since then, we have been taking the actual law and putting it through our OMB process in terms of figuring out what guidance we will issue to the various Federal agencies and so on. That work is well underway, so I think in the next several months you will see the specific guidance that we issue with regard to FISMA.

Mr. HURD. Thank you.

Mr. SCOTT. And we tend to do annual updates of that, so you will see ongoing updates as time passed as well.

Mr. HURD. Excellent. Thank you.

The next question is to you, Ms. Seymour, to follow up on some of the questions that Mr. Cummings had. You had mentioned that US–CERT was limited in their ability to scan the network of USIS. Why was that?

Ms. SEYMOUR. I can't answer that, sir, on behalf of USIS.

Mr. HURD. So in your role, and this is not you specifically, but you as the CIO of OPM, do you have enough authority to mandate something like that happen?

Ms. SEYMOUR. Within my own agency, sir?

Mr. HURD. Within your own agency.

Ms. SEYMOUR. Yes, I do. I have excellent leadership with Director Archuleta, and I do feel I have appropriate authority.

Mr. HURD. What about if it comes to a subcontractor that your agency is employing?

Ms. SEYMOUR. Again, I would defer to the contracting officer and I would work with the contracting officer to make sure that the appropriate clauses are in there, and that would guide the discussions that we would have with the contractor.

Mr. HURD. But as of right now, if you walked in and said I want to see this part of the network scanned, I want to do a vulnerability assessment of a certain part of the network that is being managed by a subcontractor, you would have the authority to be able to do that?

Ms. SEYMOUR. I think that there are a lot of questions there that we would probably engage with the contracting officer and legal counsel. I would like to take that question and get you a more complete response because I think there are a lot of factors there that play into that.

Mr. HURD. No, I appreciate that. One other issue. I know we are talking about FISMA here today, but at some point we will probably talk about FITARA. And I know this is something that was good legislation that was passed last year. I think it is pretty insane that the Federal CIO doesn't have complete jurisdiction over certain elements of the networks that you are tasked to protect, and that is unfortunate. So we will be looking at the implementation of that.

I know Mr. Connolly, my colleague, is very interested in that, since he was part of the group that passed the legislation in the last cycle, so I appreciate you all being here.

With that, I would like to recognize Mr. Connolly for five minutes.

Mr. CONNOLLY. I thank the chair and I thank him for his kind remarks.

By the way, I would be glad to work with you. We tried to actually codify the role of CIO and CTO in the Federal Government along the lines originally proposed by the President. We were unsuccessful in that effort the first try, so I would be glad to work with you, because while some of this is by executive order, that does not necessarily survive a particular president. I do think we need to rationalize the hierarchy of responsibility in the Executive Branch, so hopefully we can work with the Executive Branch.

This was early on and maybe didn't have the full attention of the Administration at the time, but, at any rate, I would be glad to work with the chairman, if he is interested in pursuing that legis-

latively. And I thank him again for his kind remarks. FITARA, although here at the Oversight and Government Reform Committee, we prefer to call it Issa-Connolly.

So let me start. Mr. Scott, how would you assess plans for the implementation? There are a lot of elements of the reform bill and we, as you know, intended it not to be another pain in the neck overlay of responsibility that you have to report and do all that. We actually want it to be transformative. We want it to be a management tool for actually achieving efficiency, helping with the management structure, and looking at different ways to harness the power of technology to transform.

Could you briefly just bring us up to date from your perspective, and you are new, how well organized are we and how sincere is the energy within OMB to, in fact, us it as such?

Mr. SCOTT. Thank you for the question. I think the energy level is high, and it has certainly been the subject of a lot of work that my team in particular has been working on over the last several months. Through the process that we have used, we have also had a very high level of engagement with agency CIOs, former CIOs who have had experience in the Government, members of your team and others, who have all, I think, provided great perspective not only on the intent of FITARA, but some of the practical aspects of implementing. Among those are not every agency is the same, so there are cases where flexibility is going to be needed, while still retaining the absolute intent of the law, which is to have greater accountability and responsibility on the part of the CIO.

We are about ready to enter a public comment period where we think we will get additional insight on that, so we look forward to, in a few weeks after the public comment period, closing it out and issuing our guidance. But, in summary, I would say I feel really good about where we are and where we are going, and I appreciate all the support that you and your team have provided for this.

Mr. CONNOLLY. And as I indicated to you in the break while we were voting on the floor, we would like to work with you, and with your office as well, Ms. Seymour, in particular, about implementation and how we are doing and looking at milestones, because we want to use oversight hearings to prod, but also to enhance and augment what you are doing.

Ms. Seymour, there is a role, it seems to me, obviously, for OPM, especially in sort of helping to rationalize the current structure we have. Now, if you go to a major corporation and you ask, no matter how big, how many CIOs do you have, they look at you kind of strange and say, one. Believe me, I have done this in my district. It doesn't matter how big or small, the answer is always the same: one.

Now, over 24 Federal agencies, we have 250 people with the title CIO, and we didn't, by fiat, say thou shalt only have one, but we created a series of incentives in the bill to give you the tool to help rationalize that system and make sure that there is one CIO vested with the authority, the responsibility, the accountability, the flexibility to help engineer these reforms.

Could you comment on that? Because I have to tell you, from the private sector point of view, the Federal Government is not well organized, just that anecdote about how many CIOs we have, frank-

ly, to effectuate the kind of management change we need to to be more efficient. What is OPM doing to try to take advantage of the new law in that respect?

And I know my time has just expired, Mr. Chairman. I appreciate the indulgence just for a second. Thank you.

Ms. SEYMOUR. Thank you for the question, sir. We work very closely, I work very closely with Mr. Scott and the CIO Council. I think that that is an avenue where we can share ideas, share lessons learned, where we can, by any other title, whether it is CIO, Director of IT, any other title, where we need to come together and share and put in place policies that we can then implement throughout the Federal Government. I would say that the Federal Government is probably more complex and diversified than most private sector companies, so I think that we have to work together across these sectors.

So in that construct we can, and we also need to make sure that we are not just working within the CIO Council, but that we work with the other councils as well, the Chief Acquisition Officer Council and the Chief Human Capital Officer Council. And when you get the proper C-suite folks together, you really get a lot of knowledge, expertise, and leadership to move our efforts forward.

Mr. CONNOLLY. I look forward to talking more to you about that.

Would the chairman just allow either GAO or CRS, or both, just to comment? And I am done. But I didn't want to shut them out because I know they have views as well, and GAO has been very supportive of FITARA, otherwise known as Issa-Connolly.

Mr. WILSHUSEN. Yes, sir. That work with FITARA was actually done by another director, but one thing I would like to comment on as far as a corollary, we are beginning to start an engagement that will be looking at the role of CISOs, Chief Information Security Officers, and their authorities, which, while of course not necessarily pertaining to FITARA in the role of the CIO, has some other interesting aspects to just what extent that the CISOs have authorities throughout their organizations and across the Federal Government.

Mr. HURD. Dr. Fischer?

Mr. FISCHER. I don't have any specific comments with respect to FITARA, but I would like to say we do have people who are sort of more specifically focused on this area, and we would be happy to follow up with you to answer any questions you may have.

Mr. HURD. Thank you.

Mr. CONNOLLY. Thank you, Mr. Chairman.

Mr. HURD. Thank you. And I do look forward to working with you over these next couple of weeks and months on FITARA and how we can make sure the Federal Government is doing the things that it is supposed to be doing.

I want to thank the witnesses for your appearances here today. I appreciate you all being flexible. This is a conversation we could sit here for the next three days and just scratch the surface. I look forward to future conversations with you all and get a little bit more into the nitty-gritty on these issues. And I do think this is one of those areas where the House, the Senate, and the White House can work together to make sure that we are protecting the digital infrastructure of the Federal Government and doing every-

thing we can to help the private sector protect themselves. So I look forward to working with you all.

With that, if there is no further business, the committee stands adjourned.

[Whereupon, at 5:12 p.m., the committee was adjourned.]

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

To: Ms. Seymour
Chief Information Security Officer
Office of Personal Management

From: Mr. Chaffetz
Chairman
Committee on Oversight and Government Reform

April 22, 2015 Full Committee Hearing
"Enhancing Cybersecurity of Third-Party Contractors and Vendors"

1. As we understand it, at the time of the cyberattack on USIS, the company's systems met or exceeded FISMA requirements. In fact, as we understand it, the Office of Personal Management (OPM) visited the company in May and did not detect any signs of a cyber-attack, even though we now know one was active at the time. We also understand OPM did not alert the company that it had recently suffered its own cyber-attack.

Please explain to the Committee:

2. Whether or not the facts above, as stated, are accurate.

OPM: The U.S. Office of Personnel Management (OPM) cannot attest to whether or not U.S. Investigative Services (USIS) met or exceeded Federal Information Security Modernization Act[1] (FISMA) guidance. The contract required that USIS complete a Security Assessment & Authorization (SA&A) prior to the transfer of any OPM data to USIS, which included USIS's security assessment in accordance with the FISMA, Office of Management and Budget (OMB) policy, and National Institute of Standards and Technology (NIST) guidelines. The Authority to Operate (ATO) was signed on December 20, 2012 based on the SA&A provided by USIS. The most recent OPM onsite assessment was conducted in May 2014 and July 2014 to validate a sample portion of the FISMA controls. The contract did not require USIS to submit to a comprehensive technical review of the FISMA guidance, and thus no such review was conducted during the onsite visit (see question #5).

3. Was OPM contractually obligated to share the cyber threat information regarding the cyberattack it suffered in the spring of 2014 with USIS or other contractors responsible for keeping personally identifiable information?

OPM: OPM did not disclose to USIS that OPM systems had been breached in March 2014. In our opinion, there was no contractual requirement that OPM notify USIS of the breach.

4. If OPM had shared the threat information from the 2014 network breach could it have prevented or minimized the subsequent cyberattacks against USIS and KeyPoint?

[1] Prior to December of 2014, guidelines referred to in this response were governed under the Federal Information Security Management Act of 2002.

OPM: The nature of the network breaches was different and thus knowledge of the March 2014 incident would not, in our view, have prevented the subsequent cyberattacks against our contractors. In fact, the USIS breach, which began in April 2013, preceded the OPM breach, which began in November 2013. Additionally, we understand that USIS did not have a technical solution for capturing the indicators of compromise (IOCs) and then scanning its network for these IOCs, and thus we believe that USIS would likely not have been able to use the information, had it been provided, to search for adversarial activity on its network.

5. In your oral testimony you noted that one of the "lessons learned from this year" was to strengthen OPM's relationship with contractors through contracting clauses. You cited "security assessment[s]" as an example of strengthening OPM's relationship with contractors.
    a. Was this not a common practice prior to the 2014 breaches of OPM's network, USIS, and KeyPoint?

OPM: Prior to the USIS cyber intrusion, OPM included a set of clauses in its contracts that included IT requirements which mandated that contractors perform a security assessment in accordance with FISMA guidance and NIST standards. Our contractors were also required to perform an SA&A, which includes documenting their IT systems and how the security controls are implemented. OPM is strengthening its contract clauses regarding incident analysis and response to reduce the issues encountered with having US Computer Emergency Readiness Team (US-CERT) investigate contractor networks and systems. Additionally, the contract clauses are being modified to permit technical analysis of the contractor network and systems as part of the periodic onsite reviews (see question #2). To ensure OPM's appropriate identification of these IT requirements, OPM developed a process to identify and review all contracts involving sensitive data sharing to assess them for potential updating with new IT provisions as necessary. This process is ongoing. OPM has been sharing lessons-learned with other agencies.

    b. Additionally, what does a "security assessment" specifically entail?

OPM: An SA&A is a periodic review and documentation process, in accordance with the Cybersecurity Framework developed pursuant to Executive Order 13636 (the framework for the Continuous Diagnostics and Mitigation program at the Department of Homeland Security), as well as FISMA guidance and NIST standards. The SA&A assesses and documents compliance with these requirements.

6. Has the government, or OPM specifically, previously punished any contractor that self-reported a cyber-attack?

OPM: OPM is not aware of any such instance. OPM wishes to be clear that its decision not to exercise the USIS contract options was not a punishment of USIS. The OPM Contracting Officer (CO) reviewed all the available facts and determined that it was not in the Government's best interest to renew USIS's contracts. The decision to exercise or not exercise a contract

option is managed in accordance with the Federal Acquisition Regulations (FAR) 17.207. The exercise of an option is solely at the discretion of the Government, must be based on sound business judgment, and is not punitive.

7. Do you have any concerns about how this action might cause other contractors to think twice about reporting cyber-attacks?

OPM: OPM's contract with USIS required that any such attacks be reported. All contractors are required to comply with the terms and conditions of their respective contracts with OPM.

8. Is it accurate that US-CERT performed only a "short on-site engagement" that did not encompass "a complete analysis of the entire environment"?
    a. If so why?

OPM: This question is best answered by the U.S. Department of Homeland Security (DHS)/US-CERT.

To: Ms. Seymour
Chief Information Security Officer
Office of Personal Management

From: Representative Cummings
Ranking Member
Committee on Oversight and Government Reform

April 22, 2015 Full Committee Hearing
"Enhancing Cybersecurity of Third-Party Contractors and Vendors"

1. At the hearing, I asked a question concerning the differences between the data breach OPM sustained in 2014 and the data breach USIS sustained in that same year. The question was as follows, "What protections did OPM have in place that USIS did not?" Will you clarify your response and describe any consequential differences that existed between OPM's and USIS' networks including, but not limited to, system architecture, network segmentation, security connections, and VPN encryption?

OPM: OPM understands that the USIS network was not segmented from the networks of its parent company (Altegrity) and sister companies (Kroll Advisors, Kroll Ontrack, and Hire Right), thus the Altegrity network was one logical network. While both the USIS and OPM networks were relatively flat, meaning without significant segmentation, the OPM network boundaries were better defined, whereas the boundaries of the USIS network were not defined. Additionally, a system administrator in any of the USIS, parent or sister company networks, was a system administrator throughout the USIS network. This meant that once a system administrator account was compromised, the adversary could access freely the other networks. This type of architecture and practice of broad system administrator privileged access control significantly exposes the entire network and all data on the network. USIS did not have an intrusion detection system (IDS) which means that it was not able to detect an intrusion and then capture information to analyze the attack. Additionally, USIS did not adequately capture log information which made it difficult, if not impossible, to analyze the damage caused during the attack. Finally, USIS did not have an established security operations staff nor did it have appropriate security tools, such as a security incident and event management (SIEM) tool that collects logs and alerts.

2. With respect to the above question, please contrast the consequences of those respective data breaches, including the amount of information cyber attackers were able to obtain.

OPM: Because OPM's network was better defined, meaning there were clear boundaries, it was easier for OPM to understand the traffic (and information) that was coming in, and going out of, its network. Because the USIS network was not well defined, meaning there was no segmentation between the USIS network and the networks of its parent and sister companies, it was impossible to identify and understand appropriate traffic (and information) that was coming in, and going out of, its network. This was especially critical for USIS since Altegrity has offices in foreign countries. The network architecture and the traffic to foreign countries made it

impossible to distinguish normal business operations from potential adversarial activity. Also, because there was no segmentation of the network, meaning firewalls between systems, the entire network (and all information) was exposed to the adversary. Additionally, a system administrator anywhere in the network, meaning USIS or its parent or sister networks, had access to all information on the network. This practice of broad privilege for system administrators significant increases the exposure of information to the adversary when a system administrator account is compromised.

3. At the hearing, I also asked whether USIS and its parent company, Altegrity, were "fully cooperative in responding to the government's request for information about the cyber attack?" and whether OPM was able to "get everything [it] wanted" when attempting to assess the breach at USIS. Will you clarify your response by addressing the following related questions:

    a. In its investigation of the USIS breach, did the government want to inspect Altegrity's subsidiaries, including Kroll Advisors, Kroll Ontrack, and Hire Right? If so, why did you want to assess the networks of those subsidiaries, and what, if any, conclusions were you able to reach?

OPM: Because the boundaries of the USIS network were not well defined, the Government wanted to inspect additional subnets of the network, which would have included Altegrity, Kroll Advisors, Kroll Ontrack, and Hire Right, to ensure adversarial activity was contained and had ceased. USIS restricted its Request for Technical Assistance (RTA) with US-CERT to two subnets of the hundreds of global subnets comprising the network. As a result, the Government was unable to discern if there might be ongoing adversarial activity in the other networks that could immediately re-infect the USIS network. Additionally, inspection of those other networks may have yielded forensic evidence that could have been useful in understanding the adversary's tools, tactics and procedures. This information could then be used to protect the rest of the Federal government and private industry.

    b. Was the federal government given access to all suspected networks, including those of other Altegrity subsidiaries?

OPM: No. The Request for Technical Assistance (RTA) provided by USIS to US-CERT was limited to two subnets of the Altegrity network. Given the architecture of the Altegrity network, all subnets of the network were considered suspect and the Government wanted to inspect them for malicious activity and vulnerabilities.

    c. Did USIS/Altegrity deny the federal government any access it was seeking? What were the reasons stated for the denial? If the denial was communicated in writing or via electronic communication, please provide a copy of that written or electronic communication.

OPM: This question is best answered by the U.S. Department of Homeland Security (DHS)/US-CERT.

4. What factors went into the decision by OPM's contracting officer not to renew the agency's contract with USIS in September 2014? When answering this question, please provide a copy of any written analysis by OPM that outlines the reasons the agency opted to not renew the USIS contract, as well as any written communication the agency made to USIS concerning the decision to not renew the contract.

OPM: The OPM CO decision not to renew the agency's contracts with USIS was based on several factors, including but not limited to, USIS's performance on both OPM's and other government contracts; USIS's IT posture and ability to timely remediate identified problems; USIS's financial condition; and OPM's need for continued services and ability to fulfill that need through other means. Based on his independent judgment of the facts available at the time, and consistent with the policies in FAR Part 17.2 regarding the exercise of contract options, the OPM CO determined that renewing USIS's contracts was not in the best interest of the Government.

To: Ms. Seymour
Chief Information Security Officer
Office of Personal Management

From: Mr. Connolly
Member
Committee on Oversight and Government Reform

April 22, 2015 Full Committee Hearing
"Enhancing Cybersecurity of Third-Party Contractors and Vendors"

Cybersecurity is a sophisticated and evolving national challenge. Meeting this daunting threat requires a broad, "whole of government and industry" approach that enhances three pillars that are essential to effectively dealing with cyber threats: people, policy, and practices.

With respect to the people factor, there may be no better demonstration of the importance of individuals in securing information systems than the truism that the number one cybersecurity threat or vulnerability facing any company is the behavior of its own employees. As the Ponemon Institute's *2015 State of Endpoint Report: User-Centric Risk* found after surveying information technology security professionals, "The primary reason for the difficulty in managing endpoint risk is negligent or careless employees who do not comply with security policies."

In light of significant security risks posed by human error, please describe the policies, procedures, and specific actions the U.S. Office of Personnel Management (OPM) is implementing to mitigate and minimize such risks. Along with any pertinent factors that OPM deems important, please make sure your response addresses:

OPM: All Federal staff and contractors with access to OPM's IT resources must complete an extensive online training course prior to gaining access and annually thereafter. This training covers vulnerabilities introduced by human errors such as weak passwords, unsecured workstations, use of social media, etc. If an employee does not complete this annual training, his or her supervisor is informed, and his or her network account is disabled. OPM's requirements for IT security review are provided in both the OPM IT Security and Privacy Policy and in contract clauses. Both contractor and Federal staff in IT security positions are required to attend more extensive training each year. Additionally, OPM periodically provides focused training, such as training on how to recognize phishing emails, and routinely discusses IT security at agency-wide events.

OPM also recently began a restructure of the network security model from strictly "Defense in Depth" to a model OPM identified as performing audits by visibility. This model is an expansion of the zero trust model and not only captures user activity through thorough logging,

but also looks at user behavior activity. This model of mapping correct user actions and behavior can help enforce policies and actions while also identifying adversarial actions.

1. How OPM is enhancing its utilization of automation in data center operations and network segmentation to lower security risks; and

OPM: In early 2014, OPM analyzed its costs and operations, and concluded that it would close its existing data centers and move into two modern, secure data centers. As much of OPM's hardware is near, or at, end-of-life, the network was completely redesigned for these two new data centers. The project has been ongoing for about one year, and is on schedule, and within budget. The new infrastructure will be delivered this year. OPM's next phase of activity will focus on updating business applications so that they can operate within this new, more secure environment. The new architecture provides for automated patching of servers and workstations on a timely basis. Business applications and databases are segmented to reduce the risk and damage that might be caused by various security incidents, not just adversarial activity, but other operational mishaps as well. Privileged user access has been completely revamped, both from a management and a technical perspective, and is still undergoing more stringent analysis. OPM implemented two-factor authentication for 99% of users who access the network. This accomplishment was recognized in the recent Cybersecurity Sprint implemented by the Federal CIO. OPM has now launched its own cybersecurity sprints focusing on numerous other activities to reduce risk and cost of IT services.

2. Whether OPM is considering implementation of a "Zero Trust" model of information security to bolster the agency's cybersecurity capabilities and basic cyber hygiene policies and practices.

OPM: OPM is moving to a zero trust tenet posture. All new architecture uses this approach and existing systems are being migrated. These legacy systems were not built to perform at a zero trust tenet posture; therefore the migration process will be slower than the build out of new architecture.

OPM continues to explore all opportunities provided by commercial industry leaders. OPM made a decision in early-2014 that numerous OPM systems would need to be protected at the highest levels. OPM is vigorously pursuing implementation of its target environment. As noted in the results from the Cybersecurity Sprint, OPM is in the top quartile of agencies that accelerated use of multi-factor authentication for both privileged and non-privileged users. OPM is confident in its plan, developed in 2014, but will remain nimble to accommodate advancements in technology or additional needs. We remain committed to a more secure environment.

○