DEPARTMENT OF HOMELAND SECURITY APPROPRIATIONS FOR FISCAL YEAR 2016

WEDNESDAY, APRIL 15, 2015

U.S. SENATE,
SUBCOMMITTEE OF THE COMMITTEE ON APPROPRIATIONS,
Washington, DC.

The subcommittee met at 2:15 p.m., in room SD–138, Dirksen Senate Office Building, Hon. John Hoeven (chairman) presiding.

Present: Senators Hoeven, Cochran, and Shaheen.

DEPARTMENT OF HOMELAND SECURITY

STATEMENT OF HON. ANDY OZMENT, ASSISTANT SECRETARY, OFFICE OF CYBERSECURITY AND COMMUNICATION, NATIONAL PROTECTION AND PROGRAMS DIRECTORATE

OPENING STATEMENT OF SENATOR JOHN HOEVEN

Senator HOEVEN. I would like to call this meeting of the Department of Homeland Security Appropriations Subcommittee to order. I would like to welcome Ranking Member Senator Shaheen and also our full committee Appropriations Chairman, Senator Cochran. I appreciate very much you being here, as well as our three witnesses.

This hearing, of course, is on cybersecurity. Cybersecurity is one of the most complex and challenging threats currently facing our Nation. Today, we will examine the role of the Department of Homeland Security (DHS) in our Nation's cybersecurity efforts, specifically its responsibilities for securing the dot-gov domain, protecting critical infrastructure, and facilitating and conducting robust information sharing.

I'm pleased to welcome our witnesses Andy Ozment, the Assistant Secretary of the Office of Cybersecurity and Communications from the National Protection and Programs Directorate (NPPD) within DHS; Luke McCormack, the DHS Chief Information Officer (CIO); and Greg Garcia, Executive Director of the Financial Services Sector Coordinating Council.

The focus of today's hearing, as I noted, is DHS's role in cybersecurity. First and foremost, DHS is responsible for protecting the dot-gov domain. Through NPPD, DHS secures dot-gov by providing overarching services and capabilities and best practices that agencies are required to deploy to protect their agencies' information technology (IT) infrastructure and systems.

While there is a roadmap to accomplish this mission, I understand DHS still has work to do to fully deploy capabilities to ensure each agency is protecting its data.

At the same time, we must ensure departments and agencies across government are appropriately funded to operate and support their own IT infrastructure and systems. Each Chief Information Officer (CIO) bears responsibility to their customers and data. That includes the DHS CIO with us today.

We will discuss in detail programs such as Einstein for intrusion detection and prevention, continuous diagnostics for monitoring activity within systems, and incident reporting through US–CERT's online system.

Cybersecurity efforts are substantial and growing. In fiscal year 2015, Congress provided $12.4 billion for cybersecurity across the government. DHS is responsible for 11 percent or $1.4 billion of that funding, largely due to its responsibility for securing dot-gov.

DHS's second cybersecurity mission is supporting critical infrastructure protection. DHS leverages its experience in deploying capabilities for dot-gov in supporting protection of critical infrastructure. At the same time, the role is very different, as 85 percent of U.S. critical infrastructure is privately held. Robust public-private partnerships are the cornerstone of this responsibility.

No discussion of cybersecurity would be complete, however, without mentioning the Department's third mission area, the dissemination of cyber threat and incident information. Yet again, this is not a mission that DHS can own exclusively and execute alone. The intelligence community and national defense apparatus has access to information significant to detecting U.S. cyber-interests broadly. They struggle with how to best share that information while protecting sources and methods.

Conversely, private sector entities are often the first to realize something wrong is happening in cyberspace and can alert the government and their peers.

For those reasons, both the government and the private sector need the right information sharing mechanisms and capabilities. Timely, actionable information needs to flow in all directions. There is no silver bullet. Responding to the threat will require visionary leadership on the part of the Department; the government as a whole; and State, local, and private sector partners. Parochial interests and bureaucratic process should not be allowed to stand in the way of progress.

With strong detection, prevention, mitigation, and information sharing efforts, we can address evolving threats head on and work toward a more robust cybersecurity environment. And I look forward to your recommendations, to that end.

This is a complicated area, but it is one of great priority right now.

Let me also note that this date marks a solemn anniversary. Two years ago today, the city of Boston suffered a terrible terrorist attack. The Senate will be observing a moment of silence at 2:49, the time of the attack. With the indulgence of Senator Shaheen and our witnesses, we will do the same during this hearing. So we will notify you at that time, 2:49, and there will be a moment of silence.

With that, I would like to turn to the ranking member of the committee. She and I just returned from a visit of the southern border, including Houston, McAllen, Laredo, and San Antonio. I appreciate very much your going. I think it was very informative.

There is a lot going on when it comes to DHS. Whether it is border security or cybersecurity, this is complicated stuff. And we need good people doing a good job, so we want to do everything we can to help and support, in terms of doing the best possible job of funding that effort.

With that, I will turn to Ranking Member Shaheen.

STATEMENT OF SENATOR JEANNE SHAHEEN

Senator SHAHEEN. Thank you very much, Mr. Chairman. As you point out, we had a fascinating and informative trip to the southern border. And while border security, obviously, was a topic of conversation throughout the trip, cybersecurity didn't come up much, so we look forward to hearing from each of our panelists today.

I also, like you, Mr. Chairman, say how much I appreciate Chairman Cochran being here for this hearing. It is always nice to have the full committee represented when we are having a subcommittee hearing.

And I also very much appreciate your mentioning that this is the 2-year anniversary of the Boston Marathon bombing. We had a number of New Hampshire folks who were injured in that bombing, so it is something that we feel very personally throughout New England, and I know through the rest of the country. So I am very appreciative that we will all be pausing to remember and acknowledge the bombing and its victims.

As the Chairman pointed out, the Department of Homeland Security's role in cybersecurity is very complex and multifaceted, and the agency's effort should be carefully coordinated with other Federal agencies, with all government organizations, and, of course, with the private sector.

Cybersecurity is at the forefront of our national consciousness, and we hear every day about another cybersecurity challenge.

On the news this morning, there was a report about the potential vulnerability of cockpits because of the ability to hack into security networks. So this is an issue that, as all of you know, is on the front pages every day. Anybody who has seen the news knows that the Federal Government, private companies, academic institutions, individuals, no one is free from the potential of a cyberattack.

Now, through this hearing, we hope to focus on DHS's role in protecting the Nation from cyberattacks, and I look forward to discussing the National Protection and Programs Directorate (NPPD) activities and how partners such as Federal agencies and the private sector use their programs. In addition, we will hear from DHS's chief information officer on how his office partners with the NPPD to stay ahead of cyber threats.

The Department is also helping secure our Nation by the work of its various law enforcement agencies tasked with tracking down cybercriminals, and the Science and Technology Directorate, which is working to develop and improve technologies that protect our information systems.

And I have to say, I had a fascinating briefing earlier this week on our efforts internationally to work with other governments on securing cyber networks.

The Office of Management and Budget (OMB) reports that the President's cybersecurity request for fiscal year 2016 is $13.9 billion, an 11-percent increase. Of this total, $1.4 billion is requested for DHS programs, including protection, investigations, and science and technology. And much of the requested funding will be dedicated to programs that help us both catch up and keep up with the daily threat from cyberattacks.

Now, since the Internet was developed with an open architecture, we are retroactively addressing security vulnerabilities through major programs, such as intrusion detection and continuing diagnostics, and these efforts are important. Investments that mitigate future risks are equally important. We should focus on future workforce needs and support businesses by ensuring the development of quality cybersecurity products and encouraging the use of best practices.

It is concerning that budget pressures are forcing us to focus more on immediate needs rather than also making the necessary investments that will save us money and prevent attacks in the future.

So again, thank you all for being here today. I look forward to hearing what you have to say and to an exchange, following your remarks.

Thank you, Mr. Chairman.

Senator COCHRAN. Mr. Chairman.

Senator HOEVEN. I would now like to recognize the chairman of the full Appropriations Committee and thank Senator Cochran for joining us.

Senator Cochran.

STATEMENT OF SENATOR THAD COCHRAN

Senator COCHRAN. Mr. Chairman, thank you. I am very pleased to join you and other members of this panel to discuss with the Department of Homeland Security experts here what we should know about cybersecurity, what we should appreciate the opportunity to learn, what Congress as a principal part of the decision-making process should be considering in terms of funding, in terms of legal authority to act on behalf of our Nation's interests in cybersecurity, and exactly what we should do about the challenges that we face.

Senator HOEVEN. Thank you, Mr. Chairman. And again, thanks for joining us.

We will go with 5-minute rounds for the questions, but, first, of course, we will start with your prepared statements.

So Mr. Ozment, if you would like to proceed?

SUMMARY STATEMENT OF HON. ANDY OZMENT

Mr. OZMENT. Thank you. Chairman Cochran, Chairman Hoeven, Ranking Member Shaheen, thank you for your unwavering support for the Department of Homeland Security and the National Protection and Programs Directorate, or NPPD. We look forward to continuing this cooperation as we work to secure and enhance the resilience of our Nation's cyber and physical infrastructure.

Speaking to our cyber mission, we view ourselves as a customer service organization with three customers: the Federal Government civilian and executive branch; State, local, tribal, and territorial governments; and the private sector. In helping these three customers manage their cybersecurity risks, we focus on three areas.

The first is to implement best practices, particularly through the cybersecurity framework. And these best practices, we believe that companies and agencies should invest at least 70 percent of their effort in the space. The second is robust information-sharing in near real-time whenever possible, and we believe that companies and agencies should be investing about 25 percent of their effort in this space. And the final area is effective incident response, where companies should invest the final 5 percent or so of their effort.

These are ballpark figures, but my idea here is to give you a sense of the magnitude and relative effort that should be expended. We know that best practices alone can defeat the vast majority of cyber threats and force our adversaries to pay more, frankly, for the benefits that they are hoping to obtain.

I will focus my remarks today on two of our three customers, the Federal civilian executive branch and the private sector. And, of course, two of my customers are, in fact, testifying with me here today.

Regarding our Federal agency customers, I would like to highlight three key initiatives. First, we measure and motivate agency cybersecurity. Second, we provide tools and services to identify network security issues. And third, we provide a baseline of security across the Federal civilian executive branch through the Einstein program. I will explain each of these a bit further.

Last year, Congress gave us new authorities to help measure and motivate agency cybersecurity through the Federal Information Security Modernization Act, or the modernization of FISMA. We are now working closely with the Office of Management and Budget, the National Institute for Standards and Technology, and the Federal CIO Council to implement these authorities and to help Federal agencies better understand and manage their own risks.

To the second point, our Continuous Diagnostics and Mitigation program, or CDM, serves Federal executive branch civilian agencies with tools and services to identify network security issues and prioritize their mitigation.

I am delighted to announce that, just yesterday, we awarded a new task order to seven large agencies that cover 47 percent of the Federal civilian government by personnel. So in total, 55 percent of the Federal civilian government has now received awards for CDM tools and services.

This is the award. The actual deployment of these tools and services will take some months yet, but this is a major milestone to have achieved.

We are requesting $103 million for CDM in fiscal year 2016.

Finally, in the best practices realm for Federal departments and agencies, I would like to highlight our Einstein program, otherwise known as the National Cybersecurity Protection System. Einstein 1 and 2 provide intrusion detection services, so that is where we identify the bad guys and set off an alarm. Einstein 3 provides an

intrusion protection service, where it actually blocks malicious actors from intruding upon or attacking the Federal Government.

The Einstein program provides a first line of defense against cyber threats. Einstein 3 uses classified and unclassified information to block cyber espionage and attacks. It is also a platform upon which we can build future security capabilities that adapt to emerging cybersecurity risks and that help us take advantage of the innovation the private sector can provide.

We look forward to working with Congress to further clarify DHS authority to deploy Einstein 3A across Federal executive branch civilian departments and agencies.

Now let me switch my focus to the private sector. For the Federal Government, our mission includes directly protecting departments and agencies. For the private sector, our mission is to help companies better secure themselves. Through our C-Cubed Voluntary Program, we encourage organizations to adopt the cybersecurity framework as part of an enterprise risk management approach.

We also perform risk assessments with and for companies. These risk assessments give us data on the state of industry and help individual parts of our infrastructure understand and manage cyber risks. We have invested an additional $4 million in fiscal year 2016 to double the number of cybersecurity risk assessments this program can help to provide our private-sector partners.

I now would like to highlight three information-sharing programs that we offer to help the private sector. The first, the cyber information-sharing and collaboration program, allows DHS to share cybersecurity formation in near real-time with critical infrastructure partners. In this program, we built a pilot automated information-sharing program with the FS–ISAC, and I expect that my partner up here, Greg Garcia, may also speak to that.

We also offer Enhanced Cybersecurity Services, or ECS, which allows us to share classified and unclassified threat indicators with cybersecurity companies, who then use that information to protect their private-sector customers.

We have requested nearly $17 million in additional funds for fiscal year 2016 to expand the ECS program.

Finally, we are working to foster Information-Sharing and Analysis Organizations to address the private sector's request for more flexible information-sharing organizations and clear best practices for those organizations. And we are requesting $2 million in fiscal year 2016 for the program.

PREPARED STATEMENT

I would like to close by thanking members of the subcommittee for your help in passing five pieces of historic cybersecurity legislation this past year. In the interest of time, I will leave additional description of our efforts and of the NCCIC, our National Cybersecurity and Communications Integration Center, for your questions.

Thank you.

[The statement follows:]

PREPARED STATEMENT OF HON. ANDY OZMENT

INTRODUCTION

Chairman Hoeven, Ranking Member Shaheen, and distinguished Members of the Subcommittee, let me begin by thanking you for the unwavering support that you provide to the Department of Homeland Security (DHS) and the National Protection and Programs Directorate (NPPD). We look forward to continuing to work with you in the coming year to ensure a homeland that is safe, secure, and resilient against terrorism, cyber attacks, natural disasters, and other risks.

NPPD undertakes its cybersecurity activities within its overarching mission to secure and enhance the resilience of the Nation's cyber and physical infrastructure. We view ourselves as a customer service organization, and our customers are Federal Executive Branch civilian departments and agencies, private sector infrastructure owners and operators, and State, local, tribal, and territorial (SLTT) governments.

In serving these customers, our guiding principles are: prioritize our customers' needs to build and retain their trust; ensure privacy and civil rights across the depth and breadth of our cyber and communications activities; and enable continuous improvement in emergency communications and cybersecurity to stay ahead of malicious actors.

I will focus my remarks today on the Office of Cybersecurity and Communications (CS&C's) approach to service and capabilities. This includes the technical tools we use in protecting our Federal agency customers; CS&C's incident response capabilities that we deploy to both public and private entities to ensure critical infrastructure resilience; and how we help entities protect themselves, in particular our work to ensure that we help private sector and SLTT customers better manage their risks.

PROTECTING THE FEDERAL GOVERNMENT

Across the Federal Government, each department and agency is responsible for managing its own cybersecurity. However, under the Federal Information Security Modernization Act (FISMA) of 2014, DHS is provided with the authority to administer the implementation of Federal cybersecurity policies. In order to carry out this important responsibility, DHS is authorized to issue binding operational directives, monitor agency cybersecurity practices, and provide operational and technical assistance. NPPD's strategy to implement its FISMA authorities is to measure and motivate improved cybersecurity among Federal agencies through partnerships with the Office of Management and Budget, the National Institute of Standards and Technology, and the Federal CIO Council, and to build technical systems that provide a baseline of cybersecurity across the Government.

CDM: Helping Federal Agencies Understand and Manage Cyber Risk

Through the Continuous Diagnostics and Mitigation (CDM) program, DHS provides Federal Executive Branch civilian agencies with tools and services to identify network security issues, including unauthorized and unmanaged hardware and software; known vulnerabilities; weak configuration settings; and potential insider attacks. Agencies can then prioritize mitigation of these issues based upon potential consequences or likelihood of exploitation. In this way, CDM helps agencies understand and manage their own cyber risks.

DHS is moving aggressively to implement CDM across all Federal Executive Branch civilian agencies, and Memoranda of Agreement (MOA) with the CDM program cover over 97 percent of all Federal civilian personnel. Delivery Order 1, the first award under the CDM/Continuous Monitoring as a Service (CMaaS) blanket purchase agreement was for $59.5 million to purchase CDM tools for 21 agencies; this procurement demonstrated a 30 percent cost reduction over General Services Administration (GSA) pricing and resulted in $26 million in cost avoidance. A subsequent award was made for license maintenance of the tools procured in Delivery Order 1 that reflected a 50 percent cost reduction over GSA pricing. The first of six awards for Task Order 2 was made in February 2015 and will provide CDM tools and services to DHS itself. Additional awards will be issued through fiscal year (FY) 2015 and fiscal year 2016, and ultimately will cover over 60 additional Federal agencies including 23 of the 24 Chief Financial Officer Act agencies. Department of Defense, the 24th CFO Act agency, does not participate in the CDM-funded solicitation activities.

The CDM Federal Dashboard will provide DHS with summary data to understand relative and system risk across the Executive Branch. Local agency dashboards will provide each agency with detailed information into its specific, prioritized risks.

Both dashboards will use commercial off-the-shelf technology. The agency-level dashboards will begin deployment in fiscal year 2015, and the Federal dashboard is expected to fully deploy by fiscal year 2017.

These dashboards will receive automated feeds from the CDM tools and will provide a new level of rigor and timeliness to our understanding of Federal agency cyber risk.

E^{3}*A: Detecting and Blocking Threats Against Federal Networks*

Another tool utilized by NPPD to fulfill its mission is EINSTEIN 3 Accelerated (E^{3}A). E^{3}A is a perimeter defense tool: a first line of defense against cyber threats for Federal civilian Departments and Agencies. E^{3}A can be considered a set of security gates on the Federal Government's traffic, located at the handful of Internet Service Providers (ISPs) that are used by almost every Federal civilian agency to access the Internet. DHS has completed building E3A checkpoints at two ISPs: therefore, agencies that currently use these two ISPs to connect to the Internet are now able to obtain E^{3}A protection. These security gates only apply to traffic transiting to and from Federal civilian executive branch agencies. A Privacy Impact Assessment (PIA) for E^{3}A was published by DHS in 2013 to publicly document how privacy protections have been integrated into the E^{3}A process. This PIA is available through the Department's publicly-facing website.

E^{3}A uses classified and unclassified information to block cyber espionage and attacks, including by our most sophisticated adversaries. E^{3}A currently provides two protection capabilities (Domain Name Server (DNS) Sinkholing and Email Filtering) that have been found to be highly effective in detecting and blocking known threats, thereby protecting against those adversaries about whom the Government has identified telltale attributes. The Domain Name Server (DNS) Sinkholing capability allows DHS to prevent malware installed on .gov networks from communicating with known or suspected malicious Internet domains (sinkhole information) by redirecting the network connection away from the malicious domain to "safe servers" or "sinkhole servers," thus preventing further malicious activity by the installed malware. The Email Filtering capability allows DHS to scan email destined for .gov networks for malicious attachments, Uniform Resource Locators (URL), and other forms of malware, before being delivered to .gov end-users.

Currently, approximately 26 percent of Federal civilian personnel are protected by at least one of E^{3}A's capabilities. Recently, a second ISP completed its build-out of E^{3}A, so now the capacity exists to protect almost 50 percent of Federal civilian personnel. To take advantage of that new capacity, the newly covered agencies must sign an MOA and restructure their networks to ensure they can receive the full suite of E^{3}A capabilities. Agencies will be onboarded in stages, and each onboarding is expected to take several weeks. As of April 3, 2015, 51 agencies have signed MOAs to participate in E^{3}A services, and those agencies include approximately 96 percent of all Federal civilian personnel. We are continuing to work with the other major ISPs used by the Federal Government to build E^{3}A capabilities at those ISPs as well.

E^{3}A also provides a platform on which DHS can build future protection capabilities that adapt to emerging security risks, allowing future innovation from both government and industry. It is a unique system that utilizes classified information to protect unclassified network traffic for Federal Civilian Executive Branch networks and allows DHS to better detect, respond to, and appropriately counter known or suspected cyber threats identified within the Federal network traffic it monitors.

Moreover, E^{3}A is allowing DHS to create situational awareness of cyber threats by screening Federal agency Internet traffic for cyber threats across multiple agencies, enabling strong correlation of events and the ability to provide early warning and greater context about emerging risks. As the Department detects and stops adversaries' attacks with E^{3}A, we will take the knowledge we gain and share it with the private sector and SLTT governments, meeting their information needs in a manner that is consistent with the protection of privacy and civil liberties. They will be able to use this information to better protect themselves.

Obtaining the MOAs necessary to deploy E^{3}A services has been time consuming, and not all agencies are ready to sign them. Some agencies, in some cases, have questioned how deployment of EINSTEIN under DHS authority interplays with their existing statutory restrictions on the use and disclosure of agency data. As a result of this uncertainty, DHS has not been able to achieve 100 percent commitment from agencies to enter into authorizing the deployment of EINSTEIN capabilities to protect their systems. DHS and the Administration have sought statutory changes to clarify this uncertainty and to enable agencies to disclose their network traffic to DHS for narrowly tailored purposes to protect agency networks, while making clear that privacy protections for the data would remain in place. Moreover,

as E 3A's capabilities evolve, the MOAs will need to be updated. We look forward to working with Congress to further clarify DHS's authority to deploy this protective technology to Federal Executive Branch civilian systems.

Looking toward the future, NPPD is advancing its protective capabilities to detect not only known cyber threats, but also recognize potential threats that have not been previously observed. Just as the human body achieves resilience by fighting new viruses with biological mechanisms that recognize when the body is under attack, DHS seeks to build similar mechanisms for networks using mathematical trend analysis of cyber events. We will collect the data needed for this from the government agencies that we protect, following the privacy protections detailed in our publicly available PIAs. The concept comprises the ability to view the current state of cybersecurity, just as a traditional weather map provides a view of current weather. Our long-term goal is for networks and connected devices to know when to reject incoming traffic or even refuse to execute specific computer instructions because they are recognized as harmful due to their current behavior, even if the exact computer "disease" has not been seen before. This will help to create the resilience to deter many cyber threat actors by increasing the costs of individual cyber attacks.

ENHANCING INFORMATION SHARING TO REDUCE THE FREQUENCY AND IMPACT OF CYBER INCIDENTS

The National Cybersecurity & Communications Integration Center (NCCIC) serves as a 24x7 centralized location for cybersecurity information sharing, incident response, and incident coordination. NCCIC partners include all Federal departments and agencies, including law enforcement, the Department of Defense, the Intelligence Community; SLTT governments; the private sector; and international entities. The NCCIC provides its partners with enhanced situational awareness of cybersecurity and communications incidents and risks, and it provides timely information to manage vulnerabilities, threats, and incidents. In 2014, the NCCIC received over 97,000 incident reports, and issued nearly 12,000 actionable cyber-alerts or warnings. NCCIC teams also detected over 64,000 vulnerabilities on Federal and non-Federal systems and directly responded to 115 significant cyber incidents.

An example of the NCCIC's support to and collaboration with the private sector was the effort to mitigate Distributed Denial of Service (DDoS) incidents impacting U.S. banking institutions in 2012 and 2013. During the DDoS attacks, the NCCIC disseminated technical data and assistance—including 600,000 DDoS-related Internet Protocol (IP) addresses and supporting contextual information—to Federal agencies, critical infrastructure partners, international partners, and US-based ISPs. This information helped financial institutions and cybersecurity service providers improve their defensive capabilities and detect or block threats before financial services were impacted. In addition to sharing with relevant private sector entities, the NCCIC shared information with over 120 international partners, many of whom contributed to our mitigation efforts. The NCCIC, along with the U.S. Secret Service, FBI and other interagency partners, also deployed to affected entities to offer on-site technical assistance.

For fiscal year 2016, NPPD requested an additional $10.412 million and 35 FTP/19 FTE to develop situational awareness and infrastructure analysis. This increased funding will support 24/7 operations for an Integrated Analysis Cell, increased software and tool support for forensic analysis, increased resources for incident response, and improved architecture to drive cybersecurity solutions.

HELPING THE PRIVATE SECTOR AND SLTT GOVERNMENTS MANAGE RISK

NPPD helps the Nation's infrastructure owners and operators protect themselves by offering our customers risk assessments and assistance via the Critical Infrastructure Cyber Community (C3) Voluntary Program. NPPD assists all 16 critical infrastructure sectors with risk management activities, including supporting the use of the NIST Cybersecurity Framework for Critical Infrastructure (the Framework). NPPD is requesting additional resources in support of the Framework to allow the C3 Voluntary Program to double the number of cybersecurity risk assessments provided to critical infrastructure owners and operators. These assessments provide critical infrastructure owners and operators with invaluable information about their cybersecurity posture in relation to the Framework, and they offer concrete areas for improvement. This budget request will extend the reach of the C3 Voluntary Program, promote adoption of the Framework, and build the security and resilience of the nation's critical infrastructure.

Separately, NPPD is requesting $16.901 million for the Enhanced Cybersecurity Services (ECS) program. ECS has similar capabilities to E 3A. However, unlike E 3A, it is available to validated critical infrastructure companies and SLTT customers.

ECS shares sensitive unclassified and classified cyber threat indicators with qualified Commercial Service Providers (CSPs) that then use that data to protect their ECS customers. All payment and contractual relationships occur between an ECS customer and their service provider devoid of any DHS involvement. The Federal Government deals directly with the CSPs and not their end customers. The Federal Government's role is limited to ensuring CSPs meet the program security requirements for receiving sensitive unclassified and classified Government Furnished Information, providing timely and vetted cyber threat information to the qualified service providers, and receiving anonymous, aggregated data back from the service providers about the number of malicious activities detected by their ECS systems. Through their respective CSPs, ECS customers can decide whether any data is shared back to the Department. The privacy and civil liberties considerations for the program are detailed in the ECS PIA available on DHS's publicly-facing website and in a Privacy and Civil Liberties assessment mandated by Executive Order 13636 and made publicly available on the DHS Privacy Office website. This budget request will fund additional cybersecurity analysts to provide new threat and network analysis, and it will expand the ECS program to an increased number of CSPs.

CONGRESSIONAL SUPPORT

I would like to take this opportunity to thank the members of this Committee, and Congress as a whole, for the passage of five pieces of legislation this past year that have significant implications for cybersecurity. The passage of these bills represents a historic and momentous accomplishment for our Directorate. These bills contribute to the safety, security, and resilience of our Nation's digital networks and critical infrastructure. Simply put, they will make our nation safer. They include:

—The National Cybersecurity Protection Act of 2014, which provides explicit authority for DHS to provide assistance to the private sector in identifying vulnerabilities and restoring their networks following an attack, and establishes in law the NCCIC as a Federal civilian interface with the private sector.

—The Federal Information Security Modernization Act of 2014, which statutorily establishes DHS authority to administer the implementation of Federal information security policies, develop and oversee implementation of binding cybersecurity directives, provide technical assistance to other agencies through US-CERT, and deploy cybersecurity technology to other agencies upon their request.

—Two bills that help DHS continue to recruit, hire, and retain the best and brightest cybersecurity workforce. In fiscal year 2016, NPPD is requesting $16.238 million to support cybersecurity pay reform as part of DHS' efforts to improve its cybersecurity workforce.

—Separately, apart from our cybersecurity authorities, a four-year authorization for the Chemical Facility Anti-Terrorism Standards (CFATS) program, which significantly improves our ability to work with the private sector on security at high-risk chemical facilities.

Thank you for the opportunity to appear before you today. I look forward to answering any questions you may have about my testimony or NPPD's cyber activities. Additionally, before I conclude, I'd like to encourage those members who have not yet been able to visit the NCCIC or who have not been by recently to contact us to arrange a tour. A visit to the facility is a great way to better understand how NPPD works to secure our customers and respond to incidents across the Nation.

Senator HOEVEN. Thank you.

Mr. McCormack.

STATEMENT OF LUKE McCORMACK, CHIEF INFORMATION OFFICER

Mr. MCCORMACK. Thank you, Chairman Cochran, Chairman Hoeven, Ranking Member Shaheen, and members of the subcommittee. Thank you for this opportunity to speak to you about cybersecurity at the Department of Homeland Security.

In the following remarks, I will focus on the role and responsibility of the DHS chief information officer to defend the Department's information systems from cyberattacks and how the Nation's cybersecurity is strengthened through ongoing collaboration with our components, with NPPD, and across the Federal Government.

The Office of the Chief Information Officer implements information security programs at the Department level. It provides oversight to more than 90 major IT (information technology) programs across the Department's seven operational components and headquarters offices. Because of our size and mission diversity, we have some unique challenges and opportunities for success.

The Department's leadership is strengthening a collaborative environment and culture within DHS, especially across planning, budgeting, and acquisition oversight processes through the Secretary's signature Unity of Effort initiative.

With this as our foundation, the CFO (Chief Financial Officer) and CIO councils work together to clearly define budgetary needs for cybersecurity efforts in 2016 and into the near future. Just as NPPD coordinates the Federal response to cyber incidents, we collaborate with them on many Federal cybersecurity programs, oftentimes while they are still in development. Through early adoption, we provide feedback to NPPD on products and programs before they are more widely implemented across the Federal Government.

Our organization also collaborates prominently across the Federal IT community to address challenges and share our cyber experience.

I would like to share a few of the highlights of some of our critical cyber programs and initiatives.

DHS is a major partner in the Federal Risk and Authorization Management Program, commonly referred to as FedRAMP. FedRAMP provides a standardized approach for accessing and monitoring the security capability of cloud service providers. It then certifies those capabilities. Using this "do once, use many times" framework, departments and agencies can then leverage the certification, reducing their cost and reducing their time-to-market for service delivery.

Along with the Department of Defense (DOD) and the General Services Administration (GSA), DHS serves as one of the tri-chairs of the FedRAMP Joint Authorization Board, the primary governance and decisionmaking body for this program. We have requested a program increase of $2.6 million in fiscal year 2016 to support FedRAMP as cloud computing expands and our engagement intensifies.

Again, as an early adopter partnering with NPPD, the Department was the first agency to contract for Continuous Diagnostic and Mitigation. CDM uses real-time data to provide stakeholders with tools to detect and counteract day-to-day cyber threats. This real-time information will be available on an agency-level dashboard that will alert us to critical cyber risks, providing situational awareness across the Department.

Our CDM capabilities are complemented by ongoing authorization. Ongoing authorization allows us to focus our attention on the most critical system security controls, so we can make data-driven and timely risk management decisions. With CDM and ongoing authorization, DHS is leveraging technology and risk-based decisionmaking to strengthen our security posture and target our resource capabilities.

Another important initiative to strengthen our security is the Intrusion Defense Chain, or IDC. Cyberattacks are more than iso-

lated activities. They often occur in phases that are repeated and reused. The DHS IDC methodology uses lessons from past attacks to anticipate the direction of future attacks.

PREPARED STATEMENT

We continue to enhance our remediation of known vulnerabilities across the Department. It is because of these efforts that the President's fiscal year 2016 budget includes $31.7 million for mission-essential cybersecurity remediation. We also requested $16.2 million to implement an enterprise single sign-on ability. This will strengthen our ability to prevent unwarranted access to mission-critical systems.

Cyber-defense is not purely technical. Attracting, training, and retaining quality IT professionals is critical to the long-term success of our mission. DHS has developed and implemented a number of initiatives, beginning with the hiring process and extending throughout an employee's career.

I appreciate your time and attention, and I look forward to addressing your questions and concerns.

[The statement follows:]

PREPARED STATEMENT OF LUKE MCCORMACK

INTRODUCTION

Chairman Hoeven, Ranking Member Shaheen, and Members of the Subcommittee: Thank you for this opportunity to speak to you about cybersecurity at the Department of Homeland Security. As you are aware, it is vital for our Department and the Federal Government to defend our systems against cyber-attacks. The Office of the Chief Information Officer (CIO), in close coordination with the National Protection and Programs Directorate (NPPD) ensures that our Nation is secure and able to stay ahead of cyber threats.

In the following remarks, I will focus on the roles and responsibilities of the Office of the Chief Information Officer to ensure the Department's information is safe from cyber-attacks, and how the nation's cybersecurity is strengthened through ongoing collaboration with our components, with NPPD, and across-government. I will also highlight some of the Department's ongoing and future cybersecurity initiatives.

THE ROLE OF CIO AT DHS

As the DHS Chief Information Officer, my role is to implement information security programs at the Department level. My office's mission is to develop and maintain a single, Department-wide information technology (IT) infrastructure that is reliable, scalable, flexible, maintainable, accessible, and secure. I provide oversight to over 90 major IT programs across the Department's seven operational components and Headquarters offices. Because of our size and mission diversity, we have some unique challenges and opportunities for success.

DHS OCIO AND COMPONENTS

The Department's leadership recognizes the importance of strengthening a collaborative environment and culture within DHS, especially across programming, budgeting, and acquisition oversight processes. On April 22, 2014, the Secretary signed a memo entitled Strengthening Departmental Unity of Effort. Through this Unity of Effort initiative, we are:

—Actively supporting the Joint Requirements Council (JRC)—a body that develops recommendations for investment, as well as changes to training, organization, legislation, and operational processes and procedures;
—Enhance the Department's programming and budgeting process; and
—Actively collaborating with our component counterparts to drive efficiencies and improve effectiveness.

Using Unity of Effort as our foundation, the Councils of the CFO and CIO—bodies comprised of the chief financial and chief information officers from across DHS-worked collaboratively to clearly define budgetary needs for cybersecurity efforts in

2016 and into the near future. It is because of these efforts that the President's budget includes $31.7 million for essential cybersecurity remediation initiatives in fiscal year 2016.

The Unity of Effort also resulted in updating the DHS IT Strategic Plan. It is a focused, mission-driven, achievable plan that positions our technology environment to address the critical areas of people and culture, innovative technologies, cybersecurity, and governance and accountability. As part of that IT Strategic Plan, the CIO Council developed a specific cybersecurity goal: to "Empower DHS and its partners to operate secure IT systems and networks, keeping ahead of evolving cyber threats." Additionally the CIO Council is supported on all matters of cybersecurity by another cross-Department council comprised of the Chief Information Security Officers from Headquarters and our components.

PARTNERING WITH NPPD

NPPD's role is to enhance the security, resilience, and reliability of the nation's cyber and communications infrastructure. NPPD coordinates the Federal response to cyber incidents, and leads efforts to protect the Federal ".gov" domain, and collaborates with the ".com" domain to increase the security of critical networks. Due to our partnership with NPPD we are able to internally implement and collaborate on many Federal cybersecurity programs, sometimes while they are still in development. By taking on the role of an early adopting agency, we provide valuable feedback to NPPD on products and programs before they are more widely implemented across government. For example, we are currently working with NPPD to test the Continuous Diagnostics and Mitigation (CDM) dashboard. Through collaboration of this nature, DHS strengthens its cybersecurity posture across government to serves as an initiator and leader in Federal cybersecurity efforts.

CROSS-GOVERNMENT EXPERTISE AND COLLABORATION

In addition, my office contributes cybersecurity expertise to the Federal IT community. Two of the areas where we are working with colleagues across government are to enhance security of mobile applications and standardizing the approach for assessing and monitoring the security of cloud products and services.

Secure Mobility

Directly related to the Presidential memorandum issued on May 23, 2012, entitled, Building a 21st Century Digital Government, the Federal CIO Council has been charged with identifying solutions to challenges that prevent progress in IT delivery. One such challenge is ensuring the rapid adoption of mobile technologies while maintaining a security posture appropriate to the agency's mission. To address this, the Federal CIO Council established a Mobile Technology Tiger Team. DHS co-chairs the tiger team, which recently unveiled a set of criteria to be used in validating security for mobile applications. This effort provides consistency across the Federal Government and allows industry to better meet the needs of Federal customers. As additional Federal agencies adopt the criteria, mobile application development will be more secure and predictable.

The Federal Risk and Authorization Management Program (FedRAMP)

DHS is a major partner in the Federal Risk and Authorization Management Program (FedRAMP). FedRAMP provides a standardized approach for assessing and monitoring the security of cloud products and services and will significantly reduce the time-to-market for Departments and Agencies as they implement cloud computing. Testing and authorizing a cloud provider is performed once and is shared multiple times across the government. This reduces both time and cost by reusing the authorization of a cloud provider, and introduces competition in the cloud market.

DHS was engaged in FedRAMP from its inception, contributing to the development of its security standards. Along with the Department of Defense and the General Services Administration, DHS serves as one of the tri-chairs of the FedRAMP Joint Authorization Board, the primary governance and decisionmaking body for the program. DHS provides technical reviews of cloud service provider proposals for the board. As more of government moves to cloud services and our engagement intensifies, we see an expected program increase of $2.6 million in fiscal year 2016 to support FedRAMP.

DHS CYBERSECURITY INITIATIVES

As you know, Congress passed two key pieces of legislation that greatly enhances our ability to shape and resource cybersecurity initiatives. Both the 2014 Federal

Information Security Modernization Act (FISMA) and the Federal Information Technology Acquisition Reform Act (FITARA) will strengthen our ability, as a Department, to respond and establish stronger guidance and controls.

—The 2014 Federal Information Security Modernization Act allows for more nimble and risk-based security assessments and compliance. It defines roles and responsibilities for cybersecurity within the Federal Government. FISMA frames information security in a more modern and efficient fashion.

—FITARA strengthens the role of Departmental CIOs. It ensures that all IT investments are be reviewed by the CIO prior to acquisition. This is vital to reduce duplication of IT systems, provide high-value services, and ensure the continued ability to proactively combat cyber-attacks.

Continuous Diagnostics and Mitigation Program

The Department was the first agency to contract Continuous Diagnostics and Mitigation. As an early adopter, the Department expects to see positive impacts to how we detect and counteract cyber threats. CDM uses real-time data to provide stakeholders with the tools needed to protect their networks and enhance their ability to detect and counteract day-to-day cyber threats. The CDM capabilities feed into agency-level dashboards that alert us to critical cyber risks in near real time.

DHS is currently testing the CDM dashboard in two operational instances. This enables the system stakeholders to readily identify which network security issues to address first, enhancing the overall security posture of agency networks in hours instead of days. The CDM dashboard will provide extensive visibility across the DHS enterprise.

Ongoing Authorization

Originally, a system's Authority to Operate was granted every 3 years after a large paper-based security controls review. This triennial paper-based process will evolve to the Ongoing Authorization (OA) program. OA uses real-time event-driven data from CDM sensors to alert on dynamic, risk-based events. OA delivers effective, timely, event-driven security services to Federal IT systems.

DHS is a role model for the implementation of OA across the Federal government. Our OA program continues to expand. Seventy systems were enrolled in the program before the end of fiscal year 2014, exceeding the goal of 50. Currently, 82 systems are enrolled.

Security Operations Center

Like other Departments, DHS uses a federated architecture that relies on mission-focused components leveraging their intimate knowledge of their missions to police their networks. The DHS Security Operations Center (SOC) aggregates these data feeds to create a holistic view of the DHS enterprise. The Department's SOC monitors the enterprise network and reports all cyber incidents to the United States Computer Emergency Readiness Team (US-CERT) under NPPD. Additionally, the DHS Chief Information Security Officer provides advanced threat investigation services.

As our adversaries continue to evolve and become more sophisticated, we must evolve as well. To do this, we anticipate additional investment in cyber counterintelligence services like Focused Operations.

Intrusion Defense Chain

Cyber attacks are more than isolated activities. They often occur in phases, in a chain of offensive events that are repeated, reused, and predictable. In 2013, we began implementing and refining the Intrusion Defense Chain (IDC) into our security operations. The DHS IDC methodology uses the attackers' tactics against them. It hardens the Department's defenses based on what we learn from evaluating all the links of their previous attacks.

The IDC allows us to use what we learn from past attacks to bolster our defenses and identify areas that might need future investment. Defending the Department is a full-time effort and the IDC helps to provide us with an advantage tactically and financially.

Strengthening the IT Workforce

Workforce planning at DHS is an inclusive process involving top management support with input from human resources, program management, budget, acquisition, and legal partners. It is the responsibility of every DHS component to support and ensure that effective workforce plans are prepared, implemented with action plans, monitored, and evaluated.

Attracting, training, and retaining quality IT professionals is critical to the long-term success of our mission. To attract IT professionals with cutting-edge skills in

emerging technologies necessary to address cybersecurity future needs, DHS has developed and implemented a number of initiatives:

—The CyberSkills Management Support Initiative develops and executes Department-wide human capital strategies, policies, and programs that will create, enhance, and support a top-notch DHS cyber workforce.

—The DHS IT Human Capital Strategy outlines IT career paths and enables DHS to more formally address how new workers can progress along a technical or managerial career track. As part of this strategy, DHS is leveraging developmental, mentoring, and rotational programs.

—The DHS IT Immersion Program provides newly-hired employees with a formal path to learning about IT across DHS components, and to engage with senior leadership and colleagues about career management, component activities, and working in DHS IT. This supports a true IT culture, including mentoring and educational opportunities.

The Department continues to explore possibilities to collaborate on ways to create a community of high-performing IT professionals.

CONCLUSION

I appreciate your time and attention, and I look forward to addressing your questions and concerns.

Senator HOEVEN. Mr. Garcia.

STATEMENT OF GREG GARCIA, EXECUTIVE DIRECTOR, FINANCIAL SERVICES SECTOR COORDINATING COUNCIL

Mr. GARCIA. Thank you, Chairman Hoeven, Chairman Cochran, Ranking Member Shaheen. Thanks for inviting me to testify. Today, I will discuss the DHS role in cybersecurity and its partnership with the private sector. But first, I will just take a few minutes to describe how the financial sector deals with threats and vulnerabilities to our critical financial infrastructure.

The Financial Services Sector Coordinating Council, or FSSCC, was established in 2002 and includes 65 of the largest financial firms and associations. It was formed under the critical infrastructure protection framework first developed by Presidential Directive 63 in 1998. That directive was since amended in 2003 and again in 2013.

The FSSCC mission is to coordinate the sector-wide efforts to strengthen the resiliency of our critical financial infrastructure against threats and vulnerabilities. In practice, this means that we work with government and other partners on information-sharing content and procedures, incident response, cyber and operational risk management best practices, and policy options to support the above objectives.

To achieve these objectives, the FSSCC focuses on the longer term policy and strategy options. And the tactical and operational engagement is performed by the Financial Services Information-Sharing and Analysis Center, or the FS–ISAC. This is one of our member organizations under the FSSCC umbrella.

The FS–ISAC manages a formal structure for collecting, analyzing, and sharing actionable intelligence and best practices. This sharing is done within the sector and with our industry, government, and law enforcement partners.

Indeed, we have learned over the years that strong risk management includes participating in communities of trust that share information on cyber and physical threats, on vulnerabilities and incidents. And this is based on the simple concept of strength in numbers. Call it a neighborhood watch or common situational awareness.

So now on DHS programs, our financial institutions, whether they are companies or industry associations, participate in a variety of strategic and information-sharing programs operated by DHS. For example, we have a physical presence in the National Cybersecurity and Communications Integration Center, or NCCIC, which Andy Ozment described in his statement. Supplementing our NCCIC presence is the DHS Cyber Information-Sharing and Collaboration Program, or CISCP. Our sector participants consider the CISCP program valuable for fusing and accelerating threat analysis and our time to respond. This is a good tool.

Also useful is the Critical Infrastructure Cyber Community, C-Cubed Voluntary Program, again, which Dr. Ozment described. This supplements the NIST cybersecurity framework and assists our industry stakeholders with risk assessments.

The Office of Cyber and Infrastructure Analysis helps critical sectors evaluate those cross-sector interdependencies, and they are currently doing an assessment between financial services and the telecommunications infrastructure in the Chicago area.

The FSSCC also has developed a research and development agenda that is highlighting the priority R&D initiatives that we believe will enhance the protection of our critical financial infrastructure. I am happy to submit the agenda for the record.

Referencing this agenda, we have consulted with the DHS Science and Technology Directorate over time to help inform their funding priorities.

In the area of physical resiliency, the sector works closely with the National Infrastructure Coordinating Center, the NICC.

Most recently, the financial sector has been planning and executing a series of sector-wide cyber-exercises that test our ability to share information and respond to critical incidents with our government partners. The DHS NCCIC management and operations team has been an important partner in this process. They have helped develop scenarios, supported the actual exercise, and contributed to the after-action reports.

DHS also funded development of an open specification for automated threat information sharing that Dr. Ozment referred to. It is called STIX and TAXII.

The financial sector leveraged that tool to develop a capability known as Soltra Edge. It automates threat sharing and analysis, and it speeds our time to decision and mitigation from days to hours and minutes.

This tool is extremely powerful and getting more so, and it is available to anyone in the financial sector and in other sectors. There has already been a substantial amount of uptake since its formal launch in December of last year.

Now I will wrap-up with some concluding observations.

First, if Congress were to pass legislation facilitating information sharing, DHS could receive a new influx of cyber-threat information from the private sector. A lot of these liabilities go away in incentives for more information sharing. But this in turn would intensify the already pressing need for DHS to be able to process and act on that intelligence. That is going to require more personnel who are well-trained in cybersecurity and in the critical infrastructure sectors that they serve. And it requires robust, well-managed

programs to develop analytical and best practices guidance for the community, particularly at the unclassified level. I believe these requirements apply not only to senior DHS management, but to thoughtful congressional oversight as well.

Overall, our assessment is that the financial sector's relationship with DHS is productive and directionally positive. We are showing tangible successes that are improving the protection and resilience of our critical financial infrastructure. Where there are programmatic gaps or implementation deficiencies in the partnership, they are mutually acknowledged and addressed.

On a personal note, I will just say as the first person to hold the position of Assistant Secretary at the Department of Homeland Security that Andy Ozment now occupies, I just want to congratulate Assistant Secretary Ozment for continuing the momentum that we had begun in a previous administration. They have improved on the initiatives that we started and have embarked on new initiatives and new innovations in customer service, as Andy put it.

And I also thank Congress for recognizing the critical importance of this issue and funding it accordingly. If only I had the money in 2008 that Andy has in 2015.

Ultimately, we recognize that, as our joint effort matures over time, we are never done, we are only better. And we are getting better.

Mr. Chairman, that concludes my oral remarks, and I will be happy to answer questions.

[The statement follows:]

PREPARED STATEMENT OF GREGORY T. GARCIA

Chairman Hoeven, Ranking Member Shaheen, and Members of the Subcommittee, thank you for this opportunity to address the Subcommittee about funding the DHS role in cybersecurity and its partnership with the private sector.

My name is Gregory T. Garcia. I am the Executive Director of the Financial Services Sector Coordinating Council (FSSCC), which was established in 2002 and involves 65 of the largest financial services providers and industry associations representing clearinghouses, commercial banks, credit card networks and credit rating agencies, exchanges/electronic communication networks, financial advisory services, insurance companies, financial utilities, government-sponsored enterprises, investment banks, merchants, retail banks, and electronic payment firms.

The FSSCC was established in accordance with the critical infrastructure protection framework promulgated first in Presidential Decision Directive 63 in 1998, which was superseded in 2003 by Homeland Security Presidential Directive 7 and in 2013 by Presidential Policy Directive 21.

FSSCC membership includes critical financial enterprises and their industry associations whose responsibility and commitment to the protection of our sector is commensurate with their substantial importance to the resilience of the national and global economy.

As with many industry associations, its governing structure includes a rotating chairmanship and an executive committee, with numerous outcome-oriented working groups focused on specific deliverables to achieve the organization's objectives.

The current chairman, serving the first year of his 2 year term, is Russell Fitzgibbons, theChief Risk Officer and Executive Vice President of The Clearing House.

What I will cover today is an overview of the financial sector's tactical and strategic components, and how we manage cyber risk with the Department of Homeland Security, the Treasury Department, and other key government and industry partners.

FSSCC MISSION

The mission of the FSSCC is to strengthen the resiliency of the financial services sector against attacks and other threats to the nation's critical infrastructure by

proactively identifying threats and promoting protection, driving preparedness, collaborating with the Federal government, and coordinating crisis response for the benefit of the financial services sector, consumers and the nation. During the past decade, this strategic partnership has continued to grow, in terms of the size and commitment of its membership and the breadth of issues it addresses.

In simplest terms, members of the FSSCC assess security and resiliency trends and policy developments affecting our critical financial infrastructure, and coordinate among ourselves

and with our partners in government and other sectors to develop a consolidated point of view and coherent strategy for dealing with those issues.

Accordingly, our sector's primary objectives are to:

1. Implement and maintain structured routines for sharing timely and actionable information related to cyber and physical threats and vulnerabilities among firms, across sectors of industry, and between the private sector and government.

2. Improve risk management capabilities and the security posture of firms across the financial sector and the service providers they rely on by encouraging the development and use of common approaches and best practices.

3. Collaborate with homeland security, law enforcement and intelligence communities, financial regulatory authorities, other industry sectors, and international partners to respond to and recover from significant incidents.

4. Discuss policy and regulatory initiatives that advance infrastructure resiliency and security priorities through robust coordination between government and industry.

We have learned over the years that a strong risk management strategy for cyber and physical protection involves participating in communities of trust that share information related to threats, vulnerabilities, and incidents affecting those communities. That foundation is based on the simple concepts of strength in numbers, the neighborhood watch, and shared situational awareness.

Accordingly, we partner with the Department of Treasury as our sector specific agency, the Department of Homeland Security, law enforcement, the intelligence community, other critical sectors, and financial regulatory agencies forming our Government Coordinating Council counterpart—called the Financial and Banking Information Infrastructure Committee (FBIIC).

Together we are undertaking numerous initiatives to:

—Improve Information sharing content and procedures between government and the sector;

—Conduct joint exercises to test our resiliency and information sharing procedures under differing scenarios;

—Prioritize critical infrastructure protection research and development funding needs

—Engage with other critical sectors and international partners to better understand and leverage our interdependencies;

—Advocate broad adoption of the NIST Cybersecurity Framework, including among small and mid-sized financial institutions across the country; and

—Develop best practices guidance for operational risk issues involving third party risk, supply chain, and cyber insurance strategies.

FINANCIAL SECTOR PARTNERSHIP WITH THE DEPARTMENT OF HOMELAND SECURITY

Of particular relevance to the topic of this hearing, financial sector stakeholders participate in a variety of strategic and information sharing programs operated by the Department of Homeland Security. For example:

—The financial sector and Treasury Department maintain a physical presence within the DHS National Cybersecurity and Communications Integration Center (NCCIC), which serves as a hub for sharing information related to cybersecurity and communications incidents across sectors, among other roles and responsibilities.

—Supplementing our information sharing engagement within NCCIC is the DHS Cyber Information Sharing and Collaboration Program (CISCP) which enables collaborative threat analysis between industry and government in an operational environment that speeds time to response.

—Also useful to the financial sector, particularly smaller community institutions, is the Critical Infrastructure Cyber Community (C3, or "C-Cubed") Voluntary Program, which supplements the NIST Cyber Security Framework, and provides guidance on how institutions can improve their cyber risk management programs, regardless of size and sophistication.

—The Office of Cyber & Infrastructure Analysis helps critical sectors evaluate cross sector interdependencies with risk and threat assessments, and is cur-

rently undertaking an interdependency assessment between financial services and telecommunications infrastructure in the Chicago area.

—The financial sector has developed a research and development (R&D) agenda highlighting the priority R&D initiatives we believe will enhance protection of our critical financial infrastructure, and we have consulted with the DHS Science and Technology Directorate to help inform their funding priorities.

—The sector also works closely with the National Infrastructure Coordinating Center (NICC), the dedicated 24/7 coordination and information sharing operations center that maintains situational awareness of the nation's critical infrastructure for the Federal government.

—Most recently, the financial sector has begun planning and executing a series of sector-wide cyber exercises that test our ability to share information and respond to critical incidents collaboratively with our government partners. The DHS NCCIC management and operations team has been an important partner in this process, as have the Treasury Department and other key government stakeholders, lending their expertise and resources toward developing the scenarios and supporting the execution and after-action reports of the exercises.

—Through the promulgation of DHS-funded open specifications for automated threat information sharing, the Financial Services Information Sharing and Analysis Center (FS–ISAC) has developed a capability that is widely used by the financial sector and other sectors. Known as Soltra Edge, this tool automates threat sharing and analysis and speeds time to decision and mitigation from days to hours and minutes. I will discuss FS–ISAC activities in more detail below.

In sum, the financial sector has been able to benefit substantially from its close information sharing relationship with DHS.

FS–ISAC INFORMATION SHARING PROGRAMS AND OPERATIONS

For the financial sector, the primary community of trust for critical financial infrastructure protection is the Financial Services Information Sharing and Analysis Center, or FS–ISAC, which is the tactical and operational organization that informs the FSSCC's strategic policy mission.

The FS–ISAC was formed in 1999 in response to the 1998 Presidential Decision Directive 63 (PDD 63), which called for the public and private sectors to work together to address physical and cyber threats to the nation's critical infrastructures. This role was reinforced after 9/11, and in response to Homeland Security Presidential Directive 7 (and its 2013 successor, Presidential Policy Directive 21) and the Homeland Security Act.

The FS–ISAC is a 501(c)6 nonprofit organization and is funded entirely by its member firms and sponsors. In 2004, there were 68 members, mostly larger financial services firms. Since that time, the membership has expanded to more than 5000 organizations including commercial banks and credit unions of all sizes, brokerage firms, insurance companies, data security payments processors, and 24 trade associations representing virtually all of the U.S. financial services sector.

Since its founding, the FS–ISAC's operations and culture of trusted collaboration have evolved into what we believe is a successful model for how other industry sectors can organize themselves around this security imperative. The overall objective of the FS–ISAC is to protect the financial services sector against cyber and physical threats and risk. It acts as a trusted third party that provides anonymity to allow members to share threat, vulnerability and incident information in a non-attributable and trusted manner. The FS–ISAC provides a formal structure for valuable and actionable information to be shared among members, the sector, and its industry and government partners, which ultimately benefits the nation. FS-ISAC information sharing activities include:

—Delivery of timely, relevant and actionable cyber and physical email alerts from various sources distributed through the FS–ISAC Security Operations Center (SOC);

—An anonymous online submission capability to facilitate member sharing of threat, vulnerability, incident information and best practices in a non-attributable and trusted manner;

—Support for attributable information exchange by various special interest groups including the FSSCC, the FS–ISAC Threat Intelligence Committee, threat intelligence sharing open to the membership, the Payment Processors Information Sharing Council (PPISC), the Clearing House and Exchange Forum (CHEF), the Business Resilience Committee, and the Payments Risk Council;

—Bi-weekly threat information sharing calls for members and invited security/risk experts to discuss the latest threats, vulnerabilities and incidents affecting the sector;
—Emergency threat or incident notifications to all members using the Critical Infrastructure Notification System (CINS); and
—Participation in various cyber exercises such as those conducted by DHS (Cyber Storm I, II, and III) and support for FSSCC exercises such as the Hamilton series, CyberFIRE and Quantum Dawn.

FS–ISAC PARTNERSHIPS

The FS–ISAC works closely with various government agencies including the Department of Treasury, DHS, Federal Reserve, Federal Financial Institutions Examination Council (FFIEC) regulatory agencies, United States Secret Service, Federal Bureau of Investigation (FBI), the intelligence community, and state and local governments.

In partnership with DHS, FS–ISAC 2 years ago became the third ISAC to have representation on e the NCCIC watch floor. FS–ISAC representatives, cleared at the Top Secret/Sensitive Compartmented Information (TS/SCI) level, attend the daily briefs and other NCCIC meetings to share information on threats, vulnerabilities, incidents, and potential or known impacts to the financial services sector. Our presence on the NCCIC floor has enhanced situational awareness and information sharing between the financial services sector and the government, as well as other critical sectors, and there are numerous examples of success to illustrate this.

As part of this partnership, the FS–ISAC set up an email listserv with U.S. CERT where actionable incident, threat and vulnerability information is shared in near real-time. This listserv allows FS–ISAC members to share directly with U.S. CERT and further facilitates the information sharing that is already occurring between FS–ISAC members and with the NCCIC watch floor or with other government organizations.

In addition, FS–ISAC representatives sit on the Cyber Unified Coordination Group (Cyber UCG) and the group has been actively engaged in incident response. The Cyber UCG's handling and communications with various sectors following the distributed denial of service (DDOS) attacks on the financial sector in late 2012 and early 2013 is one example of how this group is effective in facilitating relevant and actionable information sharing.

Finally, the FS–ISAC and FSSCC have worked closely with its government partners to obtain security clearances for key financial services sector personnel. These clearances have been used to brief the sector on new information security threats and have provided useful information for the sector to implement effective risk controls to combat these threats.

AUTOMATED THREAT INFORMATION SHARING

The sector continues to make significant progress toward increasing the speed and reliability of its information sharing efforts through expanded use of DHS-funded open specifications, including Structured Threat Information eXchange (STIX™) and Trusted Automated eXchange of Indicator Information (TAXII™).

Late last year, the financial sector announced a new automated threat capability it created called "Soltra Edge", which is the result of a joint venture of the FS–ISAC and the Depository Trust and Clearing Corporation (DTCC). This capability addresses a fundamental challenge in our information sharing environment: typically the time associated with chasing down any specific threat indicator is substantial. The challenge has been to help our industry increase the speed, scale and accuracy of information sharing and accelerate time to resolution.

The Soltra Edge capability developed by the sector removes a huge burden of work for both large and small financial organizations, including those that rely on third parties for monitoring and incident response. It is designed for use by many parts of the critical infrastructure ecosystem, including the financial services sector, the healthcare sector, the energy sectors, transportation sectors, other ISACs, national and regional CERTs (Computer Emergency Response Teams) and vendors and services providers that serve these sectors.

Key goals of Soltra-Edge are to:
—Deliver an industry-created utility to automate threat intelligence sharing
—Reduce response time from days/weeks/months to seconds/minutes
—Deliver 10 times reduction in effort and cost to respond
—Operate on the tenets of at-cost model and open standards (STIX, TAXII)
—Leverage DTCC scalability; FS–ISAC community & best practices

—Provide a platform that can be extended to all sizes of financial services firms, otherISACs and industries
—Enable integration with vendor solutions (firewalls, intrusion detection, anti-virus, threat intelligence, etc.)

With these advancements, one organization's incident becomes everyone's defense at machine speed. We expect this automated solution to be a 'go to' resource to speed incident response across thousands of organizations in many countries within the next few years.

IMPORTANCE OF DHS FUNDING AND STRONG OVERSIGHT FOR IMPROVED PARTNERSHIP

DHS is currently responsible for enhancing the security, resilience, and reliability of the Nation's cyber and communications infrastructure—a critical and expansive mission. In the realm of information sharing, DHS's role could expand further with increased information sharing following the implementation of the President's February 13, 2015 Executive Order to promote private sector information sharing. Should Congress enact legislation establishing a streamlined voluntary information sharing legal framework, DHS will likely receive additional information from private sector partners on cyber threats. This will increase the already existing need for a robust analytic capability at DHS to develop products, particularly at the unclassified level, that will be useful and actionable to its domestic and international stakeholder community, both inside and outside the government.

It is critical that DHS have the necessary personnel and technical tools to enable them to complete their mission. Last year, Congress passed additional personnel authorities for DHS to hire trained, qualified personnel to work in cybersecurity positions, which will hopefully make the recruitment and retention of qualified personnel more successful.

In this era of fiscal restraint, we also appreciate the need to ensure that appropriated funds are being spent in the most effective and efficient manner. We believe this is a role not only for senior DHS management, but Congress as well, as the ultimate appropriators of funding. This can strengthen DHS's cyber programs and provide sector stakeholders better information with which to defend their own networks and ultimately strengthen the security of our nation's infrastructure.

Overall, our assessment is that the financial sector's relationship with DHS is productive and directionally positive, with tangible successes that we believe are improving the protection and resilience of our critical financial infrastructure. Where there are programmatic gaps or implementation inefficiencies in the partnership, they are mutually acknowledged and addressed. Ultimately, we recognize that as our joint effort matures over time, we are never done, only better.

Mr. Chairman and Members of the Committee, this concludes my testimony.

EINSTEIN AND CONTINUOUS DIAGNOSTICS AND MITIGATION

Senator HOEVEN. Thanks to all three of the witnesses, and we will start the rounds of questions. We will be pausing at 2:49. So I will start, but we may have to pause, in terms of your response.

I want to start with Mr. Ozment. My first question goes to the rollout of both Einstein and CDM. Where are you in terms of the rollout? There has been obviously some concern about the pace at which these are being deployed across all government agencies, and also the state of the technology.

So in terms of the dot-gov domain, talk about the rollout about CDM and Einstein. Do we have it across all agencies? If not, why not? And when will it happen? And is the technology ahead of the attacks that are coming our way? And you have 2 minutes, so you can just get started. I may interrupt you, but if you want to start?

Mr. OZMENT. Thank you, Mr. Chairman. I am happy to do it, and I, certainly, understand and am very happy to be interrupted when the time comes.

If you don't mind, I would like to start by giving an overview of what the Einstein and CDM programs do and how they tie together and where they are, to your question.

They are complementary elements of our strategy to secure the Federal civilian executive branch. Einstein 1 provides boundary or perimeter-based protection services—I'm sorry, Einstein 1, 2, and 3 do.

So a useful analogy is that of a military base. If you are defending a military base, first you limit the number of roads coming in and out of it. Then you put security where those roads enter the base.

Einstein 1 is like providing a license plate reader at the roads into and out of the military base. So think about that base as a single department or agency. Einstein 1 is tracking who is entering and leaving the base.

Einstein 2 adds, if you, will, a watchlist function. This car is not allowed to enter the base. It doesn't stop the car, but it sets off an alert, a bad guy came into the base. And, of course, it is more complicated than just looking for specific license plates, but it gives you a sense of the program.

Einstein 3 is a different approach. Einstein 1 and 2, those intrusion detection systems, are built on unclassified information. Einstein 3 also takes advantage of classified information. And so to make that work effectively, rather than build this classified capability at every agency, at every military base, if you will, we pulled it back to the highway.

Senator HOEVEN. Mr. Ozment, I am sorry. I am going to have to stop you now. It is 2:49.

At this time, I would like to observe a moment of silence. Let this time serve as an opportunity to reflect on the survivors, those who were loved and lost, and our resilience as a peaceful Nation.

So please, a moment of silence.

Senator HOEVEN. Thank you.

Again, to all the victims and their families in Boston and those from around the country who were affected, and even beyond our shores, our hearts and prayers go out to them once again. And we are reminded that we do face real threats in this country.

And, of course, that is a very important part of our mission, to help protect against those threats. We are also reminded of the strength and resiliency of our country and the resolve of our people.

Senator Shaheen, any thoughts you might have before we proceed?

Senator SHAHEEN. I think you said it very well, Mr. Chairman.

Senator HOEVEN. Chairman Cochran.

Senator COCHRAN. I have nothing further now.

Senator HOEVEN. Thank you, Mr. Ozment. Proceed. You were just using your military base analogy, which I thought was excellent, so please continue.

Mr. OZMENT. Thank you, chairman.

So with our analogy here, we have Einstein 1 and 2 set up at the boundaries of the military base, essentially reading the license plates of the cars entering the base, setting off an alert if a bad guy drives in. Einstein 3 is pulled back to the highways, the highways that serve multiple bases—in this case, the Internet service providers (ISPs).

Now, Einstein 3 will be built at a handful of Internet service providers that serve the vast majority of Federal Government traffic. It only applies to the traffic to and from the Federal Government at those Internet service providers.

Einstein 3, think about it as a guardhouse. At that highway, as we have cars heading toward the bases, the guardhouse can actually stop. It checks the license plates. It looks for anomalous behavior of the cars and can actually stop cars that it believes to be malicious.

It is also a platform, if you will. So you have built a guardhouse. You can put up a gate. You can put up security cameras. You can have guards there. You can, in fact, do different things at this guardhouse to adapt to an adopting threat. That is exactly the case with Einstein 3.

With Einstein 3, we have started with two security capabilities at this guardhouse, but it is also a critical platform that we can use to work with the private sector and incorporate new and innovative security technologies at the guardhouse itself.

Now, that is great. That is security at the perimeter for these bases that are our departments and agencies. But, of course, anytime you are working in security, whether physical or cyber, you want a layered defense. You don't want to defend just at the perimeter. You also want to worry about security inside the base.

CDM, Continuous Diagnostics and Mitigation, is part of our interior defense for the departments and agencies. In our analogy of a base, this program, CDM, is essentially the tools of the guards that go around the inside of the base for security purposes. CDM also has multiple phases.

The first phase is the equivalent of going around and making sure that the doors on buildings are closed and locked, windows are locked, the basic security of the infrastructure is there. Phase two will focus on identity management and will essentially be going inside each building and saying, are the people inside this building, which is inside this base, are they people who are authorized to be here? With additional capabilities, we will add different security technologies to this interior guard, if you will.

So where are we on these two programs right now? Einstein 1 and 2 have broad perimeter coverage across Federal civilian departments and agencies.

I say that specifically to exclude the Department of Defense and the intelligence agencies. Those are excluded from this program.

But for civilian departments and agencies, Einstein 1 and 2 reach between 80 percent and 90 percent coverage. Now the reason for not having full coverage there is every department and agency has more Internet connections. Most departments and agencies have more Internet connections than they want. So they are trying to consolidate down to a small number of connections where the security is. So as departments and agencies further narrow their extra Internet connections, our coverage will go up.

For Einstein 3, we are in the middle of building out that capability. We have built it with two Internet service providers, Verizon and CenturyLink. Those two service providers give us coverage for about half of the Federal civilian departments and agencies by personnel.

Now, there are two parts to Einstein 3, which is we build the capability and then we work with departments and agencies to route their traffic through the capability. So we can build the guardhouse, but if they are not sending their traffic to the guardhouse, it doesn't work.

So with Einstein 3, about a quarter of the government is routing some or all of their traffic to our guardhouses. So a quarter of the government is receiving at least one protection.

We have just put the second ISP online, so we have really just expanded the capacity from a quarter of the government to half. Now we are working with departments and agencies to take advantage of that new capacity that we just rolled out. Then we are continuing to work with ISPs to build out this capability at other ISPs.

Switching to CDM, that inside-the-perimeter program, as I mentioned in my opening statement, just yesterday we announced the second of a set of awards for this program. We now have awarded to departments and agencies that constitute more than half of the departments and agencies.

Now this is announcing the award. Now that we have the tools and services, we need to deploy them. That will take some months yet, but that is a particularly important milestone that I am very proud that we have achieved.

So with that, hopefully, I have answered the question, chairman. If it there is anything else I can add, I am happy to do so.

Senator HOEVEN. That was really well done, in terms of actually explaining how this stuff works to someone who doesn't work in your field. Certainly, far from an expert. I didn't even want to use the term "expert." But this is complicated stuff. That was a good job of explaining how it works, and I appreciate that.

I am going to follow up on that question, because I think you went a long way down the trail, but you did it in an understandable way, and I appreciate that.

At this point, I will turn to Senator Shaheen.

INCIDENT REPORT

Senator SHAHEEN. Thank you.

One of the challenges, and I think we talked a little bit about this when I visited the NCCIC, where the NPPD operates and where you all are working, is how to quantify what the challenge is and how to track what is happening in a way so that we can prioritize resources and help explain what the threat is to the Nation.

So I was interested to see that DHS received over 97,000 incident reports, and I am going to ask you to explain what those are, and issued 12,000 actionable alerts, and detected 64,000 vulnerabilities, responding to 115 incidents in 2014.

So those are numbers that I think show, to some degree, the extent of the challenge, but it is hard to understand exactly what that means out of context. So can you try to put those numbers into some context and explain what that means and what we should be looking at to prioritize our response to those?

Mr. OZMENT. Absolutely. Thank you, Ranking Member Shaheen.

Regardless of where you get your data on cybersecurity, whether it is the statistics that we report on our activity, whether it is from

a private-sector security company and their reports, or the academic reports in this field, almost every report you look at will indicate that the problem is extraordinarily large in scale and growing. Now, no single entity has a lens on the entire problem, so there is nowhere you can go to see everything at once. Although, certainly, we view that as part of the problem that we have to tackle, to improve that lens.

You mentioned some of the statistics. Let me, I think, provide some of the context within which to frame them.

Senator SHAHEEN. Great.

Mr. OZMENT. One of them is, I started in cybersecurity around 1998 and originally worked as a network operator. When I worked as a network operator, when we had an incident, it was a big deal. We pulled out all the stops. It was momentous in my life. I got no sleep.

Unfortunately, the world is such today that if you are a Fortune 1,000 company, this is no longer a noted or notable incident, just because somebody has intruded upon your company. In fact, quite the contrary. Every CIO or CISO (Chief Information Security Officer) I know operates under the assumption that somebody has already broken into their network and is, in fact, living and working on their network from abroad.

So we have moved from this understanding that mostly we are secure and sometimes people break in, to a world where we, by and large, now believe that mostly we are insecure and there is always somebody who has broken it. The challenge for us is how rapidly we can detect them and remove them.

CYBERSECURITY: GOVERNMENT AND PRIVATE-SECTOR UNDERSTANDING

Senator SHAHEEN. Can I just ask, how much of the rest of government do you think understands that reality?

Mr. OZMENT. I think, in the CIO community, and I will defer to my colleague Mr. McCormack on this, but I think it is very widely understood. I think even in the past 6 or 8 years, I have seen a dramatic increase in understanding and senior leadership. Now for the first time since I entered government, I would say that it is widely understood across senior leadership.

Senator SHAHEEN. Mr. Garcia, how widely do you think that is understood in the private sector?

Mr. GARCIA. The private sector, writ large, is not where it should be. For the financial sector, I think we have a fairly sophisticated understanding of, number one, the problem, and, number two, the business proposition for addressing ourselves, for investing in cybersecurity.

Just to give you one example, after DHS, I was an executive at a major bank. One of the things we tried to do was actually measure the value of our cybersecurity investment. So we just take one example where, are we getting our money's worth from all this information-sharing that we are doing and the resources that we are deploying toward it and the people as well? Let's take an example of having gotten one piece of data, one threat intelligence that we didn't know about.

We understood that that particular malware attack has the capacity to disable computers or to wipe the data clean or corrupt the

data in some way. And if we did not have that information, we could not have stopped it from happening. If it had just infected one division within the bank, maybe that is 1,000 computers, you are going to have to go back and wipe all of those thousand computers clean and reimage them. $500, $750 per computer and multiply that by 1,000 computers, 10,000 computers, and suddenly you have a real number associated with catching just one threat.

So when you build that out over time and you think of all the other ways that we can be investing in security, it isn't easy. It is sometimes an art. It is hard to prove the negative, that because we didn't see anything, nothing happened. But those methods for measuring progress are improving and at increasingly higher levels within corporate America. So we are making progress.

Senator SHAHEEN. I will get back to you.

Can I get Mr. Ozment to finish answering that question, putting numbers into some context?

Mr. OZMENT. So I think a key thing to emphasize from us is, as we sit within my organization, we do not believe that we have scaled to the level commensurate with the risk we are facing.

RESOURCES

Senator SHAHEEN. And is that a function of resources?

Mr. OZMENT. We are receiving the resources right now that we need, assuming that we receive, of course, the President's budget request. We think we are in good shape. Part of it is, you can only scale and grow so fast. It is a new field in the sort of national perspective.

Senator SHAHEEN. We can only grow so fast because we don't have the personnel, the technology?

Mr. OZMENT. Personnel is probably the biggest single holdup, and then just by the nature of organizations. If you grow organizations too rapidly, it is difficult.

The only other thing I would add is when you look across these, one of the things that can be confusing about the scale of numbers, and particularly people often report on attempted intrusions, that number has become, by and large, meaningless because attempting to break in is free. An adversary can try 1 million times per day against one victim and largely there is no punitive action that would deter them from doing it.

So adversaries automate their attempted break-ins and just go across broad swaths of the Internet. So we have stopped paying attention to a number that used to be an important signifier to us in this community, because, essentially, it is infinite now.

That being said, sometimes people hear these broad numbers and largely give up. They say that this problem is intractable. The flip side of this is we look at intrusions that we know about. And again, whether it is our data or a private-sector company's data, the vast majority, 80 percent to 90 percent of the incidents that you learn about, could have been prevented by basic best practices.

That is one of the reasons we focus so much of our efforts on best practices. It is not the most exciting topic in the world, and it often receives less attention than incident response or even information-sharing, which can be more dynamic. But it is the basic thing that

we need organizations, whether government agencies or companies, to take those actions and sort of raise the bar for our attackers.

Senator SHAHEEN. Thank you.

Thank you, Mr. Chairman.

EINSTEIN AND CONTINUOUS DIAGNOSTICS AND MITIGATION: LEVEL OF SECURITY

Senator HOEVEN. Mr. Ozment, go back to the analogy you were talking about before, or basically the rollout of CDM and Einstein in terms of deploying them across all agencies, before we get into the private sector aspect.

Will these technologies put us ahead of the technologies that attackers use to try to infiltrate our systems? Are you ahead now? Are you staying ahead? Because obviously hackers are constantly improving their ability to undertake these attacks.

Mr. OZMENT. Certainly. One of the things you will observe from me is that I am a former computer scientist and programmer, so I think in lists. So I have three answers for you on this question.

The first is, for Einstein itself, the technology of intrusion detection and intrusion prevention is not a new technology. In no way would I call it innovative or cutting-edge. Neither is a fence. But it is still a core component of a layered protection for protecting a physical installation.

That being said, these technologies depend upon the information that is fed them. So first, it is a necessary but not sufficient technology. Second, what is innovative about what we are doing is the information we are putting into these systems, particularly for Einstein 3, the classified information that we derive from our partners in law enforcement and the intelligence community. That information helps us stay ahead of our adversaries and keep them out of our networks, even if we haven't seen them before.

The final aspect of it is that it's necessary to have a fence, and it is great that our fence uses classified information that makes it a cutting-edge fence. It is still not sufficient. So the final aspect of Einstein 3 is that it is a platform that we have made this guardhouse at the highway that serves multiple bases, and we can install new technologies on the guardhouse as we go.

We are even now exploring what are the next technologies to put into the system to continue to build out its capabilities. That is for the Einstein program.

For the CDM program, it is a similar evolution. First, build the basics that every organization should have, but, unfortunately, not every organization does have, and then add the more sophisticated technologies on top of it. That first component of CDM, which is that guard inside the base checking doors to make sure they're locked, a big part of that is ascertaining whether or not computers are vulnerable, meaning whether they have been patched.

Again, there are numerous private-sector reports on this: that 80 percent to 90 percent of intrusions takes advantage of a vulnerability that we have known about for at least a year, and that there is a patch, a fix for it, widely available.

So this is the basic blocking and tackling of security. And if we haven't rolled out the tools that let us do it systematically, measur-

ably at scale, then we can't build anything more sophisticated on top of that.

So that is what the first phase of CDM tackles. The second phase, as we start looking at who is in the building and should they be there, starts to be more cutting-edge.

Senator HOEVEN. Again, going back, agencies have their own security, and then you come along and provide CDM and Einstein across all agencies. But to the extent that some of these agencies aren't yet fully using both of those programs, as you mentioned in your testimony, they still have taken some steps for security. Maybe some aspects of their software, their number of access points and so forth which don't fully comply with some of the best practices that you talked about and some of your security protocols, but some steps. So, how secure are they?

In other words, first, how secure are the ones where you have Einstein and CDM deployed? What is your opinion in terms of how good their security is? Are they secure, and are you comfortable? And then what is the state of security for those agencies that haven't deployed them yet?

Mr. OZMENT. Unfortunately, it is not quite as simple as saying that agencies that have CDM and Einstein are secure and those that lack them are insecure. It varies widely, depending on an agency's capability and investment in cybersecurity.

One of the purposes of Einstein and CDM, though, is to provide a basic level of security, so that we can be comfortable that we have that baseline of security across the Federal Government, regardless of the agency's skill or resources at a given moment.

With respect to the Einstein program, another key advantage really that both programs provide us is agencies can and should be effective at seeing what is happening to them on their network, but we believe that we will be able to identify attacks that are not visible within one agency because it is a small anomaly within one agency, but when you see it across seven agencies, you recognize that it is something bigger. It is putting together the pieces of the mosaic and understanding the broader picture of what you see.

And then the only thing additionally I would add, just to reassure you, on the Einstein program, we are providing something around departments and agencies that couldn't have existed before. They may have their own intrusion detection systems, but, again, the systems would be local and don't use classified information. With CDM, some agencies have built out parts of this capability before and we are not duplicating what they have already built out. The CDM program has, frankly, a fairly wide variety of vendors and the reason we have that is because our goal is to fill in the gaps of what agencies may already have rather than replace what they bought.

EINSTEIN AND CONTINUOUS DIAGNOSTICS AND MITIGATION: DEPLOYMENT SCHEDULE

Senator HOEVEN. When will all agencies have both? What is your goal?

Mr. OZMENT. With CDM, we have broken the agencies essentially into five buckets and we are going through each bucket awarding and deploying to those agencies.

So you just heard that we awarded the second bucket. We intend to award the fifth bucket by the second quarter of fiscal year 2016 and then essentially have built out that final bucket over the next two quarters. So we will have all of these buckets both purchased and built out by the fourth quarter of fiscal year 2016.

Now, something I do want to flag, however, is we have grouped agencies in part by size. So as we get to that final bucket, it is a large number of agencies; it is an extremely small percentage of the Federal Government by personnel.

So as you heard, with just two buckets, we are already over 50 percent. As we go through these buckets, the remaining buckets get smaller.

Senator HOEVEN. Is that for both programs?

Mr. OZMENT. I'm sorry?

Senator HOEVEN. Is that for both programs?

Mr. OZMENT. So that is for CDM. Einstein is a different approach.

Einstein is based on the ISP. If we were to build classified capabilities at every agency, it would be prohibitively expensive. So by pulling back to the highway and building at just a handful of ISPs, we can keep our costs down and still cover most of the Federal Government that way.

Right now, as you know, we have two of those ISPs providing service. We are now talking to the third ISP to get it under contract. We hope to have all of our capabilities built out with these ISPs by the end of fiscal year 2017.

Again, as you get toward the end, you get declining additional coverage of the government. We get the biggest chunks early.

One thing I want to highlight for Einstein though is we build it; they still have to come. So that is why, for example, right now, we have 50 percent capacity for the government, but only 26 percent taking advantage of a countermeasure.

Now that does not mean that agencies are being resistant. We built the capability. Now they have to modify their networks. It takes some time.

But I will tell you that we do have challenges with agencies who are concerned about whether the legal authorities in this space are clear. They want the protection. They very much would like to be part of the program. But they have statutes that were not intended to address this issue, that were developed for entirely different purposes, but that restrict who can see the information that that agency receives.

So there is all sorts of protected information throughout the government. It may be protected because it was intended that it never be accessible to law enforcement or to regulators, you name it. Some of those statutes are broad enough that agencies are concerned whether or not they violate the statute for this program to be operational.

So that is why we have come to Congress to ask for a positive authorization of this program.

Senator HOEVEN. Thank you.

EINSTEIN AND CONTINUOUS DIAGNOSTICS AND MITIGATION: DHS-WIDE PROTECTION

Senator SHAHEEN. So, Mr. McCormack, are all the agencies within DHS protected?

Mr. MCCORMACK. Absolutely. I just wanted to bridge onto several things that were discussed with Mr. Ozment.

One is, just in my assessment of the maturity of the CIOs and their awareness of cyber, being a component CIO and Department CIO at the Department of Justice (DOJ) and here at DHS, absolutely, there is sensitivity to that. I think what OMB has done recently with their cyber assessments where they are having discussions with Department leadership, I mean, organically, we do that now because of the nature of what we do at DHS, so we are always having those conversations. But those are very intimate conversations going across all departments and agencies, at this point. So I think that has been very successful.

One other thing on the Einstein, I think another thing that makes that very powerful is not only do the guardhouses have that level of sophistication, using Andy's metaphor, but the fact that these guardhouses are now going to be able to talk to each other at machine-speed and inform each other is very powerful as well. That is a big improvement as to the configuration that we have today.

Last, I would say, on the CDM, as we discussed earlier, as I said in my opening statement, we are early adopters of both of those programs. For instance, for us, in Einstein, they just implemented the Einstein capability in the ISP that we happen to use.

Now we have to reconfigure our network, as Andy was talking about. We will have that done approximately at the end of May, so we will be routing our traffic through that and taking advantage of those capabilities.

That is not to say that we don't have some of those capabilities now. We don't have the classified capability that we are very interested in getting because that is a higher order of protection. But most departments and agencies have built some type of capability using commercial services, et cetera, to do the protection that you asked about.

On CDM, we're an early adopter of that. We were in phase one. They just awarded phase two. So we are in the process of implementing that. That will take several months to implement.

We do have continuous monitoring throughout the Department. It is not as homogenized as we would like to have it, and this is going to allow us to fill in those gaps and give us some capability that we hadn't had before and give us that sort of broad dashboard so that we can quickly look at where our gaps are and focus our attention on that. So that is the priority issue that you had spoken about, so we can narrow our focus and know where we have some gaps and quickly address those concerns.

Senator SHAHEEN. Mr. Ozment, is the Senate covered?

Mr. OZMENT. So the Senate is not covered in this program. We are very happy to talk about the Senate, but our understanding is, for concern of separation of branches, that the legislative branch is

not interested in the programs. But if there is a change in that opinion, we are extraordinarily happy to work with you.

INCIDENT DETECTION AND RESPONSE

Senator SHAHEEN. Okay. So back when the Foreign Relations Committee took action on Syria in 2013, one of the advisories that we got was that there was information suggesting that the email accounts of those of us on the committee might be hacked into. Where did that originate? Was that DHS that would have gotten that alert and then sent that to the Senate to act on?

Mr. OZMENT. So I can't speak to that particular incident, but that type of information can originate in a number of ways. It can originate in a law enforcement investigation. It can originate through intelligence.

When we, DHS, my organization, when the NCCIC deploys an incident response team to a victim, they may, as they help that victim, discover information that the adversary has been on another victim. So there is any number of ways that we can find out about new victims of intrusions.

One of the things that we have all worked on for the past few years in the executive branch is making sure that we do a coordinated, immediate outreach to those victims to let them know. I am happy to tell you that whereas 2 years ago we did not have a process for that, we have a process for it now and do a good job, not just of making sure the victim gets a knock on the door, but making sure the victim only gets one knock and not three knocks from three different agencies.

Senator SHAHEEN. So when I read off all those statistics earlier, and I talked about the 115 incidents that you responded to in 2014, is that the response to victims who have had a cyberattack? And what do you do when that happens? Call the agency and then do what?

Mr. OZMENT. So those are responses to a victim of either cyberattack or intrusion. We do tend to differentiate an intrusion from an attack that breaks things.

So we may have found out about those through any of the means I just mentioned.

What happens when we find out? We call a victim or sometimes a victim calls us. It can happen either way. So we let the victim know or they let us know. We offer our assistance.

That assistance can be as lightweight as our just telling them we have seen this before. Here's what we know about it.

Senator SHAHEEN. What do you do in a worst-case scenario?

Mr. OZMENT. Worst case scenario, we send a team onsite to help them figure out where in the network it is and essentially to kick the bad guy off the network and get them up and running again. Ideally, we do that with law enforcement.

Senator SHAHEEN. That is what I was going to ask. Can you identify the bad guy and then do you report that to law enforcement in some way?

Mr. OZMENT. So we do not focus on identifying the bad guy, although we can find information that gives us hints and we can pass that on. We are sometimes called by companies who are unwilling to have law enforcement onsite, but our strong preference

and really our belief is that the right thing to do is to be onsite with law enforcement—law enforcement focused on the investigation, the attribution, how to catch the bad guy; us focused on figuring out where in the network the bad guy is, getting them off of it, getting the company or the agency up and running again.

Whether that is the Secret Service or the FBI or Homeland Security investigators, if we are out with a victim, we will be encouraging them every day to bring in law enforcement.

Senator SHAHEEN. Thank you.

INFORMATION SHARING

Senator HOEVEN. I would like to shift to the state of information-sharing. So I would like to get Mr. Ozment's sense of where we are in terms of timely, actionable information-sharing, public sector, private sector.

Mr. Garcia, the same question to you.

In any order, whoever wants to go first, fire away.

Mr. OZMENT. Okay, I will go first, I guess.

I actually want to break information down into three buckets again.

One is the in-person collaboration and exchange of information, and we cannot minimize the importance of that, because so much of knowledge in complicated spaces is tacit knowledge that is best shared when you engage with people directly. But it doesn't scale. So while we have to do that, that is far from sufficient.

Next is what I view as sort of the analytic reporting, which is contextual information that helps the recipient understand broadly what is going on. An example of this would be a report talking about attacks that are targeting these three sectors. They are broadly taking these approaches. We think they are after this type of information, or this is the goal they are trying to achieve. It may or may not be actionable in a tactical sense, but it gives that strategic context that helps the recipient understand what is going on.

Third and final is tactical information-sharing, what we often call cyber threat indicators that are the actionable things that a recipient can use to protect themselves.

We have programs in all three areas, and I think all three are necessary. A lot of the focus right now is on that third area of tactical information-sharing, so I will focus on that. But I do know that we also put a lot of effort into those first two areas.

So for that tactical information-sharing, that is the type of information-sharing that we can make happen at machine-speed and what we have been very focused on doing. So starting over 3 years ago at DHS, we realized the need that we would have to share these indicators, we would have to share them in an automated way and do it at machine-speed, and that there was no standard by which to characterize them and to share them. So we started that work over 3 years ago.

That led to the STIX (Structured Threat Informaton eXpression) standard and the TAXII (Trusted Automated eXchange of Indicator Information) standard. STIX is how you describe the information to be shared. "I am sending you this piece of information. This is what it means. This is how you use it. This is how you have to protect it. And this is how you share it, if you like." So it gets quite

complicated, but it is the standardized language for describing all those things.

TAXII is how computers tell each other that at machine-speed.

So we started, 3 years ago, developing those standards. In 2013, we started releasing all of our products in this STIX format, this machine-readable language. We were not yet sharing it at machine-speed, but when you got it, you didn't have to type it in. You could feed it to a program that could understand it and then read it as a computer would read it.

Then a year ago, in February 2014, we started a pilot with the Financial Services ISAC (Information Sharing and Analysis Center), part of the FSSCC (Financial Services Sector Coordinating Council). And with the Financial Services ISAC, we started this pilot where we would send information that was STIX-formatted with TAXII, so machine-speed, machine-readable information, back and forth.

We ran that pilot. It was very much successful. As a consequence of that, we have been building. We had a pilot scale system now. Now we want to serve a large swath of the private sector and the government. So we have to build a robust, scalable system. So we have been doing that. We hope to report good news on that in the coming weeks.

Senator HOEVEN. Mr. Garcia.

Mr. GARCIA. Yes, sir, Mr. Chairman. I agree with everything that the Assistant Secretary said. I would add two pieces to that. One is process, and the other is relevance.

Our information-sharing engagement with the government from the financial sector is good and getting better. As I said in my opening statement, where there are gaps or inefficiencies, they are acknowledged and we are addressing them. We have a working group that involves our sector-specific agency, the Treasury Department, as well as DHS and other Federal agencies, and the financial sector working on these process issues. That is very simple questions like: Who is on the phone tree, and in what order? And how does information generated within DHS actually get over to the Treasury Department? And how does Treasury actually get certain information from the NSA? And who has authority to share it outward? What about the tear line? The tear line is you have a classified section and unclassified section. How do you split those two so you can actually get the actionable information to the owner and operator of the bank or insurance company to actually deal with it?

So the process is not easy. The government is not monolithic; the financial sector industry is not monolithic. And getting through all that vast wiring diagram to get information out in time to the right people is a challenge. It always will be. It is a systemic issue that is just the nature of the beast.

The second is relevance. As the threats evolve, as technology evolves, and vulnerabilities, the way we deal with those is different. Where we have taken care of one problem, a new one emerges. I have been on the receiving end when I was at DHS, and I thought we had some pretty juicy information about some classified threat, and I shared it with a cleared industry official, and he said, "Are you kidding? I have known about that for 6 months." So that wasn't relevant.

So it is a constant process of engaging with the partners to know, does this piece of information work for you? Is this relevant? Can you do something with this?

So three times a year, we have very large meetings between industry and government where we have classified sessions. Every month, the Treasury Department is holding classified sessions with cleared industry people. That exchange is constantly going, recalibrating and recalibrating what matters.

Senator HOEVEN. So you feel that with the ISAC and the industry—in this case, the financial services industry—it is working? You feel that you have generally good security and you are working to make it better with information-sharing and response and coordination and technology deployment, both individually and some of these technologies that cross businesses or agencies?

I mean, it is going the right way? You feel like it is working?

Mr. GARCIA. It is going the right way. As I said at the start, we are never done, we are only better. I think the STIX and TAXII open specification that Andy referred to is very important for us because it is laying out an open standard for all industry to apply to their information-sharing. It is simply how you describe the information and how you transport it in a machine-to-machine way.

That is a good thing. That is taxpayer dollars well spent.

Senator SHAHEEN. You talked about the fact, Mr. Garcia, that the financial services sector is ahead of much of the rest of the private sector, in terms of dealing with cyber threats.

Why do you think that is? And how do we get folks in the utility sector and some of those other areas where they haven't responded as quickly to be aware of the challenge and to work with them to get them up to speed to where they ought to be?

Mr. GARCIA. I certainly don't want to claim that the financial sector is far ahead of everyone else. But first of all, the financial sector is heavily regulated so there are very explicit requirements that we have for ensuring the safety and soundness of the financial system.

Senator SHAHEEN. So are utilities, though.

Mr. GARCIA. Indeed. The second point is that it is the Willie Sutton factor. That is where the money is.

The financial services sector is a symbol. It is a very large and potent symbol of America, and it, therefore, becomes a target naturally on the global stage.

But I think because we recognize that we as a sector are targeted every day, that it is not a competitive issue among us. We don't say, "We are more secure than the other bank. Come bank with us." We recognize that it is the three musketeers. We have to be one for all and all for one so that we can form a collective intelligence, a collaborative posture, to take on the bad guys.

So because of that, we have formed a very strong trust community. As I said at the start, strength in numbers. If you don't have strength in numbers, you are not going to be able to defeat the adversary, period.

I think that that notion of trust community might not be as mature in other sectors. They certainly are accelerating that. There is greater recognition.

And then finally, I think we are doing a lot of work sector to sector. The financial sector is heavily dependent on the electric sector. The electric sector is dependent on financial services. We are all dependent on telecommunications, information technology. So there are critical interdependencies that really illuminate those vulnerabilities, those shared vulnerabilities.

From a business-to-business standpoint, government is important in helping us deal with this, but this is a business-to-business issue. How do I know when the lights are going to come back on? And my electric company better have an answer for that.

So we are dealing with those issues both in terms of business and in terms of policy and critical infrastructure protection.

Senator SHAHEEN. Senator Hoeven was asking about information-sharing. I was here—I think you were here, too, Senator Hoeven—several years ago when there was an effort to get a cyber bill through the Senate. I think it broke down along, basically, the concern about sharing information as well as who was going to be in charge of holding that information and responding to it.

There is new legislation that has been drafted. Do you have a view on whether that is preferable and how the private sector might respond to that new legislation, and whether it is needed? I will ask you all that as well.

Mr. GARCIA. Yes. I couldn't comment on the details of legislation, but as a general matter, we are supportive of any information-sharing legislation that facilitates that.

While we believe we have very robust information-sharing within the financial sector, there remain concerns about liabilities.

Let's say I will share information with government. How do I know that it is not going to be used for regulatory purposes against me? Or I do take action on it and, it results in a class-action lawsuit because I didn't act within 10 days or some other potentially arbitrary standard.

So to the extent that Congress can provide levels of assurance to the private sector, that good-faith information-sharing that is intended to protect critical infrastructure will not go punished in some ancillary way, I think that is going to facilitate more information-sharing.

Information-sharing is not the silver bullet, but it certainly is the currency of our collective protection.

INFORMATION-SHARING LEGISLATION

Senator SHAHEEN. Mr. Ozment.

Mr. OZMENT. Let me start by actually emphasizing the point Mr. Garcia just made, which is information-sharing is critically important, but it is not a silver bullet. In fact, if you haven't implemented best practices, I can share information with you all day long and you have no way of implementing that information.

Senator SHAHEEN. Should legislation include best practices? Should it include a standard by which sectors should operate?

Mr. OZMENT. I don't think that we need that in statute. I think the government and private sector worked together to develop the cybersecurity framework over the last 2 years and that we are advocating for the voluntary adoption of that framework and see a lot of enthusiasm for it. So I think——

Senator SHAHEEN. Has anyone adopted it yet? The financial sector?

Mr. GARCIA. Yes. The framework that Andy was referring to was developed jointly between industry and the National Institute of Standards and Technology (NIST), so there is general support for it.

It is very broad in nature, which is the elegance of it, in the sense that it is very scalable. Very small community institutions, banks like Chairman Hoeven used to be the CEO of, can adopt the NIST cyber framework, as can major banks.

A lot of us have done the mapping. Many of the financial institutions have very sophisticated, robust cybersecurity practices and controls. And we see that we map very closely to the NIST framework.

So I think we are there. I think the challenge now is to push that NIST framework out to the broader business community, particularly small and midsized institutions, because they are part of this ecosystem as well.

Senator SHAHEEN. Are there other ways in which we are encouraging other industries and the private sector to adopt those standards?

Mr. OZMENT. We absolutely are. So a good portion of the programs that I have are focused, in fact, on encouraging the adoption of standards. We have requested increases in our budget this year for some of those programs.

One of them is the C-Cubed Voluntary Program. This is our cybersecurity advisers, so individuals who are across the United States help companies understand cyber best practices and adopt them. And also risk assessments.

So as I mentioned in my opening remarks, we will work with companies and do a risk assessment with them. Now, we can do that in person, and we also have downloadable tools that they can use to do their own. One of the reasons we do it in person is to give us a better sense of the pulse of industry and where industry is.

So we seek to do more with us. They are a great educational tool, both for the infrastructure or the company that receives it, and, frankly, they help us very much understand industry's needs.

So we have multiple programs where we are out there. We are also working with the sectors and the sector coordinating councils to do sector-wide risk assessments but also to work with them and customize a cyber framework to their sectors' individual needs.

There is a lot of great work going on in the space. And, frankly, we are seeing a level of adoption and energy around the framework that I would not have even hoped for 2 years ago.

Senator SHAHEEN. That is encouraging. Thank you.

STAFFING: RECRUITING AND RETAINING

Senator HOEVEN. Okay, we will try to wrap this up now, either in one or possibly two more rounds, but maybe we'll just set this round up to go a little bit longer and see if we can't bring things to conclusion.

A couple different questions that I have. I am going to go to Mr. McCormack and just ask, in terms of staffing, how are you doing in terms of recruiting and retaining staffing for DHS agencies?

Mr. MCCORMACK. Thank you. Staffing is always an ongoing activity for us, and we certainly do appreciate the flexibility that we now have in our pay scale and the like. We are working very closely with our CHCO (Chief Human Capital Officer) organization to go through the necessary processes, to do the skills assessment, etc., to implement that across the Department.

We also have direct hire authority, which really helps us in allowing us to pursue the variety of talent that we are interested in.

Retaining is always an opportunity and a challenge. As Andy and I were talking right before the hearing started, I just shared a small story. When I was over at DOJ, we had a young lady over there, very sharp, midcareer, who was actively pursued through LinkedIn. Out of the blue, she ends up getting an offer that is more than double her salary, moves her out of state, puts her up, lets her build her dream house, and changed her life.

We were honored that—it is a big world—and of all the places across the world that they could come, they come right to the Federal Government. That is the flattering part of it. The challenge is that we lost a good employee there. So that is always a real dynamic that we have to work with.

So how do we address that? Well, we continue to recruit. We continue to grow. We have a lot of techniques to do that. We are working very closely on that. But that is a real opportunity for us, to continue to build our workforce from the lowest level up to the senior level and continue to bolster that workforce to deal with the adversaries. It is a real opportunity for us.

Senator HOEVEN. Do you feel you are in a position to do that?

Mr. MCCORMACK. Yes. I think we have all the tools in place. You all have helped us with that. So we really do appreciate that. That is an ongoing pursuit. That is a constant, continual activity.

As we grow our organization and grow the level of skill set that we need, that is just an ongoing maturity curve that we are going to continually face.

Senator HOEVEN. Mr. Ozment, the same question.

Mr. OZMENT. I too would really focus on the workforce issue and really emphasize the importance of you and the Congress acting in December of this year and passing, in fact, two bills related to the DHS security workforce. So I truly thank you for that.

As we implement those bills, that will be incredibly helpful for us in sustaining our cybersecurity workforce. There are two sort of additional considerations that I would put on the table for that.

First of all, ultimately, those bills and that effort will help us enormously in recruiting and retaining great talent. But I will also tell you, from my organization's perspective, when I look at my cybersecurity talent that I recruit, I do not look at them and think, this person will be with me for a full government career. I think this person will work with me. They will contribute a great deal. They will learn a great deal. At some point, they will likely circulate to the private sector. And then, hopefully, I will catch them again at a different point in their career.

That is a different model of government service. It is not a bad model. It is just one that we have to adjust to and build our workforce processes to accept.

The second thing I would say is, in addition to the tactical problem of how we hire for ourselves, we also have to worry about, of course, building a national workforce so that Mr. McCormack and I don't have to just poach from each other or from other companies, but, in fact, there is a broader talent pool available that we can all hire and draw from. That is where our cybersecurity education and awareness efforts come in.

Senator HOEVEN. Do you feel you have the ability to get what you need? Yes or no?

Mr. OZMENT. Yes. Yes, sir. Thank you.

INFORMATION-SHARING ORGANIZATIONS

Senator HOEVEN. What is the difference between an ISAC and ISAO (Information Sharing and Analysis Organization)?

Mr. OZMENT. We heard two things from the private sector about information-sharing organizations. One, a lot of companies that were in ISACs, most companies in ISACs, feel really positive about them. But there were a lot of companies that said, I don't fit in an ISAC.

The ISACs were constructed since 1998 along sector-focused lines. So it would be the financial services ISAC, electric subsector ISAC, you name it.

There are companies that said, I just don't fit. I don't see myself in one of these sectors, or I see myself in all of these sectors, or I have trust relationships with people in my city and I want to share with them and have them be my hub. I don't want to be part of the sector construct.

Essentially, in the government, we said, why are we imposing a government hierarchical structure on you? We should let you, the private sector, organize yourselves as you see fit, and we'll work with you.

So ISACs continue to exist and are incredibly valuable. ISAOs are new organizations for people or companies that are not interested in the traditional ISAC approach and want to form a different type of group.

Senator SHAHEEN. That is a really bad acronym.

Mr. OZMENT. That is very true. I apologize.

Senator HOEVEN. Are there any good acronyms in cybersecurity?

Senator SHAHEEN. Maybe not.

Mr. GARCIA. If I could put a fine point on it, all ISACs are an ISAO, but not all ISAOs are ISACs.

Senator HOEVEN. ISACs are industry specific. ISAO is something else.

Mr. OZMENT. Any shape and size.

Mr. GARCIA. And it could be for-profit. ISACs are not-for-profit.

CYBER CAMPUS

Senator HOEVEN. I am concerned about the civilian cyber campus concept, the cost and idea of putting everything in one place. I would like each of you to comment on that.

Mr. Ozment, why don't you start? But I want all three of you to comment on that. I have concern about the cost. I have concern about trying to put everything in one place.

So please comment on that.

Mr. OZMENT. So all departments and agencies that are involved in the cybersecurity mission have agreed in concept with the vision and goals and objectives of the cyber campus.

It is planned to be a federally owned and operated facility that will house as original anchors DHS and DOJ cybersecurity elements. Our hope is that the campus will lessen and streamline the costs of operating what are currently dispersed and largely leased facilities while simultaneously enhancing unity of effort. Sometimes there is no substitute for being able to walk down the hall and talk to a person face-to-face.

So we support the President's fiscal year 2016 request for $227 million in the GSA budget to began construction of the campus.

Senator HOEVEN. Do you have some kind of cost analysis that shows the relative cost of one consolidated campus versus multiple sites? Have you done a cost-benefit analysis where we can actually compare the costs?

Mr. OZMENT. I would have to defer to GSA for that broader analysis.

Senator HOEVEN. Okay. That would be something I would want to see.

Mr. McCormack.

Mr. MCCORMACK. We also support the concept. As an agency, we wouldn't house our folks in there. We would continue to house our folks in our configuration as we have today, but we are obviously very interested in the information that we would share with the cyber campus and the information that would come out, very similar to what we do with NCCIC. We actually have someone installed in NCCIC, but our whole workforce isn't in the NCCIC.

So certainly, we support the concept, but we as an agency, and I am sort of speaking on behalf of any agency, that the internal traditional cybersecurity organization that is protecting that agency doesn't plan on being in the cyber campus.

Senator HOEVEN. Mr. Garcia.

Mr. GARCIA. Mr. Chairman, I am afraid I am not well enough informed on the program to opine.

Senator HOEVEN. It was primarily for the other two, but I just wanted to see if you had any thoughts on it.

Mr. GARCIA. Thank you.

Senator HOEVEN. Okay, thank you.

STAFFING: PAY

Senator SHAHEEN. Doesn't it, though, seem sort of counterintuitive that, when we are talking about issues around cybersecurity and around communicating virtually on the Internet, the only way we think we can do that is to build a brick-and-mortar campus? I mean, that seems to me like that sort of misses the point of what we are trying to accomplish here, that it would be better to put all that money into improving our IT systems rather than building a new building to put people together. You don't have to respond to that.

But I do want to zero in on the issue of more flexibility in the pay scale. I don't know which one of you said that, whether it was you, Mr. McCormack, or you, Mr. Ozment. But one of the questions that I had is, as we are looking at providing additional flexibility so we can recruit and retain people, how do we include performance as part of what we factor in, in looking at how we're dealing with that flexibility in the pay scale?

Mr. MCCORMACK. I think that was me that mentioned that. I think I also mentioned that the first thing they'll do is a workforce assessment. And then through that analysis, and the pay analysis, they will take things into consideration, such as performance, also job categories and the level of training and those things.

All of those things will get mixed together to make those determinations. I know that CHCO is working very closely with the DOD and the NSA, who has already done this, and using some of their policies and best practices. So I would expect all that to come together and then assess on the basis of, again, job performance. The type of job, the level of training, would then determine what type of pay or bonus or retention bonus, those sorts of things, that would be equated to that job position.

Senator SHAHEEN. Okay. I think, clearly, this is an issue as we try to retain talent and recruit top talent. I think a bigger issue is the one you talked about, Mr. Ozment, and that is that we are not educating enough STEM graduates in this country.

In New Hampshire alone, by 2018, we need 43,000 STEM graduates. So this is a huge issue and it is one we really need to think about, not just at the DHS level, but as we are looking at education and other ways that we can incentivize encouraging young people to go into those fields.

I am going to leave you out of this Mr. Garcia, because this is a public question.

To what extent and how do you all coordinate with DOD and with other agencies that have their own cyber centers?

COORDINATING WITH OTHER AGENCIES

Mr. OZMENT. So from the national and cross-governmental perspective, I can tell you we coordinate and collaborate deeply daily.

Senator SHAHEEN. So give me an example.

Mr. OZMENT. So every morning at 8:30, the cyber centers, the six cyber centers, have a phone call where they all walk through all the issues.

Senator SHAHEEN. Who are the six cyber centers?

Mr. OZMENT. NCI JTF, the National Cyber Investigative Joint Task Force, which is housed by the FBI; the NCCIC, which is part of DHS and NPPD; DCCC, the Defense Cyber Crime Center, and I will confess I don't know where it is geographically located, but the Department of Defense; the intelligence community——

Senator SHAHEEN. I have a diagram for this. Go ahead.

Mr. OZMENT. Okay.

Senator SHAHEEN. Now I see what you are talking about. Go ahead.

Mr. OZMENT. Indeed. The intelligence community. And I forget their acronym, forgive me, but their, essentially, cybersecurity team.

Senator HOEVEN. ICRC.

Senator SHAHEEN. You are good. You have seen this before.

Mr. OZMENT. ICRC (Intelligence Contingency Readiness Center). Thank you.

The U.S. Cyber Command Joint Operations Center and the NSA NTOC, the National Threat Operation Center.

Senator SHAHEEN. So you all talk first thing in the morning?

Mr. OZMENT. We all talk daily. Now, you know, depending on the mission, some of us have more recurring close ties than others. But we also have liaison exchange.

So on the NCCIC floor, for example, we have FBI liaisons, NSA, Northern Command, Cyber Command, Coast Guard, Homeland Security investigators, Secret Service. Those are the people there every day. Appearing about once per week or so, we have Treasury, Energy, and I am sure I am missing agencies. But we do a lot of liaisons and essentially swapping people.

And we have our people out at almost all of the centers as well.

Senator SHAHEEN. One of the things that you talked about when I visited the NCCIC was the fact that part of what you were looking for in this year's appropriation was to be able to anticipate and get ahead of cyber threats, to develop systems, whatever technology to be able to stay one step ahead of the hackers.

How do you share that kind of effort among all of those agencies? So if you develop some great way to keep the system secure, do you share that with DOD, and vice versa?

Mr. OZMENT. Absolutely. The problem is too big for us to be worried about hoarding solutions. I will tell you I literally spent an entire day yesterday, and my schedule is nowhere near as busy as yours, but I rarely spend a full day in one place. I spent a full day with our Science and Technology Directorate at the National Security Agency literally having this conversation: Here's what we are finding works on the technology front. What are you finding? Is there anything we know about that you don't and vice versa? We have to stay together, and we have to stay abreast of this threat.

And that is about the technology. On the actual information itself, Ranking Member, I failed to answer your question about information-sharing legislation, would you like me to give a few thoughts on that?

INFORMATION-SHARING LEGISLATION

Senator SHAHEEN. Yes, that would be great.

Mr. OZMENT. It is critically important that we in the government share among ourselves whatever information we have about cyber threats. We are doing, frankly, a pretty darn good job of it, far better than at any time during my time in government.

With respect to the cybersecurity information-sharing legislation, the administration believes that there should be one place where information from the private sector comes into government, and that is for two reasons.

One is just efficiency. We need to give the private sector one coherent, consistent answer so they don't have to decide between multiple choices.

The other is for privacy and civil liberties protections. The administration's proposal has a number of privacy and civil liberty

protections in place, but one of them is to narrow what we are talking about. That is to narrow it to cyber threat indicators. These are the things used by network defenders to protect themselves against cyber threats and incidents. A cyber threat indicator doesn't mean you've had an attack or you've been broken into. A good defender learns about cyber threat indicators just by defending themselves.

I got a phishing email. We were smart. We didn't click on the link. We identified it as phishing, but maybe nobody has ever seen it before. So I share the "from" address on this phishing email, and other people can protect themselves.

There is no incident. But now we are all better off protected.

So we believe that DHS should be the one portal by which this information comes into government. We believe that provides us with a better place to put in place privacy and civil liberties protection, because it is centralized and we can do our oversight there. The NCCIC is not law enforcement and it is not intelligence, so that gives comfort to those who are concerned about these issues.

At the same time, we are very up front that we are getting this information and we are going to share it with our government partners, because we all need to see it in government. So while we will put in place the privacy protections to ensure that what we are passing on is appropriate, it is also incumbent upon us at DHS to make sure we get it to our partners at all the other cyber centers and relevant agencies in near real-time, once those privacy protections have been put in place.

Senator SHAHEEN. So you think you can do that without legislation?

Mr. OZMENT. We absolutely need legislation to provide liability protection to the private sector, to give them the comfort to share information with us.

Senator SHAHEEN. Thank you.

Thank you, Mr. Chairman.

Senator HOEVEN. Thank you, Senator Shaheen.

And we're finishing up at about the right time because we have votes that will start at about 4 o'clock.

So I would like to thank all three of our witnesses. I think you did a really excellent job of laying out what you are doing. I think it was very helpful.

Again, it's a tremendously complex area. It's really important that we are focused on it as a Nation and doing the very things that you are doing both in the public sector and in the private sector.

As we take up this cyber legislation, it is going to be a real challenge. As Senator Shaheen said a minute ago, we tried once before to bring a bill forward, and there just is such a diversity of opinions out there in terms of how to do this. But it is a real challenge to get people with your level of expertise to work with policymakers to foster an understanding so that we can try to get this right.

It is very important that we do. So I think you are going to continue to be right in the middle of some very, very important work.

And I think, Mr. Garcia, as you said, or maybe it was Mr. Ozment, but I know all three of you recognize and appreciate that this is a process. It is not like we are going to do this and, gee,

it's fixed, and we solved that problem, and we'll go do something else.

This is a process, and we are going to continue to be working at it, for a long, long period of time, forever.

So again, thanks. Appreciate it very much.

Senator Shaheen, any closing comments?

Okay, so this will conclude our hearing today. I want to thank all of the witnesses for your testimony and for the work that you do.

ADDITIONAL COMMITTEE QUESTIONS

The hearing record will remain open for 2 weeks from today. Senators may submit written questions for the record. And we would ask that the witnesses respond to them within a reasonable length of time.

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

QUESTIONS SUBMITTED TO HON. ANDY OZMENT

QUESTIONS SUBMITTED BY SENATOR JOHN HOEVEN

THE MULTI-STATE INFORMATION SHARING AND ANALYSIS CENTER

Question. The Multi-State Information Sharing and Analysis Center (MS-ISAC) is also the only ISAC receiving direct Federal assistance. Last year they received $9.7 million from DHS, and this year the President's budget recommends a reduction to $9 million. Even though all 50 States receive bulletins from the MS-ISAC, only 24 States and one territory receive Managed Security Services.

What are some of the factors preventing all States from participating in the MS-ISAC?

Answer. Please note the fiscal year 2015 MS-ISAC budget is $12.956 million, rather than the $9.7 million the question references. All 50 States are members of the MS-ISAC, along with 679 local governments, three territories and eight tribal governments. Over the past few years, DHS has worked with the MS-ISAC to expand its Albert monitoring system, an automated cybersecurity information analysis tool, to all 50 States and six territories in fiscal year 2015, beyond the 33 States currently covered by the program. However, State participation in Albert requires a lengthy State approval and onboarding process. Many States have a process that includes approval from political appointees, Generals Counsel, and technology managers. Our primary stakeholders, CISOs, have an understanding of what Albert does but it can take time to get that information up the decision chain. Participation is completely voluntary and some States are determining whether the approval timeframe addresses their requirements.

Question. Will the reduction in funding reduce the capability for the MS-ISAC to provide its current level of service?

Answer. DHS will be working to right size the MS-ISAC budget based off growing DHS requirements and mission and in response to the level of State and territory participation in the cost-share initiative for fiscal year 2017 and beyond. DHS stands by the funding request and fully supports the President's budget. We worked through a process to request enough funding this year so that, along with the carryover, we would maintain our current level of support.

The MS-ISAC reduction in fiscal year 2016 exceeds the estimated cost share amount due to late fiscal year obligations. MS-ISAC obligations are done at the end of the fourth quarter of each fiscal year, thereby causing MS-ISAC to draw down against those prior year funds during the following fiscal year.

QUESTIONS SUBMITTED BY SENATOR THAD COCHRAN

Question. Could you explain to the subcommittee the function and value of developing and utilizing test ranges in the cyber domain?

Answer. Cyber test ranges fulfill two principal functions. First, test ranges can be used to test and evaluate cyber technologies, products, and systems. A test range

provides a suite of tools, processes and expertise to evaluate products under conditions that simulate operational use in order to capture key indicators of product performance. Test ranges can deploy networks of simulated government and commercial organizations with real world applications, services and content. For example, the National Cyber Range (NCR) deployed a simulated public Internet environment for USCYBERCOM's Cyber Flag exercises that provided realistic content from hundreds of foreign and domestic Web sites and instantiations of cafe, school, hospital, commercial, and home networks. Ranges such as the NCR can employ live malware, red teams, and classified tactics, techniques, and procedures tied to specific threat actors to evaluate whether and how a particular product mitigates basic and advanced threats. Within DHS, the Office of Science and Technology has partnered with the National Science Foundation to develop the Defense Technology Experimental Research (DETER) test-bed, which is used to test and evaluate cybersecurity technologies, including DHS-funded researchers, the larger cybersecurity research community, government, industry, academia and educational users.

Second, a cyber test range can be used for educational purposes. It can provide a virtual training environment where cybersecurity professionals can practice or demonstrate competency in a skill or ability. Training activities using a cyber test range also provide opportunities for operational teams to demonstrate their collective ability to analyze unique threats, work together to develop effective countermeasures, and to develop and test contingencies in an effective and timely manner.

Question. Does the administration's fiscal year 2016 budget request provide adequate resources to address evolving Department requirements and cybersecurity test capabilities?

Answer. The administration's fiscal year 2016 budget request provides adequate resources to address evolving departmental requirements and cybersecurity test capabilities. Furthermore, the request includes resources for several high-priority areas including: Incident response, analysis, automated information sharing and capacity building for non-Federal stakeholders. As part of our ongoing work to support the nation's cybersecurity, we work with industry and government partners to identify and evaluate open source tools and to develop technology to improve interoperability among tools to reduce the time for detection and mitigation of cyber events.

Question. Does the National Guard's unique flexibility to move between the commands of Governors and the President position it to be a particularly useful organization for defending against cyber-attacks?

Answer. The National Guard's diverse capabilities as well as their unique authorities under State Active Duty and title 32 make them a useful organization for defending against cyber attacks. Many National Guard members have cybersecurity experience from industry, making them highly qualified to understand the cyber threat to civilian infrastructure and serve as an effective partner with DHS. DHS regularly conducts exercises with the National Guard, including last year's Cyber Guard. In this 2-week exercise, DHS, the National Guard, and other interagency partners tested operational and interagency coordination as well as tactical-level operations to protect, prevent, mitigate and recover from a domestic cyber incident. On the other hand, the National Guard cannot be the only answer to our needs. For example, members of the Guard may be needed at their private sector companies during a cyber emergency, to mitigate the impacts at those companies. To the extent that the National Guard participates in cybersecurity activities, we would welcome their integration into existing response capabilities and established Federal and National Security response relationships while assisting in defending State cyber critical infrastructure.

Question. Your Department has been recognized for its excellent efforts in consolidating its information technology infrastructure and the savings these efforts will generate. Generally speaking, is it your judgment that it is easier to protect these assets when they are consolidated and accounted for or when they are scattered around the Government?

Answer. Consolidation improves the Federal Government's security posture and incident response capability. Consolidation of assets provides the opportunity for enhanced monitoring and situational awareness across the Federal enterprise. Economies of scale can be achieved by grouping assets to key strategic locations. But of paramount importance is the ability to identify and account for assets. Without that capability, security professionals are unable to monitor, patch, configure or otherwise secure them.

Question. While it is widely accepted that a foreign or terrorist cyber-attack on our electric grid, water systems, or financial systems could cause widespread damage and have detrimental effects on our economy and consumer confidence, there has been much discussion about how involved the Federal Government should be in defending infrastructure owned by non-Federal entities. How would you define

the threshold for what types of non-Federal infrastructure might qualify as "critical" for these purposes?

Answer. The Department of Homeland Security's National Infrastructure Protection Plan, or NIPP, defines critical infrastructure as the "assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof." The destruction or unavailability of any critical entity can have a cascading effect, either within a supply chain or across sectors. It is also true that while an individual disruption may not appear to meet a threshold meriting Federal interference, in fact, an immediate and coordinated Government response is essential to the continuity of critical services and to overall national security. The distinction between publicly and privately held infrastructure does not dictate whether it merits a Federal response to ensure continuity of services and mitigation of effects, including cascading effects.

Further, Executive Order 13636 section 9 directed DHS to identify critical infrastructure that could be impacted by a cybersecurity incident reasonably resulting in catastrophic regional or national effects on public health or safety, economic security, or national security. DHS therefore conducts proactive outreach to those entities on the section 9 list to ensure that they participate in available cybersecurity programs and are aware of assistance available from DHS and its partner agencies.

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

Answer. The Office of Cybersecurity and Communications (CS&C), within the National Protection and Programs Directorate, is responsible for enhancing the security, resilience, and reliability of the Nation's cyber and communications infrastructure. CS&C is working to create a cyber environment where a given threat, such as a malicious email, can only be used once before it is blocked by all other potential victims. This will reduce the frequency of successful cybersecurity exploitations and deter adversaries by increasing the investment required for a single successful attack. To this end, DHS helps companies develop information sharing capabilities, fosters the development of information sharing and analysis organizations, and serves as a portal to share cybersecurity information with a wide range of organizations.

Within CS&C, the National Cybersecurity and Communications Integration Center (NCCIC) provides 24x7 cyber situational awareness, incident response, and incident coordination capabilities. The NCCIC serves as a nexus between the private sector, Federal Government, intelligence community, and law enforcement. The NCCIC works closely with other Federal departments and agencies with additional cybersecurity responsibilities, including the FBI, the Department of Defense, and Sector Specific Agencies such as the Departments of Treasury and Energy. Further, a number of private sector companies and Information Sharing and Analysis Centers (ISACs) maintain seats on the NCCIC floor, allowing ongoing collaboration around cybersecurity threats, vulnerabilities, and incidents. Departments/Agencies and ISACs that have a person on the NCCIC floor at least 1 day a week: Department of Defense Cyber Crime Center; Department of State; Department of Energy; Department of Health & Human Services; Department of Treasury; FBI; U.S. Secret Service; NSA; NORAD/USNORTHCOM; US Coast Guard; USCYBERCOM; Financial Services-ISAC; Multi-State-ISAC; Aviation-ISAC; DHS National Operations Center; DHS ICE/HSI. There are also 114 private companies that have signed a CRADA and collaborate with the NCCIC via the Critical Infrastructure and Key Resources Cyber Information Sharing and Collaboration Program (CISCP).

The National Cybersecurity Protection Act of 2014 recognized the NCCIC to be responsible for coordinating information sharing related to cybersecurity risks and to be the Federal civilian interface for multi-directional and cross-sector sharing of cybersecurity risks and warnings. The NCCIC has representatives from the private sector and from other Federal entities involved in cyber information sharing work at a range of levels, from those with whom we have a formal Cooperative Research and Development Agreement (CRADA, a negotiated agreement that defines the parameters of the information sharing relationship) and share consistently, to those that passively receive information from the Center.

CS&C shares information in three principal ways; first, by sharing machine-readable threat indicators that can be immediately used for network defense; second, by sharing alerts, bulletins, and warnings that provide detailed technical context to allow cybersecurity practitioners to understand particular risks and implement necessary mitigations; and finally, by convening communities of interest to engage in in-depth collaboration. In all of these activities, the NCCIC works with its Govern-

ment partners to ensure that shared information reflects the collective knowledge of the inter-agency and is both timely and actionable to help protect private sector networks.

QUESTIONS SUBMITTED BY SENATOR PATTY MURRAY

Question. Dr. Ozment, as I understand, the Enhanced Cybersecurity Services (ECS) program is currently limited to the two commercial service providers (CSPs) currently qualified by the Department. How does the Department measure the efficacy of these programs? What are the current barriers to qualifying CSPs or attracting additional CSPs to ECS? Last, has the Department explored partnering with other commercial providers in different critical infrastructure sectors?

Answer. As of May 2015, the ECS program has three (3) fully operational CSPs—AT&T, CenturyLink, and Verizon—and expects a fourth CSP to begin providing service this summer. The fourth CSP is not a traditional Internet Service Provider. The Department measures the success of this program by the increasing number of accredited CSPs, interest by individual companies in receiving services from a CSP, and monthly/weekly program performance reports. The performance reports highlight the number of ECS indicators that triggered as hits and show trends by sector and threat actor. The barriers for CSPs participating in the program result from the nature of working with companies on a classified program, particularly those that do not already have a top secret facility clearance, cleared individuals, or a Sensitive Compartmented Information Facility (SCIF). There are also resources required of potential CSPs to design, build, and gain accreditation of ECS systems. There is a cost to DHS to accredit CSPs, and we have requested enough funding in the fiscal year 2016 budget to pay for four new CSPs and to maintain the anticipated four CSPs from 2015. There is also a cost for the secure communications link, and we have budgeted for that as well.

The Department proactively partners with any company interested in becoming a CSP and continues to encourage representation across critical infrastructure sectors.

NATIONAL PROTECTION AND PROGRAMS DIRECTORATE

Question. Dr. Ozment, notwithstanding the current reach of ECS, how does the Department account for differing cyber analysis and response capabilities among State, local, tribal, and territorial (SLTT) government users? How is the Department supporting efforts like those ongoing in my home State of Washington to burnish these cyber capabilities among small and potentially vulnerable elements across critical infrastructure sectors?

Answer. In an effort to better support SLTT governments and provide technical expertise and outreach, DHS provides four primary initiatives: funding the MS-ISAC, offering voluntary risk assessments, holding cybersecurity exercises, and offering incident response assistance. The MS-ISAC is the DHS-designated Information Sharing and Analysis Center (ISAC) for all SLTT governments. The MS-ISAC supports SLTT governments by providing education and awareness, a 24x7 security operations center, and technical expertise in malware analysis, forensic analysis and incident response/mitigation. The MS-ISAC acts as a force-multiplier for DHS in reaching out to the tens of thousands of SLTT governments across the country.

Further, DHS partners with SLTT governments to help them understand and manage their cybersecurity risk. DHS offers risk assessments such as the Cyber Resilience Review and the annual Nationwide Cyber Security Review that help SLTT governments understand their capabilities in performing, planning, managing, and measuring cybersecurity practices and behaviors. DHS also offers more technical in-depth assessments, such as Cyber Hygiene and Risk and Vulnerability Assessments, which take a closer look at SLTT government networks and offer specific recommendations to improve security and resilience. These assessments, and other resources, are available via the Critical Infrastructure Cyber Community (C3) Voluntary Program, developed to support implementation of the Cybersecurity Framework. The C3 Voluntary Program offers a Web site that provides programs and resources to all DHS customers, including SLTT governments.

Additionally, DHS develops and manages large and small-scale cyber exercises with SLTT governments to test incident response plans and continuity. These exercises, conducted on location at DHS and in the field, offer SLTT governments the opportunity to evaluate their collaboration with intra-State partners, other SLTT governments, and Federal agencies, under simulated conditions of a cybersecurity incident.

Finally, DHS' US-CERT provides incident response assistance at the request of the affected entity. SLTT governments impacted by a cybersecurity incident can request either on-site or remote assistance to identify the extent of a potential compromise, remove the adversary from the affected network, and restore critical services to a more secure State.

Question. Dr. Ozment, as you are aware, significant pieces of critical infrastructure in Washington is owned and operated by public sector entities, such as local governments and public utility districts. With that in mind, how does the Department plan to provide adequate instrumentation and analytic capacity to support real-time information sharing about cybersecurity threats to these types of public sector entities? What steps has the Department taken to integrate its current framework—including the National Cybersecurity and Communications Integration Center, computer emergency response teams, and information sharing and analysis centers—with these entities?

Answer. DHS provides a range of resources to enhance the cybersecurity of public sector entities including public utilities. The National Cybersecurity and Communications Integration Center (NCCIC) is the Federal civilian interface for multi-directional and cross-sector sharing of information about cybersecurity risks and warnings. The NCCIC has representatives from private sector and from other public entities involved in cyber information sharing work at a range of levels, providing support and expertise to critical infrastructure owners and operators. The NCCIC works through the Multi State Information Sharing and Analysis Center (MS-ISAC) to provide cybersecurity expertise and information to State and local governments. Further, the MS-ISAC has two representatives with seats on the NCCIC floor.

DHS' Cyber and Information Sharing Collaboration Program (CISCP) provides a platform for organizations to receive, share, and collaborate around unclassified threat and vulnerability information. Currently, this information sharing is primarily manual via email and a secure portal. Therefore, DHS is moving quickly to deploy automated indicator sharing, which will allow organizations to share and receive cyber threat indicators in near-real-time, formatted to be used immediately for network defense (in a format known as STIX/TAXII). With Automated Indicator Sharing, cyber threat information can be shared and applied to network defenses before the adversary can launch an attack. As a starting point, organizations, including public sector entities, can join DHS' Cyber Information Sharing and Collaboration Program (CISCP). CISCP currently provides a number of benefits, including analyst-to-analyst collaboration, detailed technical bulletins, and in-depth information exchanges, and will allow participants to benefit from Automated Indicator Sharing.

Public sector entities are also eligible to pay a commercial service provider for Enhanced Cybersecurity Services (ECS), which uses classified cyber threat indicators to detect and block potential cyber attacks. Additionally, the US Computer Emergency Readiness Team (US-CERT) and the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) provide a range of technical information and resources to support the cybersecurity of critical infrastructure, including public utilities. Among the services offered by US-CERT and ICS-CERT are on-site assessment and response assistance, particularly upon the request of an organization affected by a cybersecurity incident.

QUESTIONS SUBMITTED TO LUKE MCCORMACK

QUESTIONS SUBMITTED BY SENATOR THAD COCHRAN

Question. Your Department has been recognized for its excellent efforts in consolidating its information technology infrastructure and the savings these efforts will generate. Generally speaking, is it your judgment that it is easier to protect these assets when they are consolidated and accounted for or when they are scattered around the Government?

Answer. Consolidation of IT applications, services, and infrastructure results in stronger security and accountability, which enhances our Nation's preparedness, mitigation, and recovery capabilities.

Question. While it is widely accepted that a foreign or terrorist cyber-attack on our electric grid, water systems, or financial systems could cause widespread damage and have detrimental effects on our economy and consumer confidence, there has been much discussion about how involved the Federal Government should be in defending infrastructure owned by non-Federal entities. How would you define the threshold for what types of non-Federal infrastructure might qualify as critical for these purposes?

Answer. NPPD covers policies and outreach to non-Federal infrastructure however if there was an area that could utilize assistance and knowledge from the Federal Government it is the private Information Technology sector more specifically private Internet and Network Service providers. These entities can utilize Government best practices and shared operational data to combat the advanced persistent threat and mitigate known and unknown threats before they impact the respective networks.

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

Answer. OCIO does not have a direct role in sharing information with private sector entities. However, when indicators of compromise or any other advanced threat information has been discovered on the DHS network the information is shared with NPPD for external dissemination of relevant threat information to our industry partners. A number of indicators and threat based alerts that have been disseminated by NPPD are authored by DHS internal Security Operations Centers and released for situational awareness to all interested parties.

QUESTIONS SUBMITTED BY SENATOR BILL CASSIDY

SAFEGUARDING AND PROTECTING SENSITIVE AND CLASSIFIED DOCUMENTS AT DHS

Question. In response to the recent leaks of sensitive and classified information (OPM SF–86, Wikileaks, Snowden) and in an effort to adhere to The White House Executive Order 13587—Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information, the subcommittee is following up to get a status check on how the Department of Homeland Security is specifically securing classified and sensitive information and documents inside and outside its departmental content management systems.

Answer. The Office of Intelligence and Analysis (I&A) and the Chief Information Officer's (CIO's) response is limited to the securing classified and sensitive information and documents inside Departmental Content Management Systems.

I&A Document Content Management Systems employ a variety access control mechanisms. The mechanisms restrict access to specifically authorized users and are implemented at the network, system and application layers. User access controls are transitioning to Identity and Access Management (IdAM) which is the combination of technical systems, policies and processes that create, define, and govern the utilization and safeguarding of identity information, as well as managing the relationship between an entity and the resources to which access is needed. Currently, IdAM is not completed implementation on all Document Content Management Systems.

In addition to enhancing the access to the Document Content Management Systems, I&A has integrated the enterprise audit program and the Information Security Continuous Monitoring program to safeguard the Document Content Management Systems. These measures combined with other Computer Network Defense and the Insider Threat programs have greatly enhanced the security posture of Document Content Management Systems.

DOCUMENT SECURITY

Question. The issue of document security was specifically mentioned in the fiscal year 2015 House Homeland Security Appropriations Report (H.R. 113–481, page 22 and was not revised or negated in the explanatory statement of H.R. 240 as finally passed):

"The Committee remains concerned over the need to protect classified information, especially as to methods used to secure paper forms, which can be scanned, faxed, copied, or otherwise stolen or compromised. Existing, off-the-shelf commercial technologies can be used to monitor document access and alert security personnel when sensitive documents are at-risk. The Committee directs the Department to report to the relevant committees of jurisdiction, within 90 days after the date of enactment of this Act, on the measures currently being used to ensure hard copy document security."

Does the Department of Homeland Security (DHS) have any information security programs in place that encrypts, analyzes and monitors sensitive digital content, documents and information, (MS Office, PDFs, CADE files, videos, etc.) inside and outside the firewall of departmental databases?

Answer. There are no immediate plans to fund and deploy enterprise-wide DRM technologies however; OCIO is researching possible solutions to meet this area of

concern. DHS data at rest on computing devices, in its data centers and as it traverses its networks is routinely encrypted for protection.

In general, insider threat monitoring is fully in place on C–LAN and a pilot effort is in progress for HSDN. OCSO is in charge of this effort, with cooperation from OCIO and other Components. The Insider Threat program includes the monitoring and analysis of user activity on the network, but does not include any encryption of content.

Question. Understanding the Department has a significant volume of sensitive and personally identifiable information (PII), does the Department's CIO or CISO have plans to fund and deploy enterprise-wide secure content management or digital rights management (DRM) technologies across the Department to protect against future leaks of information?

Answer. At this time, capabilities such as the deployment of digital rights management capabilities are localized and not provided at an enterprise level under OCIO. The current fiscal year 2016 budget request does not yet include development of these capabilities for unclassified systems. I&A would be responsible for implementing DRM on TS/SCI systems (C–LAN), while OCIO would create a request for the HSDN network.

However, DHS will be prepared to make marked progress due to the fiscal year 2014 and fiscal year 2015 initiatives the Department has made in ensuring that over 85 percent of its employees use a PIV card for access to the network. The OCIO has been working to expand capabilities which are foundational to providing enterprise safeguarding services as part of its security-in-depth to further protect data within DHS firewalls, and in the future as data leaves its firewalls. In the fiscal year 2016 President's budget request, DHS has plans to implement a trusted identity exchange that is critical to implementing additional data level security on sensitive but unclassified and classified networks such as the fine grained access controls critical to the success of the DHS Data Framework program (unclassified and classified), and the protection of data and information as it would leave the Homeland Security Information Network (unclassified).

DIGITAL RIGHTS MANAGEMENT

Question. Digital rights management (DRM) is a technology already widely used by the commercial sector and intelligence community to protect and continuously monitor sensitive documents and information. DRM works by encrypting information (Microsoft Office, PDFs, CAD files, and other digital formats) with NSA standard encryption, allowing Government officials to determine whether sensitive or classified documents may be accessed internally or externally from the Government's trusted environments. The encryption is embedded within the document itself, rather than wrapping the document with a security envelope, which can be discarded by trusted Government employees and forwarded unprotected. This embedding of encryption is a key differentiator that ensures the encryption stays with the document even if it is duplicated or emailed. Because of this feature, the DRM solution completely prevents unwanted access to sensitive or classified documents and allows the Government to control saving, copying, screen-capturing, and printing.

Digital rights management, once applied to a digital piece of evidence/intelligence, will track and potentially restrict every interaction with that digital content, protecting against unauthorized insider access and dissemination. This solution also provides chain of custody tracking for evidence processing both inside and outside of firewalls. In addition, DRM telemetry data can be used to measure the effectiveness of the DI's communication and information dissemination campaign. This is accomplished by tracking what was opened, how long was it was open (read), was it printed or edited, how often someone returns to read that content and geographically where the incident occurred. This is achieved through three primary functions, authentication, authorization and auditing (telemetry data).

Authentication

Question. Who is opening (successful or not) DRM'd content, with watermark attribution and geographical location identification.

Answer. At this time, capabilities such as the deployment of digital rights management capabilities are localized and not provided at an enterprise level under OCIO. The current fiscal year 2016 budget request does not yet include development of these capabilities for unclassified systems. I&A would be responsible for implementing DRM on TS/SCI systems (C–LAN), while OCIO would create a request for the HSDN network.

Authorization

Question. What actions are they permitted to take? Has the content expired or been revoked.

Answer. At this time, capabilities such as the deployment of digital rights management capabilities are localized and not provided at an enterprise level under OCIO. The current fiscal year 2016 budget request does not yet include development of these capabilities for unclassified systems. I&A would be responsible for implementing DRM on TS/SCI systems (C–LAN), while OCIO would create a request for the HSDN network.

Audit

Question. The ability to know who is accessing DRM'd content, what actions are they taking, when this event took place and geographically where this event happened. Additional metrics can easily be added if a counterintelligence officer wants to drill into a specific user to detect anomalistic behavior to see what documents they are accessing, when they accessed those documents and whether this a deviation from their normal behavior.

Answer. At this time, capabilities such as the deployment of digital rights management capabilities are localized and not provided at an enterprise level under OCIO. The current fiscal year 2016 budget request does not yet include development of these capabilities for unclassified systems. I&A would be responsible for implementing DRM on TS/SCI systems (C–LAN), while OCIO would create a request for the HSDN network.

The use of DRM like solutions has been mandated by the Office of the Director of National Intelligence (ODNI) and the White House through multiple directives.

QUESTIONS SUBMITTED TO THE OFFICE OF THE CHIEF HUMAN CAPITAL OFFICER, DEPARTMENT OF HOMELAND SECURITY

QUESTIONS SUBMITTED BY SENATOR JOHN HOEVEN

MEETING CYBERSECURITY WORKFORCE REQUIREMENTS

Question. The Government has had many challenges in recruiting and training capable IT personnel. Cybersecurity needs have compounded that challenge. As a result, DHS has a significant number of vacancies in its cyber workforce. We've certainly heard stories of people being recruited away from the Federal Government, but haven't seen metrics or data behind this outflow.

Late last year, Congress passed cybersecurity pay reform legislation giving the Secretary flexibility in classifying and upgrading key positions. It was an attempt to make the Government more competitive with the private sector. Further, the fiscal year 2016 budget includes a request for $31.3 million (1,400 personnel) including $16.3 million for NPPD for the CyberSkills Management Initiative (CSMI). In regard to this request, please provide the following:

A. Attrition statistics justifying the need for the $31.3 million request.

Answer. DHS averages a vacancy rate of approximately 5 percent in the population of approximately 1,400 Federal civilian positions present in the Department's Cybersecurity Workforce Inventory database. This population of positions is spread across 12 different DHS components and headquarters organizations and over 15 occupational series.

In response to Public Law 113–277 and Public Law 113–246, the CyberSkills Management Support Initiative is leading a Department-wide effort to enhance its cybersecurity workforce planning and analysis activities to meet new statutory reporting requirements and to prepare for the implementation of new human capital authority, which will eventually affect the hiring and compensation of cybersecurity positions.

Question. We have a financial breakdown by component of the CSMI but lack detail on the number of personnel and how precisely the funds would be distributed across the Department. Please provide a breakdown by component of all positions including transfers, new hires, and those receiving incentive packages.

Answer. Current proposals distribute the $31.3 million across components based on data derived from the Cybersecurity Workforce Inventory database and modified based on component budget input. The Department's intention is for the Office of the Chief Financial Officer and the Office of the Chief Human Capital Officer to use the results of data calls being conducted now as part of the effort to refine this distribution prior to the start of fiscal year 2016; the new dataset of mission critical cybersecurity positions that will help to inform funding is expected to be available

in September 2015. A portion of the $31.3 million will be used to increase headquarters and component human capital infrastructure to ensure effective implementation and eventual operationalization of new authority granted by Public Law 113–277; remaining funds will be proportionally distributed to components based on the size of their validated, mission critical cybersecurity workforce. This data will be complete by the end of fiscal year 2015. Components will use these funds to support targeted recruitment and retention strategies. The administration of such flexibilities must be done at the component/organization level, and each case in question, including the circumstances of the specific employee/new hire and position, must meet regulatory and policy requirements to ultimately justify the decision to make a payment.

Question. For those positions requiring hiring (versus retention incentives), how many existing vacancies within each component will be filled through the CyberSkills Management Support Initiative, and how many can be filled by the end of fiscal year 2016?

Answer. The CyberSkills Management Support Initiative plans to institute new workforce planning processes throughout fiscal year 2016 to closely monitor component vacancies using data gathered via the comprehensive cybersecurity workforce analysis process. In addition to providing leadership with more insight than ever into staffing gaps and similar issues, the data will be used to inform targeted interventions with component cyber program managers and human capital staff. This data will be complete by the end of fiscal year 2015. This coordinated approach will help to ensure that DHS effectively uses its hiring and retention flexibilities, and to address the most critical vacancies as quickly as possible.

Question. A breakdown by job category and grade-level for each of the positions.

Answer. At the start of fiscal year 2016, the Department expects to have a new database capturing the mission critical cybersecurity workforce validated through the comprehensive cybersecurity workforce analysis effort. Currently available data collected by the cybersecurity workforce inventory process in place since 2012 indicates the following for the population of approximately 1,400 civilian and active duty Coast Guard positions which the Department has been monitoring:

WORKFORCE BY OCCUPATIONAL SERIES AND GRADE

	Intelligence (0132)	Management and program analysis (0343)	Criminal investigation (1811)	Information technology management (2210)	Other	Total
GS–07	1					1
GS–09	1			5	2	8
GS–11	4		2	19		25
GS–12	2	1	21	52	2	78
GS–13	14	2	583	102	11	712
GS–14	12	6	61	214	18	311
GS–15	5	2	8	49	4	68
G Band		1				1
H Band				4		4
I Band		3		20	6	29
J Band	2	2		49	2	55
K Band				9	1	10
L Band				1		1
Executive (SES, SL, ST, etc.)				1	8	9
Commissioned Officer (O–1 through O–10)	4			11		15
Chief Warrant Officer (W–2 through W–4)			7	26		33
Non-Commissioned Officer (E–4 through E–9)	1		3	27		31
Other					3	3
Total	46	17	685	589	57	1,394

Question. The Office of the Chief Human Capital Officer intends to work with components to track the population of mission critical cybersecurity positions and al flexibilities used to recruit or retain employees associated with those positions throughout fiscal year 2016.

What conditions are being attached to the incentives? In other words, will recipients be required to stay with the Government for a period of time after receiving the additional pay?

Answer. As indicated in our response to the second question, the act of granting an incentive to a new hire or employee requires that each case in question, including the circumstances of the specific employee/new hire and position, meet regulatory and policy requirements to ultimately justify the decision to make a payment. Once an incentive is approved, an employee must also sign a written agreement to complete a specified period of employment with the agency. For example, a recruitment incentive service agreement must specify the length, commencement, and termination dates of the service period; the amount, method and timing of incentive payments; the conditions under which an agreement will be terminated by the agency; any agency or employee obligations if a service agreement is terminated (including the conditions under which the employee must repay an incentive); and any other terms and conditions for receiving and retaining a recruitment incentive.

QUESTIONS SUBMITTED TO THE OFFICE OF THE CHIEF SECURITY OFFICE, DEPARTMENT OF HOMELAND SECURITY

QUESTIONS SUBMITTED BY SENATOR BILL CASSIDY

SAFEGUARDING AND PROTECTING SENSITIVE AND CLASSIFIED DOCUMENTS AT DHS

Question. In response to the recent leaks of sensitive and classified information (OPM SF–86, Wikileaks, Snowden) and in an effort to adhere to The White House Executive Order 13587—Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information, the subcommittee is following up to get a status check on how the Department of Homeland Security is specifically securing classified and sensitive information and documents inside and outside its departmental content management systems.

Answer. The totality of these mandates and initiatives are managed in the Department of Homeland Security by the Information Sharing and Safeguarding Governance Board (ISSGB). The elements involved include information systems enterprise audit programs, information assurance programs, insider threat user activity monitoring, physical security of facilities and system hubs, rigorous access control programs for physical and virtual environments, personnel security background checks and periodic reviews, developing programs involving the continuous evaluation of personnel holding security clearances, and active training and awareness programs for all cleared personnel. Recommend assigning this question to OCIO and I&A.

DOCUMENT SECURITY

Question. The issue of document security was specifically mentioned in the fiscal year 2015 House Homeland Security Appropriations Report (H.R. 113–481, page 22 and was not revised or negated in the explanatory statement of H.R. 240 as finally passed):

"The Committee remains concerned over the need to protect classified information, especially as to methods used to secure paper forms, which can be scanned, faxed, copied, or otherwise stolen or compromised. Existing, off-the-shelf commercial technologies can be used to monitor document access and alert security personnel when sensitive documents are at-risk. The Committee directs the Department to report to the relevant committees of jurisdiction, within 90 days after the date of enactment of this Act, on the measures currently being used to ensure hard copy document security."

What is the Department doing to respond to the fiscal year 2015 House Homeland Security Appropriations Report "Document Security" language? Specifically, will the Department respond with some program details as to how to address document security issues? And, is this report on track to be submitted within the 90-day period directed by Congress?

Answer. The response to the required report was submitted on time to Congress June 1, 2015.

SUBCOMMITTEE RECESS

Senator HOEVEN. And with that, this subcommittee stands in recess. Again, my thanks.

[Whereupon, at 3:58 p.m., Wednesday, April 15, the subcommittee was recessed, to reconvene at a time subject to the call of the Chair.]