INVESTING IN CYBERSECURITY: UNDERSTANDING RISKS AND BUILDING CAPABILITIES FOR THE FUTURE

WEDNESDAY, MAY 7, 2014

U.S. Senate,
Subcommittee on Homeland Security,
Committee on Appropriations,
Washington, DC.

The subcommittee met at 2:01 p.m., in room SD–192, Dirksen Senate Office Building, Hon. Mary L. Landrieu (chairman) presiding.

Present: Senators Landrieu, Coons, Coats, and Cochran.

OPENING STATEMENT OF SENATOR MARY L. LANDRIEU

Senator Landrieu. Good afternoon, everyone. Let me call our meeting to order, please. This is a meeting of the Appropriations Subcommittee for Homeland Security. I appreciate being joined by my ranking member, Senator Coats, and I appreciate all the work of Senator Coons. Thank you for being here as well. You've both been leaders in the area of cybersecurity and I appreciate your support and help.

I thank our panelists for being here.

I'm going to shorten my opening statement, turn it then to Senator Coats and Senator Coons if you have a brief opening statement, go right into the panelists. We've had a vote called at 3:15, so we're going to try to see if we can work through the next hour and a half and not have to come back after the vote. But we are very interested, of course, in the testimony, and that will be subject to change as we go.

But today we meet to review our level of investment in cybersecurity and the results that we have achieved to date. Our purpose is to better understand the new and emerging risk as well as the capabilities that we need to continue to build to secure our networks for the future.

Serving on both the Homeland Security subcommittee and the Energy subcommittee, I believe that I have a unique perspective, along with other members as well, on the extent that critical infrastructure throughout our country relies more and more on our interdependent technologies that we need to grow, innovate, and keep our country thriving. Without the use of the Internet and advances in smart grid technology, for instance, America's companies would not be able to keep the power on in the most affordable, efficient way our Nation has ever known.

Today we will talk about some of the vulnerabilities facing these critical networks, what we're doing through Homeland Security to help and be supportive of keeping our Government and our economy strong and growing. We are all aware of some of the threats that have occurred. We'll talk more specifically about that, but I want to just thank you all for being a part of this hearing.

We've got a wonderful panel that I'll introduce in just a moment, a first and a second panel. At this point I'm going to turn it over to Senator Coats for his opening remarks.

STATEMENT OF SENATOR DANIEL COATS

Senator COATS. Madam Chairman, thank you. I'm going to be brief also, given that vote coming up and the fact that we want to get to the substance of this hearing.

We all know how interconnected we have become and unfortunately vulnerable, vulnerable to some bad actors that have not only disrupted a lot of people's personal lives by securing their private information, but also pose a major threat to our critical infrastructure. This cyber threat has been labeled by many in the security business and in our national security and military as the number one threat to the United States. Now, there are a lot of threats out there, but this is serious.

A number of us, the three of us on this panel that are here today and others, have been working for some amount of time through a couple of different Congresses to try to come up with legislation that strengthens our ability to prevent these types of attacks and protect our critical infrastructure as well as the retail outlets and American business and just about everyone who's affected with this. In fact, my law school alma mater, Indiana University, was hacked. Fortunately, they were able to—so this thing runs the gamut. It's not just our electric grid and so forth, but it comes right down to our private lives and even our educational institutions.

So clearly we need to move forward with sensible legislation. The Department of Homeland Security (DHS) plays a very critical role, not only in protecting dot-gov, but also in being the portal through which a lot of this has to take place and work through in order to provide the kind of protections we need. Whether it's information-sharing, whether it's working together with private sector and public sector, this is something that is urgent, and the longer we put it off the more vulnerable we become.

I'm pleased that on the second panel Scott Bowers from Indiana will be talking about the impact of this on the private sector. I'm glad to have him here.

Madam Chairman, I'm looking forward to the testimony and the kind of questions and back and forth we can have to hopefully move this thing forward in an expeditious way.

Senator LANDRIEU. Thank you very much, Senator Coats.

Senator Coons.

STATEMENT OF SENATOR CHRISTOPHER A. COONS

Senator COONS. Thank you, Madam Chair. I'm grateful to you for your leadership on this, to Senator Coats for your partnership and leadership in this. This is a very real threat. We have issues of jurisdiction, of funding, of workforce. We've got a lot of good work to do and I'm really grateful for the service of the folks who are going to be testifying in front of us today.

Thank you, Madam Chair. I'm eager to hear the testimony.

Senator LANDRIEU. Thank you very much.

Let me introduce our first panel: Mrs. Phyllis Schneck, Deputy Under Secretary for Cybersecurity, DHS, National Protection and Programs Directorate (NPPD); Mr. Peter Edge, Executive Associate Director, Homeland Security Investigations (HSI); and Mr. William Noonan, Deputy Special Agent in Charge, Criminal Investigations, Cyber Operations, DHS, U.S. Secret Service.

Thank you all, and we'll begin with your 5-minute testimony.

STATEMENT OF DR. PHYLLIS E. SCHNECK, DEPUTY UNDER SECRETARY FOR CYBERSECURITY, NATIONAL PROTECTION AND PROGRAMS DIRECTORATE, DEPARTMENT OF HOMELAND SECURITY

Dr. SCHNECK. Good afternoon, Chairwoman Landrieu, Ranking Member Coats, Senator Coons. Thank you very much for the strong support that you've provided to the Department of Homeland Security and to the National Protection and Programs Directorate. First and foremost, we look forward to continuing to work with you on these issues and securing our critical infrastructure, our way of life, from that combined physical and cyber threat, as we are all connected, as you mentioned.

Thank you very much for the opportunity to appear before you today to discuss our efforts for critical infrastructure resilience and cybersecurity. We focus very much on this threat, this interconnected threat, as cybersecurity and cyber and connectivity connect all of us through our way of life, our water, our banks, our electricity, all of our States. It's a privilege today to sit at the table with my colleagues from the U.S. Secret Service, from Homeland Security Investigations, representing that cybersecurity at the U.S. Department of Homeland Security is a unity of effort. It is one DHS. Along with our colleagues in the U.S. Coast Guard, we also enjoy a strong relationship with our Office of the Chief Information Officer to ensure that our programs also run well on our network and we learn from that which tries to attack the sweet target known as dhs.gov.

I'm going to talk about our operations, our major investments, and our overall strategic vision, starting at our core, our National Cybersecurity and Communications Integration Center (NCCIC), which some of you have been able to visit. That—great analogy, Senator Coons—is our portal. It's our 24×7 watch center, where we have cyber command and control, understanding inputs that come in 24×7 from trusted relationships, from partnerships in the interagency, law enforcement, intelligence community, across DHS, and certainly information that we learn from our own programs, those things that are protecting our stakeholders, our Federal civilian agencies, our State, local, tribal, territorial governments, as well as the private sector.

One great example is the recent Heartbleed, a defect in a piece of software. When we found out as the U.S. Government that this existed, again the ability for an adversary to decrypt, thus make not confidential, traffic that was thought to be confidential through a defect in software—we found this out on April 7. Within 24 hours, DHS had full resources out on all of our Web sites for all of our stakeholders and was beginning the process of scanning all of the U.S. Government agencies to find where that software might be running.

For our programs, we work through humans, we work through machines; humans through trusted partnerships, again with our stakeholders and certainly across Federal and State government, and with our private sector, building that trust across infrastructure, across cyber and communications, so that information can be shared quickly as we face an adversary that works with great speed, has plenty of money, and has no lawyers and no way of life to protect.

We also have invested in the critical infrastructure cybersecurity community voluntary program to launch the efforts of the cybersecurity framework built by the National Institute of Standards and Technology (NIST) and DHS all of last year, to take guidelines from cybersecurity and get them into even our smallest companies, so that they can adopt good cybersecurity, bring it as a boardroom issue, and enable larger companies to now request better standards of cybersecurity for those companies that supply them, connect to them, and protect all of our private information.

On the machine side, our programs protect our Federal Government agencies from things that come in and try to attack them or vulnerabilities that can cause harm. We can also detect those things. It's "see something, say something," as with the rest of Homeland Security. When those programs spot something on one agency, we then have the ability through our NCCIC, our core, our portal, to spot that behaviorally, like your body fights a cold, and protect all the other agencies and the private sector with that information, at the same time providing all the best in privacy and civil liberties to the extent that our law provides, as well as showing the public everything we do. Full transparency is on our Web site.

So again, we are able to use Government information and protect the private sector, and we roll that out to the critical infrastructure as well as through enhanced cybersecurity services, using classified information to protect our private-sector entities, all the while combining what we can see only in Government to protect all of our stakeholders.

We can also automate, running at machine speed, sending information about bad cyber behavior to everybody. So again "see something, say something," with the ability to, using our cybersecurity integration center, through human analysis, machine analysis, all kinds of inputs from all kinds of partners, injecting that back into both automated programs as well as automated information that we can disseminate as widely as possible, as quickly as possible.

So I've talked about a lot of high-profile programs. I don't want to forget the importance of our talented workforce and building the talent of the future. It is a priority of Secretary Johnson and he and I went and visited two universities and we'll be doing more, and we spoke to students in Ph.D. programs as well as undergrad programs. I've also gone out and spoken with students at both the high school level and the college level, so that we can begin to truly look at how we not only show the talent of the future what DHS can do and what they can learn from our larger mission, again from the Secret Service, Homeland Security Investigations, U.S. Coast Guard, our CIO, Federal Emergency Management Agency (FEMA), and others, but also we can identify that talent set that we'll need to be training for, so that we can start to look at how we build that talent going forward.

I thank you very much again for your support and look very forward to working with you, continuing to work with you, as we build these programs and certainly, Chairwoman Landrieu, Ranking Member Coats, and Senator Coons, look very forward to your questions. Thank you.

[The statement follows:]

Prepared Statement of Dr. Phyllis Schneck

INTRODUCTION

Chairwoman Landrieu, Ranking Member Coats, and distinguished members of the subcommittee, let me begin by thanking you for the strong support that you have provided 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 and other hazards.

Thank you for the opportunity to appear before the committee today to discuss NPPD's efforts to strengthen the Nation's critical infrastructure security and resilience against cyber events and other catastrophic incidents. The President's fiscal year 2015 budget request for NPPD is $2.9 billion, offset by $1.3 billion in collections for the Federal Protective Service. This request includes $746 million for cybersecurity capabilities and investments.

America's national security and economic prosperity are increasingly dependent upon physical and digital critical infrastructure that is at risk from a variety of hazards, including attacks via the Internet. I view integrating cyber and physical security as integral to the larger goal of infrastructure security and resilience. DHS approaches physical security and cybersecurity holistically; both to better understand how they integrate and how best to mitigate the consequences of attacks that can cascade across all sectors of critical infrastructure. This risk management approach helps drive the discussion at the executive level in organizations of all sizes across government and industry, where it can have the most impact on resources and implementation.

LEVERAGING INTEGRATED CAPABILITIES: IMPLEMENTING PPD–21 AND EO 13636

On February 12, 2013, the President signed Executive Order (EO) 13636, Improving Critical Infrastructure Cybersecurity and Presidential Policy Directive (PPD) 21, Critical Infrastructure Security and Resilience, which set out steps to strengthen the security and resilience of the Nation's critical infrastructure, and reflect the increasing importance of integrating cybersecurity efforts with traditional critical infrastructure protection. Taken together EO 13636 and PPD–21 are foundational efforts for helping drive the security market and provide a framework for critical infrastructure to increase their cybersecurity efforts. To implement both EO 13636 and PPD–21, the Department established an Integrated Task Force to lead DHS implementation and coordinate interagency, public and private sector efforts, and to ensure effective integration and synchronization of implementation across the homeland security enterprise.

The fiscal year 2015 budget request reflects targeted enhancements to continue implementation of the EO and PPD. Enhancements of $14 million, including 48 positions, is requested for the Critical Infrastructure Cyber Community (C^3 or "C-Cubed") Voluntary Program; Enhanced Cybersecurity Services (ECS); Regional Resiliency Assessment Program; National Coordinating Center (Communications) (NCC) 24×7 communications infrastructure response readiness. NPPD has partially offset these enhancements with $9 million in reductions to realign resources to support these key EO and PPD initiatives. The following EO and PPD initiatives in the fiscal year 2015 budget specifically enhance cyber capabilities:

C^3 Voluntary Program

The C^3 Voluntary Program is a public-private partnership aligning business enterprises as well as Federal, State, local, tribal, and territorial (SLTT) governments to existing resources that will assist their efforts to use the National Institute of

Standards and Technology Cybersecurity Framework to manage their cyber risks as part of an all-hazards approach to enterprise risk management. The program emphasizes three elements: converging CI community resources and driving innovation and markets to support cybersecurity risk management and resilience through use of the Cybersecurity Framework; connecting CI stakeholders to the national resilience effort through cybersecurity resilience advocacy, engagement and awareness; and coordinating CI cross-sector efforts to maximize national cybersecurity resilience. The $6 million enhancement, including 10 positions, is requested to manage and support this program and increase the number of evaluations completed.

Enhanced Cybersecurity Services

The ECS capability enables owners and operators of critical infrastructure to enhance the protection of their networks from unauthorized access, exfiltration, and exploitation by cyber threat actors. The requested enhancement of 24 positions and $3 million allows ECS to execute the operational processes and security oversight required to share sensitive and classified cyber threat information with qualified Commercial Service Providers that will enable them to better protect their customers who are critical infrastructure entities.

Regional Resiliency Assessment Program (RRAP)

The $5 million, including 11 positions, is requested to complete five additional cyber-centric RRAPs. Through these RRAPs, NPPD will identify cross-sector physical and cyber interdependencies and better understand the consequences of disruptions to lifeline sectors. We often observe that physical consequences can have cyber origins and anticipate that the findings will provide valuable data about the energy, water, and transportation sectors and their reliance on cyber infrastructure.

National Coordinating Center for Communications Operations

The proposed increase of three positions and $1 million in funding to the NCC will maintain 24×7 communications infrastructure response readiness and requirements coordination between FSLTT and industry responders. Due to the loss of staff previously provided to DHS from the Department of Defense on a non-reimbursable basis, the NCC will no longer be able to provide 24×7 readiness without these additional resources.

HEARTBLEED

The Department recently responded to a serious vulnerability, known as "Heartbleed," in the widely used OpenSSL encryption software that protects the electronic traffic on a large number of Web sites and devices. Although new computer "bugs" and malware crop up almost daily, this vulnerability is unusual in its pervasiveness across our infrastructure, its simplicity to exploit, and the depth of information it compromises.

While the Federal Government was not aware of the vulnerability until April 7th, DHS responded in less than 24 hours, utilizing the National Cybersecurity and Communications Integration Center (NCCIC) to release alert and mitigation information to the public, create compromise detection signatures for the EINSTEIN system, and reach out to critical infrastructure sectors, Federal departments and agencies, SLTT governments, and international partners. Once in place, DHS also began notifying agencies that EINSTEIN signatures had detected possible activity, and immediately provided mitigation guidance and technical assistance. Additionally, DHS worked with civilian agencies to scan their .gov Web sites and networks for Heartbleed vulnerabilities, and provided technical assistance for issues of concern identified through this process.

Of note, the Administration's May 2011 Cybersecurity Legislative Proposal called for Congress to provide DHS with clear statutory authority to carry out this operational mission, while reinforcing the fundamental responsibilities of individual agencies to secure their networks, and preserving the policy and budgetary coordination oversight of OMB and the EOP. Even with the rapid and coordinated Federal Government response to Heartbleed, the lack of clear and updated laws reflecting the roles and responsibilities of civilian network security caused unnecessary delays in the incident response.

INTEGRATED CYBERSECURITY OPERATIONS

Along with our operational assistance, DHS has several programs that directly support Federal civilian departments and agencies in developing capabilities that will improve their own cybersecurity posture. Through the Continuous Diagnostics and Mitigation (CDM) program, led by the NPPD Federal Network Resilience Branch, DHS enables Federal agencies to more readily 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 by adversaries.

Available to all Federal civilian agencies, the CDM program provides diagnostic sensors, tools, and dashboards that provide situational awareness to individual agencies and at a summary Federal level. This allows agencies to target their cybersecurity resources toward the most significant problems, and enables comparison of relative cybersecurity posture between agencies based upon common and standardized information. The CDM contract can also be accessed by defense and intelligence agencies, as well as by State, local, tribal, and territorial (SLTT) governments. 108 departments and agencies are currently covered by Memoranda of Agreement with the CDM program, encompassing over 97 percent of all Federal civilian personnel. In fiscal year 2014, DHS issued the first delivery order for CDM sensors and awarded a contract for the CDM dashboard. The $143 million and 15 staff requested in fiscal year 2015 will support deployment of the Federal dashboard and capabilities to Federal agencies.

In addition, the National Cybersecurity Protection System (NCPS), a key component of which is referred to as EINSTEIN, is an integrated intrusion detection, analytics, information sharing, and intrusion-prevention system utilizing hardware, software, and other components to support DHS responsibilities for protecting Federal civilian agency networks. In fiscal year 2015, the program will expand intrusion prevention, information sharing, and cyber analytic capabilities at Federal agencies, marking a critical shift from a passive to an active role in cyber defense and the delivery of enterprise cybersecurity services to decision-makers across cybersecurity communities.

In July 2013, EINSTEIN 3 Accelerated (E3A) became operational and provided services to the first Federal Agency. As of February 2014, Domain Name System and/or email protection services are being provided to a total of seven departments and agencies. Full Operational Capability is planned for fiscal year 2016. With the adoption of E3A, DHS will assume an active role in defending .gov network traffic and significantly reduce the threat vectors available to malicious actors seeking to harm Federal networks. In fiscal year 2015, $378 million is requested for NCPS. We will continue working with the Internet Service Providers to deploy intrusion prevention capabilities, allowing DHS to provide active, in-line defense for all Federal network traffic protocols.

It is important to note that the Department has strong privacy, civil rights, and civil liberties standards implemented across its cybersecurity programs. DHS integrates privacy protections throughout its cybersecurity programs to ensure public trust and confidence. DHS is fully responsible and transparent in the way it collects, maintains, and uses personally identifiable information.

Operational Response

Increased connectivity has led to significant transformations and advances across our country and around the world. It has also increased complexity and exposed us to new vulnerabilities that can only be addressed by timely action and shared responsibility. Successful responses to dynamic cyber intrusions require coordination among DHS, the Departments of Justice (DOJ), State (DOS) and Defense (DOD), the Intelligence Community, the specialized expertise of sector specific agencies such as the Department of the Treasury, private sector partners—who are critical to these efforts—and SLTT, as well as international partners, each of which has a unique role to play.

DHS is home to the National Cybersecurity and Communications Integration Center (NCCIC), a national nexus of cyber and communications integration. A 24×7 cyber situational awareness, incident response, and management center, NCCIC partners with all Federal departments and agencies, SLTT governments, private sector and, critical infrastructure owners and operators, and international entities. The NCCIC disseminates cyber threat and vulnerability analysis information and assists in initiating, coordinating, restoring, and reconstituting national security/emergency preparedness (NS/EP) telecommunications services and operates under all conditions, crises, or emergencies, including executing Emergency Support Function #2—Communications Annex responsibilities under the National Response Framework.

The NCCIC also provides strategic cyber-threat analysis, through its United States Computer Emergency Readiness Team (US–CERT) and the Industrial Control Systems Cyber Emergency Response Team (ICS–CERT) in conjunction with the National Infrastructure Coordinating Center (NICC), to reduce malicious actors exploiting vulnerabilities. Threat management decisions must incorporate cyber threats based on technological as well as non-technological factors, and consider the varying levels of security required by different activities. Since its inception in 2009, the NCCIC has responded to nearly a half million incident reports and released more than 37,000 actionable cybersecurity alerts to our public and private sector partners. In fiscal year 2013, NCCIC received 228,244 public and private sector cyber incident reports, a 41-percent increase from 2012, and deployed 23 response teams to provide onsite forensic analysis and mitigation techniques to its partners. NCCIC issued more than 14,000 actionable cyber alerts in 2013, used by private sector and government agencies to protect their systems, and had more than 7,000 partners subscribe to the NCCIC/US–CERT portal to engage in information sharing and receive cyber threat warning information.

Further demonstrating NPPD's commitment to greater unity of effort in strengthening and maintaining secure and resilient critical infrastructure against both physical and cyber threats, the NICC has moved its watch operations center to collocate with the NCCIC. The NICC is the information and coordination hub of a national network dedicated to protecting critical infrastructure essential to the Nation's security, health and safety, and economic vitality. In accordance with and supporting the physical-cyber integration directives of PPD–21, this new integration will enhance effective information exchange, and improve the alacrity of protection with real-time indicator sharing. Concurrently, the NCCIC will refine and clarify the NICC–NCCIC relationship to advance national unity of effort within NPPD and the Federal Government.

Data Security Breaches

On December 19, 2013, a major retailer publicly announced it had experienced unauthorized access to payment card data from the retailer's U.S. stores. The information involved in this incident included customer names, credit and debit card numbers, and the cards' expiration dates and card verification-value security codes. Another retailer also reported a malware incident involving its point of sale system on January 11, 2014, that resulted in the apparent compromise of credit card and payment information. A direct connection between these two incidents has not been established.

During both incidents, NPPD's NCCIC utilized its unique cybersecurity, information sharing and mitigation capabilities to help retailers across the country secure their systems to prevent similar attacks while simultaneously providing timely analysis to the United States Secret Service (USSS). DHS's ability to provide a cross-component response during this incident underscores the importance of leveraging complementary missions at the Department. Working closely together, elements with cyber capabilities such as the USSS, U.S. Coast Guard, Immigrations and Customs Enforcement's office of Homeland Security Investigations, Office of the Chief Information Officer, and NPPD are able to increase focus on not just responding to incidents but also reducing vulnerabilities, protecting against future attacks, and mitigating consequences.

In response to this incident, NCCIC/US–CERT analyzed the malware identified by the USSS as well as other relevant technical data and used those findings, in part, to create two information sharing products. The first product, which is publicly available and can be found on US–CERT's Web site, provides a non-technical overview of risks to point of sale systems, along with recommendations for how businesses and individuals can better protect themselves and mitigate their losses in the event an incident has already occurred. The second product provides more detailed technical analysis and mitigation recommendations, and has been securely shared with industry partners to enable their protection efforts. NCCIC's goal is always to share information as broadly as possible, including by producing actionable products tailored to specific audiences.

While the criminal investigation into the these activities is on-going, NPPD, through the NCCIC and other organizations, continues to build shared situational awareness of similar threats among our private sector and government partners and the American public at large. At every opportunity, the NCCIC and our private sector outreach program publish technical and non-technical products on best practices for protecting businesses and customers against cyber threats and provide the information sharing and technical assistance necessary to address cyber threats as quickly as possible. DHS remains committed to ensuring cyberspace is supported by a secure and resilient infrastructure that enables open communication, innovation, and prosperity while protecting privacy, confidentiality, and civil rights and civil liberties by design.

UNDERSTANDING CYBER AND PHYSICAL CRITICAL INFRASTRUCTURE INTERDEPENDENCIES

One of NPPD's top priorities is providing our government and private sector partners with the information, analysis, and tools they need to protect our Nation's critical infrastructure in the face of physical and cyber risks. Key to this effort is understanding the consequences of potential disruptions to critical infrastructure, including interdependencies and cascading impacts, from all hazards to better equip and prepare our partners and stakeholders. Understanding consequences helps identify potential mitigation measures and prioritize the allocation of limited resources for both government and private sector.

In February of 2014, NPPD established the Office of Cyber and Infrastructure Analysis to implement elements of PPD–21, which calls for integrated analysis of critical infrastructure, and EO 13636, identifying critical infrastructure where cyber incidents could have catastrophic impacts to public health and safety, the economy, and national security. An Integrated Analysis Cell was established to provide near real-time information to NPPD's two operational centers: the National Infrastructure Coordinating Center (NICC) and National Cybersecurity and Communications Integration Center (NCCIC). Similarly the work that has been done to implement section 9 of EO 13636 through the Cyber-Dependent Infrastructure Identification Working Group exemplifies how the skills that have been developed in NPPD over the years focused on critical infrastructure can similarly be applied to the analyzing cyber infrastructure. $33 million is requested in fiscal year 2015 to support these efforts.

Engaging with Federal, SLTT, and Private Sector Entities

NPPD is committed to engaging with Federal, SLTT, and private sector stakeholders. More than 1,100 participants were involved in the development of NIPP 2013, providing thousands of comments reflecting our partners' input and expertise. NPPD has become increasingly focused on engaging stakeholders at the executive level, and working with the DOE, will implement a sustained outreach strategy to energy sector Chief Executive Officers to elevate risk management of evolving physical and cyber threats to the enterprise level. NPPD will also explore similar efforts across the critical infrastructure community.

NPPD serves as a principal coordination point for stakeholder engagement for Cybersecurity through the Cyber Security Evaluation Program (CSEP). CSEP which provides voluntary evaluations intended to enhance cybersecurity capacities and capabilities across all 16 Critical Infrastructure Owner/Operators, as well as SLTT governments through its Cyber Resilience Review (CRR) process. The goal of the CRR is to develop an understanding and measurement of key cybersecurity capabilities and provide meaningful maturity indicators to an organization's operational resilience and ability to manage risk to its critical services during normal operations and times of operational stress and crisis.

VISION FOR THE FUTURE

DHS has a solid foundation upon which to build and enhance future cybersecurity capabilities to ensure information resilience against an adversary that leverages the best of technology and doesn't lack for funding. DHS continues to strengthen trust and public confidence in the Department through the foundations of partnership, transparency, and protections for privacy and civil liberties, which is built in to all that we do. Our Department is the lead civilian agency responsible for coordinating the national protection, prevention, mitigation, and recovery from cyber incidents across civilian government, State, local, tribal, territorial (SLTT) and private sector entities of all sizes. DHS leverages our interagency and industry partnerships as well as the breadth of our cyber capabilities extending from NPPD, Immigration and Customs Enforcement's Homeland Security Investigations, U.S. Coast Guard and U.S. Secret Service, to make our NCCIC the source for dynamic data aggregation of for global cyber indicators and activity.

We are working to further enable the NCCIC to receive and disseminate information at "machine speed."[1] This enhanced capability will enable networks to be more self-healing, as they use mathematics and analytics to mimic restorative processes that are currently done manually. Ultimately, this will enable us and our partners to better recognize and block threats before they reach their targets, thus deflating the goals for success of cyber adversaries and taking botnet response from hours to

[1] Automatically sending and receiving cyber information as it is consumed and augmented based on current threat conditions, creating a process of automated learning that emulates a human immune system and gets smarter as it is exposed to new threats.

seconds in certain cases. We are working with the DHS Science & Technology Directorate in many areas to develop and support these capabilities for NCCIC. The science of decisionmaking is about seeing enough behavior to differentiate the good from the bad, and that comes from the collective information of industry and Government. That is voluntarily provided to us because of underlying trust. This effort is currently being built in our Structured Threat Information Expression (STIX) and Trusted Automated eXchange of Indicator Information (TAXII™) programs that we have begun offering as a free method for machine-to-machine sharing of cyber threat indicators to others in the Government and private sector.

We must increase data exchange and information flow with industry through stakeholder engagement to optimize the information shared voluntarily. This must be done in a manner that promotes privacy and civil liberties protections, focusing on the sharing of cyber threat information that is non-attributable and anonymized to the greatest extent feasible.

DHS's extensive visibility into attacks on government networks must be fully leveraged to protect all government networks as well as our critical infrastructure and local entities, in a way that is consistent with our laws while preserving the privacy and individual rights of those we protect. Legislation providing a single clear expression of DHS cybersecurity authority would greatly enhance and speed up the Department's ability to engage with affected entities during a major cyber incident and dramatically improve the cybersecurity posture of Federal agencies and critical infrastructure.

CONCLUSION

Infrastructure is the backbone of our Nation's economy, security and health. We know it as the power we use in our homes, the water we drink, the transportation that moves us, and the communication systems we rely on for business and everyday life. We have an extremely dedicated and talented workforce engaged in activities that advance our mission to protect that information and their innovation will continue to propel NPPD and DHS forward in fiscal year 2015 and beyond. Each employee is dedicated to a safe, secure, and resilient infrastructure that enables our way of life to thrive.

Chairwoman Landrieu, Ranking Member Coats, and distinguished members of the subcommittee, thank you all for your leadership in cybersecurity and for the opportunity to discuss the fiscal year 2015 President's budget request for NPPD's cybersecurity efforts. I look forward to any questions you may have.

Senator LANDRIEU. Thank you very much.

Mr. Edge.

STATEMENT OF PETER T. EDGE, EXECUTIVE ASSOCIATE DIRECTOR, HOMELAND SECURITY INVESTIGATIONS, IMMIGRATION AND CUSTOMS ENFORCEMENT, DEPARTMENT OF HOMELAND SECURITY

Mr. EDGE. Good afternoon, Chairwoman Landrieu, Ranking Member Coats, and Senator Coons. Thank you for the opportunity to appear before you today to discuss the risks of cyber crime and the impact of U.S. Immigration and Customs Enforcement's Homeland Security Investigations' role with respect to conducting investigations and building capabilities to protect our Nation's borders and enhance public safety for the future.

The Internet poses a significant challenge to law enforcement. When a criminal never has to meet his victim face-to-face, but can hide behind what appears to be a legitimate Web site, consumer fraud runs rampant. When criminal organizations can employ technical means to steal intellectual property, American ingenuity is stymied. When money-launderers can utilize non-traditional Internet-based financial services, circumventing regulatory safeguards and public safety, that's a detriment and a danger to our country.

Criminal networks are becoming increasingly sophisticated in taking advantage of the many ways in which the Internet can streamline communications, financing, and logistics, just as it does for legal enterprise. As a consequence, law enforcement agencies must respond by properly preparing investigators for work in cyber space. As information systems and computer networks become increasingly prolific, the technical challenges facing law enforcement investigations of criminals operating through the Internet grow daunting, and the considerations in collecting electronic evidence become increasingly complex.

Our Cyber Crime Center, which was established in 1997, brings the full range of Homeland Security Investigations cyber investigations and computer forensics assets together in a single location to coordinate global investigations and to provide to our field offices in their efforts to combat cyber-enabled crime. The scope of these investigations includes any instance where information technology or computer networks are substantially employed to facilitate international smuggling, money-laundering, and Internet-based financial frauds or identity theft, even proliferation of strategic commodities or the digital theft of intellectual property or export-controlled technical data. Trafficking in child pornography and other child exploitation crimes are also a significant focus for us.

The Cyber Crime Center further works to develop tools and capabilities to conduct online cyber investigations, focusing on collaborative relationships with other Government agencies, to include DHS's Science and Technology, our friends at NPPD, National Cybersecurity Communications Integration Center, and our domestic and international law enforcement partners, especially our DHS counterpart, the United States Secret Service, as well as EUROPOL.

The Cyber Crime Center's budget has increased by more than $30 million since 2011, expending $137 million in fiscal year 2013. This growth underscores the increasing role the Internet plays in criminal activity and the need for skill and diligence to thwart crime in cyber space.

U.S. Immigration and Customs Enforcement has recognized the potential for criminal exploitation and the money-laundering threat posed by virtual currency. We therefore strategically deployed a multi-pronged investigative strategy designed to target illicit virtual currency, currency exchangers, and underground black markets, such as carding, illegal drugs, illegal firearms, and child pornography forums.

HSI has established itself as a world leader in online exploitation investigations because of the breath of its authorities and presence throughout the world. In fiscal year 2013 alone, our agency was responsible for more than 2,000 criminal arrests relating to child exploitation, while launching in excess of 4,000 child exploitation investigations worldwide. Both are new records for Homeland Security Investigations and the Department of Homeland Security.

In 2013 there were 927 children identified as victims during the course of Immigration and Customs Enforcement (ICE) HSI-led joint online child exploitation investigative work.

The Cyber Crime Center oversees the agency's computer forensics program, which comprises approximately 250 computer forensics agents and analysts. Our computer forensics agents jointly train with the Secret Service and Internal Revenue Service (IRS) Criminal Investigations. Homeland Security Investigations' computer forensics agents (CFAs) also support investigations in the use of digital media as well as support to Federal, State, and local law enforcement upon request.

In fiscal year 2013, HSI–CFA has encountered approximately 3.9 petabytes of data, equal to approximately 62 billion pages of image files or 71 billion pages of Powerpoint files. In April 2013, we engaged in a relationship with the National Association to Protect Children (PROTECT) to launch the Human Exploitation Rescue Operative (HERO), Child Rescue Corps. During the 12-month internship, we hired wounded warriors who were integral in conducting computer forensics law enforcement-based investigations.

Senator LANDRIEU. You have to try to wrap up if you would.

Mr. EDGE. The Cyber Center will continue to evaluate its cyber capabilities, programs, and training, and will make sure the agency can effectively continue combating this ever-changing landscape in the future.

Thanks again for the opportunity to appear before you, and I look forward to answering any questions you may have.

[The statement follows:]

PREPARED STATEMENT OF PETER T. EDGE

INTRODUCTION

On behalf of the men and women of U.S. Immigration and Customs Enforcement (ICE), thank you for the opportunity to appear before you today to discuss cybersecurity and the impact ICE's Cyber Crime Center (C^3) makes with respect to protecting our Nation's borders and enhancing public safety. C^3 has been in existence since 1997 and was created to support the investigative mission of the U.S. Customs Service. Now, 17 years later, C^3 is recognized worldwide as a center of excellence in cyber law enforcement. ICE expenditures for cyber crime investigations have increased 39 percent since fiscal year 2010. Additionally, cyber crimes investigations account for 9 percent of total Domestic Investigations expenditures compared to 6.5 percent in fiscal year 2010.

Fiscal year:	2010	2011	2012	2013	Fiscal year 2010 to fiscal year 2013 variance
Cyber Crime & Child Pornography Investigations	$92	$98	$109	$119	$28
Cyber Crimes Center	16	17	11	18	2
Total Cyber Crimes Expenditures	108	115	120	137	30
Percent of Total Expenditures	6.5%	6.8%	7.0%	8.6%	27.4%
Total HSI Domestic Expenditures	$1,648	$1,701	$1,723	$1,596	$(52)

ICE Homeland Security Investigations (HSI) is the principal investigative arm of the U.S. Department of Homeland Security (DHS) and the second largest Federal criminal investigative agency, with broad legal authority to enforce more than 400 Federal statutes. HSI has taken a leading role in coordinating domestic and international law enforcement actions among our law enforcement partners through several centers of excellence that we lead—including C^3.

The Internet poses a significant challenge to law enforcement. When a criminal never has to meet his victim face to face, but can hide behind what appears to be a legitimate Web site, consumer fraud runs rampant. When transnational criminal organizations employ technical means to steal intellectual property, American ingenuity is stymied. When money launderers utilize non-traditional, Internet-based financial services, circumventing regulatory safeguards, public safety is further threatened. Criminal networks are becoming increasingly sophisticated in taking advantage of the many ways in which the Internet can streamline communications, financing, and logistics—just as it does for legal enterprise. As a consequence, law enforcement agencies must respond by properly preparing investigators for work in cyberspace. As information systems and computer networks become increasingly prolific, the technical challenges facing law enforcement investigations of criminals operating on, or through, the Internet grow daunting, and the considerations in collecting electronic evidence become increasingly complex. A recent HSI enforcement action targeting intellectual property violations saw the deployment of 5 percent of HSI's Computer Forensics Agents (CFAs) in a single day. These CFAs were tasked with securing the electronic evidence from nine Web sites, and they will be heavily involved in sorting through the evidence for potential prosecutions.

CYBER CRIMES CENTER

C^3 brings the full range of ICE cyber investigations and computer forensic assets together in a single location to coordinate global investigations and to provide support to our field offices in their efforts combat cyber-enabled crime. C^3 is comprised of three units: the Cyber Crimes Unit, the Computer Forensics Unit, and the Child Exploitation Investigations. The C^3 facility houses a cyber investigations training room and a computer forensics laboratory. The Center is staffed by special agents, intelligence research specialists, computer forensics analysts, and mission support personnel. Each of C^3's units plays an integral role in supporting investigations of cybercrime and cyber-enabled crime. The scope of these investigations includes any instance where information technology, or computer networks are substantially employed to facilitate international smuggling, money laundering, Internet-based financial frauds or identity theft, proliferation of strategic commodities or the theft of export controlled technical data, and trafficking in child pornography and other child exploitation crimes. The Cyber Crimes Unit and Child Exploitation Investigations Unit provide coordination, de-confliction, resources, training, and subject matter expertise in these investigations. The Computer Forensics Unit oversees the agency's computer forensics program, including the agency's participation in, and contributions to, the Treasury Computer Forensics Training Program.

Cyber Crimes Unit

The Cyber Crimes Unit supports HSI investigations of cyber enabled criminal activities. The Cyber Crimes Unit provides oversight, coordination, de-confliction, resources, and subject matter expertise to HSI offices in the investigation of international smuggling, proliferation, fraud, and money laundering activities where information systems, networks, and the Internet serve as significant facilitating mechanisms for the crime. The Cyber Crimes Unit particularly focuses its efforts towards cyber economic crimes involving financial fraud, the theft of digital intellectual property and technical data controlled under export laws, and the targeting of cross-border illicit Internet marketplaces. The Cyber Crimes Unit also works to develop and deliver training to HSI personnel in the investigation of cyber-enabled crimes. The Cyber Crimes Unit further works to support HSI cyber investigations through its Emerging Technology program which focuses on collaborative relationships with other government agencies and academic institutions intended toward development of technical solutions to technical problem sets facing law enforcement.

Emerging Technologies

The Cyber Crimes Unit is also dedicated to the development of tools and capabilities to conduct online cyber investigations. Emerging technology, such as The Onion Router, also known as TOR, or the utilization of virtual currencies, allow the transnational criminal organizations to navigate in cyberspace anonymously. C^3 has partnered with DHS Science and Technology to collaborate with academia and other partners to develop tools and best practices, to stay abreast of emerging technologies and continue to lean in to prevent and deter illegal activities.

Virtual Currency

In contrast to traditional currency, monetary instruments, or other methods of transferring value, virtual currencies serve as mediums of exchange, but are not accepted as legal tender in any recognized government jurisdiction. However, virtual currencies can be used to conduct transactions entirely within a virtual economy, transferred between individuals, or used in lieu of a government-issued currency to purchase goods and services.

The appeal of virtual currencies, especially "open" or "convertible" currencies that can be exchanged for traditional currency, and vice versa, is that they may allow value to be transferred much more rapidly and cheaply (especially internationally) than through traditional banking payment systems, and often with greater anonymity and reduced oversight.

ICE has recognized the potential for criminal exploitation and the money laundering threat posed by virtual currency. ICE has, therefore, strategically deployed a multi-prong investigative strategy designed to target illicit virtual currency platforms, currency exchangers, and underground black markets such as "carding," illegal drugs, illegal firearms, and child pornography forums.

ICE recognizes that our approach to combating the illicit use of virtual currency systems must include collaboration and coordination with our domestic and international partners. To that end, ICE works closely with our Federal, State, local, and international law enforcement partners, and other members of the interagency.

RECENT INVESTIGATIONS

Crack99

Among HSI's broad investigative authority, we are the primary enforcer of the Arms Export Control Act and as such has responsibility to work with industry to safeguard this data from being exploited and smuggled out of the country. This includes the investigation of Web sites that offer the sale of prohibited items as well as transnational criminal organizations that steal the data without the knowledge of industry.

HSI Philadelphia learned during a private industry outreach meeting, of an online company known as Crack99, believed to be involved in the illegal sale of U.S.-manufactured software products. HSI collaborated with Defense Criminal Investigative Services and conducted numerous undercover purchases of stolen software from Crack99. Once payment had been made and accepted in China, the software was posted and received, often compressed into specialty files and then "cracked" to overcome the license restrictions. The software programs were used in multiple design and engineering systems that had a broad range of user applications to include: explosive simulation, aircraft mission simulation, oil field management, antenna design and radio frequency signaling.

Many of the U.S.-manufactured software programs offered by Crack99 were controlled for export and were subject to the Department of Commerce's Export Administration Regulations. The estimated monetary loss of these illegal software sales conducted by Crack99 was valued at approximately $1 million. Crack99 had "cracked" the software of thousands of U.S. businesses.

HSI Special Agents identified the U.S.-based servers and seized all accounts, Web sites and domains associated with Crack99's distribution of stolen software. Two servers and six domain names were seized. The three main suspects were charged, convicted and sentenced for various violations of conspiracy, fraud, smuggling and copyright infringement.

Mt. Gox

In May 2013, through an interagency taskforce led by ICE in Baltimore, Maryland, three U.S. bank accounts associated with what was then the world's largest Bitcoin (a specific virtual currency) exchanger, Japan-based Mt. Gox, were seized for violations of 18 U.S.C. section 1960, operating a money service business in the United States without a license. Some of the funds were linked to the illicit purchase of drugs, firearms, and child pornography. These and many other ongoing criminal investigations have provided ICE with a better understanding of the risks and challenges posed by virtual currencies.

Online Child Exploitation Investigations

ICE has established itself as a world leader in online child exploitation investigations due to the breadth of its authorities and presence throughout the world. Under the auspices Operation Predator, HSI child exploitation investigations focuses on the enforcement, disruption and dismantlement of individuals and groups involved in the possession, receipt, distribution, transportation, and production of child pornography. Since the launch of Operation Predator in 2003, HSI has initiated more than 30,700 criminal investigations; arrested more than 10,900 child predators; and contributed to more than 8,000 indictments and criminal convictions for child exploitation violations. In fiscal year 2013 alone, our agency was responsible for over 2,000 criminal arrests relating to child exploitation, while launching in excess of 4,000 child exploitation investigations worldwide, both new records for HSI. In fiscal year 2013, there were 927 children identified as victims during the course of ICE HSI-led or joint child exploitation and/or child sex tourism investigations. Key to HSI's fight against child exploitation is HSI's C^3. C^3 directs HSI in its mission to investigate large-scale producers and distributors of child pornography, as well as individuals who travel abroad for the purpose of engaging in sex with minors, also known as Child Sex Tourism (CST). C^3 employs the latest technology to collect evidence of persons and organized groups who sexually exploit children through the use of Web sites, chat rooms, newsgroups and peer-to-peer trading. C^3 also provides assistance to HSI field offices, coordinates major investigations, and conducts undercover operations throughout the world to identify and apprehend violators.

Operation Round Table

In March 2014, HSI completed the largest online child exploitation investigations in ICE's history, involving victims in 39 States and five countries. Fourteen men operating a child pornography Web site on the Darknet's Onion Router (TOR) were arrested and charged as part of a conspiracy to operate a child exploitation enterprise, following an extensive international investigation by HSI and the U.S. Postal Inspection Service (USPIS).

To date, investigators have identified 251 minor victims in 39 States and five foreign countries: 228 in the United States and 23 in the United Kingdom, Canada, New Zealand, Australia and Belgium. Eight of the victims were female and 243 were male. The majority of victims, 159, were 13 to 15 years old; 59 victims were 16 and 17; 26 victims were 10 to 12; four victims were 7 to 9; one victim was 4 to 6; and two victims were 3 years old or younger. All victims have been contacted by law enforcement and U.S. victims have been offered support services from HSI victim assistance specialists.

Victim Identification Program

Although the traditional law enforcement goal in combating child exploitation is normally viewed to be "arresting and prosecuting predators," the true goal is to protect children. In furtherance of this goal, HSI launched the Victim Identification Program (VIP) in December 2011. Its mission is to combine technological and investigative capabilities and resources to rescue child victims of sexual exploitation. The VIP is a simple idea that combines traditional investigative techniques with cutting edge technology for the purposes of rescuing child victims of sexual exploitation. The victim identification process starts with the discovery of new child abuse material (images, video, and/or audio) that depicts an unidentified minor or minors being sexually abused. HSI analyzes and enhances the material in order to identify clues that may lead to the identity of the victim, suspect or geographic location. When enough clues come together to form a viable lead, the lead is sent out to the appropriate HSI field office for follow-up investigation. During its first 2 years of operation, the VIP has been responsible for more than 180 victims identified and/or rescued from around the country. HSI is increasingly shifting its focus and dedicating more of its time and resources towards identifying and rescuing the victims of child sexual exploitation and the prevention of these crimes. This focus on victims is not in conflict with ongoing efforts to arrest and prosecute the perpetrators of these horrendous crimes as the identification of victims often leads to the arrest of their abusers.

Project iGuardian

In April 2014, ICE launched an educational outreach program called Project iGuardian, in conjunction with the National Center for Missing and Exploited Children's NetSmartz and the Internet Crimes Against Children (ICAC) Task Forces. Project iGuardian is an outreach awareness program that aims to educate kids, teens, and parents about online safety and how to stay safe from online sexual predators. HSI recognizes the importance of education and community awareness regarding the dangers of online activity. Project iGuardian aims to counter a disturbing fact: many online child predators are able to find victims online because children are not aware of how dangerous online environments can be.

Virtual Global Taskforce

ICE is a founding member and the U.S. representative of the Virtual Global Taskforce (VGT), an international alliance of law enforcement agencies and private industry sector partners working together to prevent and deter online child sexual abuse. In December 2012, HSI was appointed chair and secretariat of the VGT. The Deputy Assistant Director of C^3 assumed the duties of chair for a 3-year tenure. At the same time HSI was appointed the chair, the VGT also agreed to include investigations of CST into its portfolio.

Operation Predator—Smartphone App

In September of 2013, HSI launched a new smartphone app, the first of its kind in U.S. Federal law enforcement, designed to seek the public's help with fugitive and unknown suspect child predators. All tips can be reported anonymously through the app, by phone or online, 24 hours a day, 7 days a week. In many cases, HSI has been able to make an arrest just hours after issuing a nationwide plea for public assistance. These cases demonstrate the power of the press, social media and the general public in helping solve cases.

Computer Forensics Program

C^3 operates and maintains a robust computer forensics program. HSI computer forensic agents/analysts (CFAs) support all HSI investigations involving the use of digital media, as well as provide support to Federal, State and local law enforcement upon request. The computer forensic program is currently comprised of approximately 250 CFAs located in over 110 domestic and foreign HSI offices. The CFAs operate in various environments, supporting investigations to include advanced mobile device data extraction, hard drive repair, data mining of large multi-terabyte data sets, password decryption, border search of electronic devices and on-scene computer forensic assistance. For example, HSI CFAs were instrumental in the seizure of closed circuit video systems that were used in the identification of the Boston Marathon bombing suspects and provided key support for the analysis of suspect media related to Operation Round Table detailed above.

In fiscal year 2013, HSI CFAs encountered approximately 3.9 petabytes of data (equal to approximately 62 billion pages of image files or 71 billion pages of power point files) and analyzed over 4,400 mobile devices; this is a 45-percent increase in the volume of data encountered and a 35-percent increase in the number of mobile devices analyzed from the previous fiscal year.

HSI is a founding member of the Treasury Computer Forensic Training Program (TCFTP), which is a joint computer forensic training initiative between HSI, the U.S. Secret Service and the Internal Revenue Service-Criminal Investigations. Management of the training program rotates every 2 years, with HSI responsible for administering the program for 2014 and 2015. For 2014, it is anticipated that approximately 200 individuals will receive basic or advanced computer forensic training through the joint training program. This program was designed to provide CFAs operating in the field with the skills necessary to support the ever changing environment of the computer forensic requirements for HSI's investigative mission. In addition to providing training through the TCFTP, the computer forensic program regularly provides computer forensic training for capacity building efforts to foreign law enforcement.

Human Exploitation Rescue Operative Chile Rescue Corps

In April 2013, ICE, entered into a partnership with U.S. Special Operations Command and the National Association to Protect Children (PROTECT) to launch the "Human Exploitation Rescue Operative (HERO) Child Rescue Corps" program. The 12-month internship program is a highly competitive, highly selective non-paid internship, designed for wounded, injured and ill Special Operations Forces to receive training in high-tech computer forensics and law enforcement skills to assist HSI and law enforcement in their efforts to combat child sexual exploitation. Upon successful completion of the training, HERO participants are embedded into computer forensic analyst positions within HSI offices to receive on-the-job training experience. Fifteen HERO participants of the inaugural class have successfully completed all aspects of the program thus far and HSI in the process of extending offers of employment to all 15 individuals under the Veterans' Recruitment Appointment authority. The HERO program is in the process of recruiting, interviewing and selecting candidates for the 2nd HERO class, which is scheduled to begin in August 2014.

DHS Secretary's Honors Program—Cyber Student Initiative

The DHS Cyber Student Volunteer Initiative, introduced in 2013 by DHS and HSI, offered college students majoring in a cybersecurity-related field an unpaid volunteer position to gain invaluable hands-on experience at a DHS component agency. HSI was the sole DHS component to participate in the inaugural program, which was designed to provide high-performing students with challenging work projects, real-life learning scenarios, and mentoring from cybersecurity professionals at various HSI field offices. Based on the success of the program, DHS and HSI offered the Student Volunteer Initiative program again in 2014, which was expanded to include new volunteer opportunities at the U.S. Secret Service, the U.S. Coast Guard, the Transportation Security Administration, the Office of Intelligence and Analysis, the DHS Office of the Chief Information Officer, and State and major urban area fusion centers.

CONCLUSION

Thank you again for the opportunity to appear before you to highlight ICE's Cyber Crime Center and the significant role we contribute in combating transnational criminal organizations operating in cyberspace and in an increasingly more complex and sophisticated virtual reality. As the cyber world and other new virtual technologies continue to evolve, ICE will remain vigilant and adapt its investigative tools and techniques to dismantle those criminal organizations that use this platform to hide illicit activity.

Senator LANDRIEU. Thank you so much for that excellent testimony.

Mr. Noonan.

STATEMENT OF WILLIAM NOONAN, DEPUTY SPECIAL AGENT IN CHARGE, CRIMINAL INVESTIGATIVE DIVISION—CYBER OPERATIONS, SECRET SERVICE, DEPARTMENT OF HOMELAND SECURITY

Mr. NOONAN. Yes, ma'am. Good afternoon, Chairman Landrieu, Ranking Member Coats, and Senator Coons. Thank you for the opportunity to testify on the Department of Homeland Security's investments to counter cyber threats and the capabilities the Secret Service utilizes and is developing to deter cyber crime around the world. I am honored to appear today alongside my colleagues from Immigration and Customs Enforcement and the National Protection and Programs Directorate.

While no single agency or department has the personnel and resources to eliminate all cyber threats, DHS brings to the table a strong combination of Federal law enforcement experience, established partnerships across Federal, State, and local governments, international law enforcement, and the private sector, as well as a workforce that is committed to strengthening the security and resiliency of our Nation's critical infrastructure.

When the Secret Service was created as an investigative division of the Department of Treasury in 1865, its sole focus was to protect the Nation's financial system from the proliferation of counterfeit currency. Over the past 149 years the agency's mission has expanded to include protecting the President, the Vice President, visiting world leaders, and national special security events. Today our integrated mission addresses numerous threats, including those originating in cyber space.

The Secret Service's authorities to investigate cyber crime date back nearly 30 years to when Congress passed the Comprehensive Crime Control Act of 1984. That law granted the Secret Service authority to investigate criminal offenses related to unauthorized access to computers and the fraudulent use or trafficking of access devices.

As the Nation's financial payments systems evolved from paper to plastic to electronic transactions, so too has the Secret Service's investigative priorities. Advances in computer technology and greater Internet access to personally identifiable information and sensitive financial data have created online marketplaces for transnational cyber criminals to share stolen information and criminal methodologies.

Over the past 10 years, the Secret Service has observed marked increase in the quantity and complexity of cyber crimes targeting private industry, in particular the financial services sector. These crimes include network intrusions, installation of malicious software, and account takeovers, leading to significant data breaches affecting every sector of the world's economy.

The widely reported data breaches of Target, Neiman Marcus, White Lodging, and Michaels are just some of the most recent well-publicized examples of major data breaches perpetrated by cyber criminals who are intent on targeting our Nation's financial payments systems. Over the past 4 years alone, the Secret Service cyber crime investigations have resulted in more than 4,900 arrests associated with approximately $1.4 billion in fraud losses and the prevention of $11 billion in potential fraud losses.

Through continued work with our key Federal, State, local, international, and private-sector partners, we are confident we will continue to bring domestic and transnational cyber criminals to justice.

In support of the Secret Service's protective mission, special agents trained through the agency's Critical Systems Protection (CSP) program successfully completed more than 657 domestic and 5 international protective advances since 2010 in support of the President, Vice President, and national special security events. The incorporation of tools and specialized training to reduce the risk associated with a viable cyber threat during protective operations enhances the Secret Service's ability to provide complete protective coverage.

CSP technology provides visibility into the once unknown cyber environment, which gives our agency the tools to identify cyber threat actors as well as mitigate potential network attacks on the critical infrastructure that supports permanent and temporary venues under Secret Service protection.

With the subcommittee's support, the Secret Service will continue to focus on improving our protective investigative capabilities and enhancing the training of our special agent workforce through the Electronic Crimes Special Agent Program, as well as provide training for our State and local law enforcement partners through the National Computer Forensic Institute. We will also continue to share actionable information with our partners through DHS's National Cybersecurity and Communications Integration Center and the network of Information-Sharing and Analysis Centers (ISACs), in particular the Financial Services and Multistate ISACs, while aggressively investigating cases through our domestic international field offices, as well as our network of electronic crimes task forces.

On the basis of the Secret Service's experience with cyber investigations and protection, I hope today's discussion provides the subcommittee useful information on how to best deter and mitigate the threat of these crimes in the future. This concludes my opening remarks. I look forward to your questions. Thank you.

[The statement follows:]

PREPARED STATEMENT OF WILLIAM NOONAN

Good afternoon Chairman Landrieu, Ranking Member Coats, and distinguished members of the subcommittee. I appreciate the opportunity to testify on the investments the Department of Homeland Security (DHS) is making in cybersecurity, and the capabilities the Secret Service has and is developing to deter cyber-crime around the world. I am honored to appear today alongside my colleagues from Immigration and Customs Enforcement (ICE) and the National Protection and Programs Directorate (NPPD). While no single agency or department has the personnel and resources to eliminate cyber-threats, DHS brings to the table a strong combination of Federal law enforcement experience, established partnerships with the Department of Defense, the Department of Justice (DOJ), State and local governments, international law enforcement and the private sector, as well as a workforce committed to strengthening the security and resiliency of our Nation's critical infrastructure.

Cyber-threats impact all aspects of the Secret Service's integrated mission. When the agency was created as an investigative arm of the Department of Treasury in

1865, its purpose was to protect the Nation's financial system from the proliferation of counterfeit currency. No one at the time could have foreseen that the Secret Service would one day be responsible for the protection of the President of the United States, let alone that protection would have to take into account the potential for computers to affect physical security. Likewise, no one at the time could have foreseen that financial crimes would encompass computer-based attacks on our Nation's financial services sector and would regularly include criminal actors working across international borders to perpetrate complex thefts and money laundering schemes.

The Secret Service traces its investigations into cyber-crime back nearly 30 years, when Congress authored 18 U.S.C. sections 1029 and 1030 as part of enacting the Comprehensive Crime Control Act of 1984 (Public Law 98–473). That law granted the Secret Service authority to investigate criminal offenses [1] related to the unauthorized access to computers [2] and the fraudulent use, or trafficking of, access devices [3]—defined as any piece of information or tangible item that is a means of account access that can be used to obtain money, goods, services, or other thing of value.[4] As the Nation's financial payment systems evolved from paper to plastic to electronic transactions, so too has the Secret Service's investigative priorities. Advances in computer technology and greater access to personally identifiable information (PII), including sensitive financial data, via the Internet have created online marketplaces for transnational cyber-criminals to share stolen information and criminal methodologies.

Over the past 4 years alone, Secret Service cyber-crime investigations have resulted in over 4,900 arrests, associated with approximately $1.37 billion in fraud losses and the prevention of over $11.24 billion in potential fraud losses. Through continued work with our key partners at DOJ, in particular the local U.S. Attorney's Offices, the Computer Crime and Intellectual Property Section (CCIPS), and the International Organized Crime Intelligence and Operations Center (IOC–2), we are confident we will continue to bring cyber-criminals to justice.

Since 2010, in support of the Secret Service's protective mission, special agents trained through the agency's Critical Systems Protection (CSP) program successfully completed more than 657 domestic and five international protective advances. The incorporation of tools and specialized training to reduce the risks associated with a viable cyber-threat during protective operations enhances the Secret Service's ability to provide complete protective coverage at venues visited by the President, Vice President and other Secret Service protectees.

CSP technology provides visibility into the once unknown cyber-environment, which gives the Secret Service the ability to identify cyber-threat actors, as well as mitigate the potential impact of a network attack on a protective venue or on the critical infrastructure that supports the venue. CSP-trained special agents also lead the Critical Infrastructure Protection Subcommittee during National Special Security Events (NSSEs). Through their work with Federal, State and local law enforcement, along with the private sector, CSP-trained special agents develop a comprehensive operational security plan to safeguard critical infrastructure and key resources associated with protective events and associated venues.

Based on the Secret Service's three decades of experience investigating cyber-crime, in particular the expertise we have developed with respect to the transnational organized cyber-crime threat to our Nation, as well as our more recent efforts to protect the President, Vice President, and NSSEs from a cyber-threat, I hope to provide the subcommittee useful information on how best to deter and mitigate the threat of these crimes in the future.

THE TRANSNATIONAL CYBER-CRIME THREAT

Over the past 10 years, the Secret Service has observed a marked increase in the quality, quantity, and complexity of cyber-crimes targeting private industry, in particular the financial services sector. These crimes include network intrusions, hacking attacks, installation of malicious software, and account takeovers leading to significant data breaches affecting every sector of the world economy. The widely reported data breaches of Target, Neiman Marcus, White Lodging, and Michael's are just the most recent, well-publicized examples of this decade-long trend of major data breaches perpetrated by cyber-criminals who are intent on targeting our Nation's banks and financial payment systems.

[1] *See* 18 U.S.C. section 1029(d) and 1030(d)(1).

[2] *See* 18 U.S.C. section 1030.

[3] *See* 18 U.S.C. section 1029.

[4] *See* 18 U.S.C. section 1029(e)(1).

In partnership with the Secret Service, Verizon published their most recent Data Breach Investigations Report (Verizon Report) in 2014 to examine current trends and criminal tactics used to conduct data breaches. The analysis included in the 2014 Verizon Report covered more than 63,000 security incidents, including 1,367 confirmed data breaches occurring in calendar year 2013. The report identified three primary motives for the criminals committing these acts: (1) financial gain; (2) espionage; and (3) activism.

Cyber-criminals, motivated by greed, perpetrated the majority of the breaches studied each of the past 5 years through the Verizon Reports. These criminals primarily use a combination of sophisticated hacking techniques and the deployment of malicious software to accomplish their objective of obtaining sensitive financial information to use as part of increasingly sophisticated frauds. The victims of the crimes studied in the 2014 Verizon Report span 95 different countries, with 34 percent of all reported incidents affecting financial institutions. The study revealed that point-of-sale (POS) intrusions, like the recently reported events, are primarily attributed to organized criminal groups operating out of Eastern Europe. More concerning, in 88 percent of POS intrusions, the data is exfiltrated in a matter of minutes. However, in 98 percent of the breaches it took weeks or months to discover the crime.

The increasing level of collaboration among cyber-criminals allows them to compartmentalize their operations, greatly increasing the sophistication of their criminal endeavors as they develop specialized skills to carry out cyber-attacks against the Nation's financial and other critical infrastructures. These specialties increase both the complexity of investigating these cases, as well as the level of potential harm to companies and individuals. For example, illicit underground cyber-crime marketplaces allow criminals to buy, sell and trade malicious software, access to sensitive networks, spamming services, payment card data, PII, bank account information, brokerage account information, hacking services, and counterfeit identity documents. These illicit digital marketplaces vary in size, with some of the more popular sites boasting membership of approximately 80,000 users. Within these digital marketplaces, criminals often use various digital currencies to conduct transactions, such as paying for stolen information, requesting various criminal services, or laundering illicit proceeds.

As a part of our cyber-crime investigations, the Secret Service targets the most capable cyber-criminals and the individuals who operate illicit infrastructure that supports transnational organized cyber-criminals. For example, in May 2013, as part of a joint investigation through the Global Illicit Financial Team, the Secret Service shut down the digital currency provider Liberty Reserve. Liberty Reserve is alleged to have had more than one million users worldwide and to have laundered more than $6 billion in criminal proceeds. This case is believed to be the largest money laundering case ever prosecuted in the United States and is being jointly prosecuted by the U.S. Attorney's Office for the Southern District of New York and DOJ's Asset Forfeiture and Money Laundering Section. In a coordinated action with the Department of the Treasury, Liberty Reserve was identified as a financial institution of primary money laundering concern under Section 311 of the USA PATRIOT Act (Public Law 107–56), effectively cutting it off from the U.S. financial system.

The Secret Service has successfully investigated many underground cyber-criminal marketplaces. In one such infiltration, the Secret Service initiated and conducted a 3-year investigation that led to the indictment of 11 perpetrators allegedly involved in hacking nine major American retailers and the theft and sale of more than 40 million credit and debit card numbers. The investigation revealed that individuals from the United States, Estonia, China and Belarus successfully obtained credit and debit card numbers by hacking into the wireless computer networks of major retailers—including TJ Maxx, BJ's Wholesale Club, Office Max, Boston Market, Barnes & Noble, Sports Authority and Dave & Buster's. Once inside the networks, those individuals installed "sniffer" programs[5] that would capture card numbers, as well as password and account information, as that information moved through the retailers' credit and debit processing networks.

After the data were collected, the alleged conspirators concealed the information in encrypted computer servers they controlled in the United States and Eastern Europe. The credit and debit card numbers were then sold through online transactions to other criminals in the United States and Eastern Europe. The accounts associated with the stolen numbers were "cashed out" by encoding card numbers on the magnetic strips of blank cards. The alleged perpetrators then used these fraudulent

[5] Sniffers are programs that detect particular information transiting computer networks, and can be used by criminals to acquire sensitive information from computer systems.

cards to withdraw tens of thousands of dollars at a time from ATMs. The illegal proceeds were allegedly concealed and laundered by using anonymous Internet-based digital currencies within the United States and abroad, and by channeling funds through bank accounts in Eastern Europe. Card numbers were then sold through online transactions to other criminals in the United States and Eastern Europe. The accounts associated with the stolen numbers were "cashed out" by encoding card numbers on the magnetic strips of blank cards. The alleged perpetrators then used these fraudulent cards to withdraw tens of thousands of dollars at a time from ATMs. The illegal proceeds were allegedly concealed and laundered by using anonymous Internet-based digital currencies within the United States and abroad, and by channeling funds through bank accounts in Eastern Europe.card numbers were then sold through online transactions to other criminals in the United States and Eastern Europe. The accounts associated with the stolen numbers were "cashed out" by encoding card numbers on the magnetic strips of blank cards. The alleged perpetrators then used these fraudulent cards to withdraw tens of thousands of dollars at a time from ATMs. The illegal proceeds were allegedly concealed and laundered by using anonymous Internet-based digital currencies within the United States and abroad, and by channeling funds through bank accounts in Eastern Europe.[6]

The impact of these criminal acts extends well beyond the companies compromised, potentially affecting millions of people. Cyber-crime directly impacts the our economy by requiring additional investment in implementing enhanced security measures, inflicting reputational damage on American companies, and dealing with the financial losses from fraud—all costs that are ultimately passed on to consumers. Proactive and swift law enforcement action protects consumers by preventing and limiting the fraudulent use of payment card data, stolen PII, or both.

CYBER INVESTIGATIONS

The Secret Service proactively investigates cyber-crime using a variety of investigative means to infiltrate transnational cyber-criminal groups. As a result of these proactive investigations, the Secret Service is often the first to learn of planned or ongoing data breaches and is quick to notify financial institutions and the victim companies with actionable information to mitigate the damage from the data breach and terminate the criminal's unauthorized access to their networks. One of the most poorly understood facts regarding data breaches is that it is rarely the victim company that first discovers the criminal's unauthorized access to their network; rather it is law enforcement, financial institutions, or other third parties that identify and notify the likely victim company of the data breach by identifying the common point of origin of the sensitive data being trafficked in cyber-crime marketplaces.

When the Secret Service identifies a potential network intrusion, the agency contacts the owner of the suspected compromised computer system in order to assess the data breach and to stop the continued theft of sensitive information and the exploitation of their networks. After the victim of a data breach confirms that unauthorized access to their networks has occurred, the Secret Service works with the local U.S. Attorney's office, or appropriate State and local officials, to begin a criminal investigation into the matter.

During the course of these criminal investigations, the Secret Service identifies the malware and means of access used to acquire data from the victim's computer network. In order to enable other companies to mitigate their cyber-risk based on current cyber-crime methods, we quickly share information concerning the cybersecurity incident with the widest audience possible, while protecting grand jury information, the integrity of ongoing criminal investigations, and the victims' privacy and confidentiality. The Secret Service shares this cybersecurity information through:

—DHS's National Cybersecurity & Communications Integration Center (NCCIC);

—The Information Sharing and Analysis Centers (ISACs);

—The public, private, and academic partnerships established through our Electronic Crimes Task Forces (ECTFs);

—The publication of joint industry notices; and

[6] Additional information on the criminal use of digital currencies can be referenced in testimony provided by U.S. Secret Service Special Agent in Charge Edward Lowery before the Senate Homeland Security and Governmental Affairs Committee in a hearing titled, "Beyond Silk Road: Potential Risks, Threats, and Promises of Virtual Currencies" (November 18, 2013).

—Contributions to leading industry and academic reports like the Verizon Report, the Trustwave Global Security Report, and the Carnegie Mellon CERT Insider Threat Study.

As we share cybersecurity information discovered in the course of our criminal investigations, we also continue our pursuit of the individuals responsible for the crimes. Due to the inherent challenges in investigating transnational crime, particularly the lack of cooperation of some countries with law enforcement investigations, it can take years to apprehend the top tier criminals responsible for cyber-crimes.

COLLABORATION WITH OTHER FEDERAL AGENCIES AND INTERNATIONAL LAW ENFORCEMENT

While cyber-criminals operate in a world without borders, the law enforcement community does not. The transnational nature of cyber-crime cases has increased the time and resources needed for successful investigation, arrest and adjudication. The partnerships developed through our ECTFs, the support provided by our Criminal Investigative Division, the liaison established by our 24 international offices, and the training provided to our special agents via the Electronic Crimes Special Agent Program (ECSAP) are all instrumental to the Secret Service's success in these investigations.

To strengthen our ability to investigate transnational cyber-crime, the Secret Service maintains ECTFs in London and Rome, has assigned agents to INTERPOL and EUROPOL, and operates cyber-crime working groups in the Netherlands, Estonia, Lithuania, Latvia, Ukraine, and Germany. The Secret Service also trains numerous international partners on investigating cyber-crime; in the past 3 years, the Secret Service has trained over 500 law enforcement officials representing over 90 countries in investigating cyber-crimes.

The Secret Service's investigations of transnational crime are facilitated by the dedicated efforts of both the Department of State and the DOJ's Office of International Affairs to execute Mutual Legal Assistance Treaties and other forms of international law enforcement cooperation, in addition to the relationships that develop between Secret Service agents and their foreign counterparts through the above-mentioned working groups and training efforts.

Within DHS, the Secret Service benefits from a close relationship with ICE's Homeland Security Investigations (ICE-HSI). Since 1997, the Secret Service, ICE-HSI (and its predecessor organization, the U.S. Customs Service), and the Internal Revenue Service have jointly trained on computer investigations through ECSAP. ICE-HSI is also a member of Secret Service ECTFs, and has been a valued partner on numerous cyber-crime investigations including the recent take down of the aforementioned digital currency, Liberty Reserve.

To further its cybersecurity information sharing efforts, the Secret Service also has a strong relationship with NPPD, including DHS's NCCIC. As the Secret Service identifies malware, suspicious IP addresses and other information through its criminal investigations, it shares information with the NCCIC which pushes actionable information out to the broader cybersecurity community to protect their systems from harm. The Secret Service continues to build upon its full-time presence at NCCIC to coordinate its cyber programs with other Federal agencies. In addition to the close partnership with the NCCIC, the Secret Service also has an effective relationship with NPPD's protective security advisors (PSAs) and cybersecurity advisors in advancement of our cyber protection activities. Currently, 66 percent of all PSAs are co-located in Secret Service field offices around the country.

CYBER PROTECTION

The Secret Service is world-renowned for the physical protection it provides to the President and Vice President, visiting foreign heads of state and government, the White House and other protected sites, and NSSEs. In order to ensure a secure environment for our protectees, the Secret Service integrates a variety of innovative technologies and maintains a highly skilled workforce.

The Secret Service's protective mission is comprehensive and goes well beyond surrounding a protectee with well-trained special agents and Uniformed Division officers. Over the years, the agency's protective methodologies have become more sophisticated, incorporating such tools as airspace interdiction systems, and enhanced chemical, biological, radiological, and nuclear (CBRN) detection systems through the Operational Mission Support program. As part of the Secret Service's continuous goal of preventing an incident before it occurs, the agency relies on meticulous advance work and threat assessments to identify potential risks to our protectees. Since much of our Nation's critical infrastructure is becoming increasingly interdependent, the threat of a cyber-attack directed toward our protective interests cannot be ignored.

The Secret Service's CSP program identifies, assesses, and mitigates risk posed by information systems to persons and facilities protected by the Secret Service. The program supports a full spectrum of protective operations to include domestic and foreign trips, as well as NSSEs. It accomplishes its mission in support of the Presidential, Vice Presidential and Dignitary Protective Divisions by assessing the level of risk caused by the disruption, damage or destruction of process control systems critical to an event or venue. The CSP program implements preventative, detective, and corrective controls to reduce risk from a viable cyber-threat during protective operations. The result is situational awareness of the overall cybersecurity environment during protective operations.

For example, since 2012, the Secret Service has deployed cyber protection tools in support of 7 of the 16 DHS designated critical infrastructure sectors. Most recently, during the 2014 State of the Union Address (SOTU), the Secret Service deployed its cybersecurity protection platform to defend critical infrastructure and key resources in the National Capital Region.

INVESTMENTS IN CYBERSECURITY

The President's fiscal year 2015 budget request for DHS includes $1.25 billion in discretionary spending for cybersecurity activities. The Secret Service's budget request accounts for $100.4 million, or roughly 8 percent of the total amount requested. The majority of this funding is requested under Domestic Field Operations to support the staffing associated with Secret Service cyber-crime investigations; training for our State and local law enforcement partners through the National Computer Forensics Institute (NCFI); training for special agents through ECSAP; and funding for the operational costs associated with our ECTFs. Within the amount requested, funding is also proposed to enhance the CSP program through the Cyber Security Presidential Protection Measures (CSPPM) program; support the staffing associated with international cyber-crime investigations; and continue the upgrades necessary to protect Secret Service data and systems from intrusion or intercept through the multi-year Information Integration and Technology Transformation (IITT) program. For the purposes of today's hearing, I would like to highlight a few of these efforts in more detail:

Cyber Protection Activities

The President's fiscal year 2015 budget request includes a total of $21.3 million for cyber protection, which primarily supports the staffing associated with this activity. Within this amount, the request also includes $3.9 million to enhance the Secret Service's cyber protection capabilities through the CSPPM program. This will enable the Secret Service to train an additional 24 special agents in the ECSAP network intrusion discipline. This training is a prerequisite for special agents to advance to the CSP program to fulfill mission critical assignments in cyber protection. The CSPPM request also includes funding to enhance the CSP's cybersecurity protection platform to improve cyber-resiliency at Secret Service protective venues, including those associated with NSSEs.

National Computer Forensics Institute

The President's fiscal year 2015 budget request includes $4 million for the NCFI, which will enable the Secret Service to train approximately 500 State and local law enforcement officers, prosecutors, and judges on current trends in cybersecurity and the potential obstacles they are likely to encounter during the course of their investigations. Located in Hoover, Alabama, the NCFI offers State and local law enforcement officers and prosecutors the training necessary to perform computer forensics examinations, respond to network intrusion incidents, and conduct electronic crimes investigations, while judges receive general education in these areas.

Since opening in 2008, the institute has held over 150 cyber investigative and digital forensics courses in 16 separate subjects and trained and equipped more than 3,000 State and local officials, including more than 2,300 police investigators, 840 prosecutors, and 230 judges from all 50 States and three U.S. territories. These NCFI graduates represent more than 1,000 agencies nationwide.

Electronic Crimes Task Forces/Electronic Crimes Special Agent Program

The President's fiscal year 2015 budget request includes $1.8 million for the training and operational costs associated with the Secret Service's ECTF and ECSAP programs. The requested amount in fiscal year 2015 will support equipment purchases and travel expenses for ECTF and ECSAP personnel. In addition to these base funds, the Secret Service usesTreasury Executive Office of Asset Forfeiture (TEOAF) funding to support the ECTF and ECSAP programs.

The Secret Service currently operates 35 ECTFs, including two based overseas in Rome, Italy, and London, England. Membership in our ECTFs includes over 4,000 private sector partners; 2,500 international, Federal, State, and local law enforcement partners; and 350 academic partners. By joining a Secret Service ECTF, our partners benefit from the resources, information, expertise and advanced research provided by our international network of members while focusing on issues with significant regional impact. For example, the New York ECTF, based in the Nation's largest banking center, focuses heavily on safeguarding our financial institutions and infrastructure, while the Houston ECTF works closely with partners such as ExxonMobil, Chevron, Shell, and Marathon Oil to protect the Nation's vital energy sector.

CONCLUSION

Safeguarding and securing cyberspace is a top priority for DHS. As part of that effort, the Secret Service is steadfast in its commitment to protect the President, Vice President, and NSSEs from the threat of cyber-attack, and to protect the Nation's financial payment systems by investigating and dismantling transnational criminal organizations involved in cyber-crime. Responding to the growth in these types of crimes, and the level of sophistication these criminals employ, requires significant resources and greater collaboration between law enforcement and its public and private sector partners. Accordingly, the Secret Service is focused on improving our protective and investigative capabilities and techniques, enhancing the training of our special agent workforce through ECSAP, providing training for our State and local law enforcement partners through the NCFI, sharing information with our partners and private industry through DHS's NCCIC while actively investigating cases though our ECTFs, and raising public awareness to deter and mitigate the cyber-threats our Nation faces today.

CYBER EDUCATION: BUILDING WORKFORCE

Senator LANDRIEU. Thank you very much.

Let me begin with you, Secretary. There are many aspects of cyber defense that we're going to try to cover in this short period of time, and of course the time will not allow us to go very in depth. But one of the areas that I've really been focused on because of my general interest in education is educating the next generation of cyber warriors or generating—educating the next generation of professionals that can step up and help fill this important gap.

It's been estimated, not by our committee but by others, the Department itself has stated a goal of educating 1.7 million students by 2021. That would be approximately 200,000 students a year. The President's budget cut the funding for cyber education by 52 percent. When we've inquired, they've said that DHS would still meet that number, but would use other programs and populations, et cetera, et cetera.

So I want to ask you all this question, but particularly the Under Secretary for Homeland. Try to take a minute or two and explain as clearly as you can how the Department of Homeland Security is working, either with the Department of Education or with DOD or with any partner that you might want to identify, to actually produce the 200,000 workers, professionals, and students at a variety of different ages, and what are some of the more successful programs that you have and some of the results that you have achieved?

Because I'm having a hard time getting a real handle on this. I hear a lot about it. I just can't quite see it.

Dr. SCHNECK. Thank you. First and foremost——

Senator LANDRIEU. You can pull that closer to you so you don't have to lean. I think it'll come closer to you. I feel like you're going to fall off that chair in just a minute. Or push yourself a little that way, whatever.

Dr. SCHNECK. The chair's nice and short. I can't fall off. This is good.

So thank you. First of all, thanks again for the support, and we look forward to working with you on this. This is a big challenge. As I mentioned, the Secretary has stated his emphasis on education and on building the next cyber workforce. One of the first things that he did was take me down to two universities and have us talk with students——

Senator LANDRIEU. Which two were they?

Dr. SCHNECK. We went to Georgia Tech and Morehouse. And he said we will do this again, and we have a program rolling out that looks at what universities we'll be going to. But that's one of many.

We are bucketing our efforts at this point sort of in three different areas, and then I can also go through some of the other types of programs we have. I'm going to want to follow up with you with a comprehensive readout. But our buckets simply are the following:

One is to identify the skill sets that we need. A lot of times when I go out and talk to students—and I do this a lot, of all ages, and leadership at all levels goes out and speaks as much as we can to students of all ages, from K through 12 actually through the graduate programs. We need them to know the skill sets they need to have, what is a cyber workforce. It's not someone who just operates a firewall. It can be anything from policy to highly technical or a combination.

The second bucket is to actively get out there and find out what they're studying, talk to the professors, influence the curricula in the universities, which is one of the things we're starting to do as we speak to the universities.

And third is, for example, to award scholarships for service, get involved in helping fund their education, give them a chance then back. They come and work in our labs. Especially at NPPD, we've had interns in cybersecurity and communications, in that component. And then we give them a taste of what it's like to serve in Government. They get those skills from us as well.

Then we have several other programs——

Senator LANDRIEU. I think that sounds good, but it's so general. What I'm going to continue to press you on is some specifics. Like I asked for the purposes of this hearing to get the document from DOD about what a cyber warrior must have, literally the levels of education and specific skill set that DOD is requiring. It is 100 pages or more of very, very specific requirements. I'm going to submit this all to the record. It's not classified in any way, of course.

[The information follows:]

The proposed funding reduction to National Protection and Programs Directorate (NPPD) Cybersecurity Education in fiscal year 2015 impacts the long-term goal of affecting 1.7 million students in 10 years through the Integrated Cybersecurity Education Communities (ICEC) project. However, NPPD leads several cybersecurity education projects serving a wide audience of students across the Nation, providing cybersecurity education programs as flexible and responsive as the rapidly changing cybersecurity environment. Each of these projects is an integral factor in strengthening the national cyber workforce pipeline and building a robust national cybersecurity workforce, ensuring we may sustain a safe, secure and resilient cyberspace. As such, NPPD proposes these additional projects be applied towards the 1.7 million student goal, one that can be reached within the 10-year timeframe.

1. Identify the Skill Sets Needed for a Cyber Workforce

In 2012, the Department of Homeland Security (DHS) conducted the Information Technology Workforce Assessment for Cybersecurity (ITWAC) in partnership with the Federal Chief Information Officers (CIO) Council. The ITWAC collected workforce data that identified the composition and capabilities of the Federal civilian cybersecurity workforce.

In 2014, DHS has partnered with academic institutions and the Department of Defense (DOD) to conduct the National Cybersecurity Workforce Assessment (NCWA). The NCWA is gathering data on the U.S. non-Federal cybersecurity workforce. Like the ITWAC, the NCWA will identify gaps and deficiencies in both the size and capability of the cybersecurity workforce. However, the NCWA will go beyond the ITWAC to define specific occupational categories aligned to the National Cybersecurity Workforce Framework and the role that government can play to remedy the identified deficiencies.

DHS also leads the development of the National Cybersecurity Workforce Framework. The Cybersecurity Framework is a national resource providing employers, employees, students, educators, trainers, and policy makers with a common language for describing cybersecurity work. The Cybersecurity Framework includes a detailed listing of knowledge, skills, and abilities (KSAs) required for specific cybersecurity positions. The KSAs are associated with Specialty Areas included in the Cybersecurity Framework to clearly define the qualifying service, education, or training needed to successfully perform tasks or functions associated with that specialty. A detailed listing of all of the KSAs included in the Cybersecurity Framework can be found at http://niccs.us-cert.gov/training/tc/framework/ksas.

2. Explore the Cyber Curricula in Universities

The National Security Agency (NSA) and DHS jointly sponsor the National Centers of Academic Excellence in Information Assurance Education (CAE/IAE), IA 2-Year Education (CAE/2Y), and IA Research (CAE/R) programs. The goal of these programs is to reduce vulnerability in our national information infrastructure by promoting higher education and research in IA and producing a growing number of professionals with IA expertise in various disciplines. There are 181 schools (in 43 States, DC, and Puerto Rico) with one or more CAE designations. Working with these schools through the CAE program provides DHS with an opportunity to influence cybersecurity curricula across the Nation. Each cybersecurity academic program has about 100 students, and therefore approximately 18,100 students annually are studying cybersecurity through the CAEs. More information on CAEs can be found at http://www.nsa.gov/ia/academic__outreach/nat__cae/index.shtml.

Note that DHS is deploying new criteria for designation as a CAE, revised in order to meet the cybersecurity demands of the Nation. The new criteria will rely on knowledge units (an academically oriented approach), moving away from the previous information assurance training standards.

3. Provide Scholarships for Service

DHS participates in the Scholarship for Service (SFS) program, designed to increase and strengthen the cadre of Federal IA professionals protecting the Government's critical information infrastructure. SFS (through the National Science Foundation) provides scholarships that may cover the typical costs to attend a participating institution, including tuition and education and related fees. In exchange, students agree to serve in a cybersecurity role in the Government for a period equivalent to the length of their scholarship (e.g., 2 academic years = 2 calendar years). The U.S. Office of Personnel Management (OPM) manages and tracks SFS placements within government. CAE-designated academic institutions may apply to receive SFS awards. A total of 51 institutions in 26 States and DC currently receive SFS scholarship awards. Over 450 students receive SFS scholarships each year. DHS sponsors the annual in-person SFS Job Fair (January in the DC area). SFS has also held virtual job fairs with DHS support. More information on the SFS program can be found at https://www.sfs.opm.gov/.

The Secretary's Honors Program for Cybersecurity (SHPC) is designed to develop technically skilled cyber professionals across DHS. Since the Program began in January 2012, there have been 11 participants who have had the opportunity to put their academic achievements to use in a hands-on environment while playing a vital role in protecting our Nation. Through rotational assignments, Honors Program participants observe how each component collaborates on cyber-related issues and work first-hand on critical issues or incidents in a fast-paced, growing environment. Participants, from SFS or CAE schools, spend 2 years in the program, and then have the opportunity to attain a permanent position at DHS.

4. Integrated Cybersecurity Education Communities Project

In fiscal year 2013, DHS/Cybersecurity Education and Awareness (CE&A) issued the competitive Cybersecurity Education and Training Assistance Program (CETAP) grant in the amount of $5 million to fund the Integrated Cybersecurity Education Communities (ICEC) project. In support of the National Initiative for Cybersecurity Education (NICE), the ICEC project holds cyber education summer camps in communities around the country, with the primary goal of educating high school teachers who will then return to their schools and affect numerous students each year, as well as integrate cyber content into their existing course curricula across multiple academic disciplines. As a result, four communities across the country will hold cyber education camps in the summer of 2014, with at least 36 high schools participating. Each high school will send six students and two teachers and each teacher will affect approximately 120 students over a year. Therefore, the anticipated impact will be nearly 9,000 students this summer.

5. Cyber Competitions

DHS/CE&A supports cyber competitions, sponsoring CyberPatriot, which affects numerous middle and high school students each year and steers them toward cybersecurity careers and studies. The expansion of the CyberPatriot program exposes cybersecurity to 12,000 students annually.

6. National Initiative for Cybersecurity Career Studies Portal

DHS/CE&A developed the National Initiative for Cybersecurity Careers and Studies (NICCS) portal, an online resource for government, industry, academia, and the general public to learn about cybersecurity awareness, education, careers, and workforce development opportunities. An ongoing success for DHS, the NICCS portal is available to the American public, assisting users of all ages in locating cybersecurity learning opportunities and careers. The NICCS portal also hosts the Cybersecurity Training Catalogue, providing a list of all cybersecurity or cybersecurity-related education and training courses offered in the United States.

NICCS Web traffic continues to show steady improvement. In May 2014, 6,280 unique users accessed NICCS, leading to just over 33,090 unique users seeking cybersecurity training this calendar year. Since its inception, NICCS has had close to 90,000 unique visitors.

7. Federal Virtual Training Environment (FedVTE) and Federal Cybersecurity Training Exercise (FedCTE)

DHS/CE&A continues to support training efforts for Federal and critical infrastructure cybersecurity professionals. The FedVTE is an online training platform, providing Federal cybersecurity and IT professionals with hands-on labs and training courses. The environment is accessible from any Internet-enabled computer and is free to users and their organizations. The FedVTE content library includes more than 800 hours of training, 150 demos, and 3,000+ pieces of content. The FedCTE provides training, labs, and competitions for Federal cybersecurity professionals. DHS is also piloting courses for State government cybersecurity professionals. Classes range from one to three days and are conducted both live and virtually on a variety of cybersecurity topics providing training, hands-on experiences, knowledge of best practices, and network opportunities. The FedVTE and FedCTE are each available to 125,000 Federal/critical infrastructure cybersecurity professionals per year.

In fiscal year 2014, DHS/CE&A will continue these major efforts and initiate several enhancements, all contributing to the effort to promote cybersecurity education across the Nation. DHS/CE&A plans to apply $5 million to the CETAP grant in fiscal year 2014, enabling the same four communities holding cyber education summer camps in the summer of 2014 to continue the camps in the summer of 2015 leading to an effect of nearly 10,000 students that is a combined total of 19,000. DHS/CE&A estimates 60 percent of the 9,000 students reached the summer of 2014 (5,400 students), plus potentially another 10,000 students will be reached outside of the summer camp, resulting in 34,400 students reached by the end of 2015. The grant also supports development of cybersecurity-integrated high school curricula, which high schools across the country can adopt and offer to numerous students each year. Further, DHS/CE&A will develop additional and continued interest in cybersecurity careers and studies following the summer camps by promoting participation in cyber competitions and in virtual mentorships and internships. DHS/CE&A will continue participation in the CAE and SFS programs, reaching thousands of community college, 4-year school, and graduate students annually. DHS/CE&A will also launch a course intended to help professors and students in designated CAE schools understand the National Cybersecurity Workforce Framework and its relevance to CAEs. Further, DHS/CE&A will release Workforce Framework 2.0, codifying cybersecurity workforce roles. Finally, DHS/CE&A plans to add a search function to the Training Catalogue, so users seeking cybersecurity training on the NICCS portal will be able to browse courses based on their individual needs, thereby facilitating access to cybersecurity training for countless American students of all ages and their pursuit of cybersecurity certifications.

In summary, DHS/CE&A's programs focus on the cybersecurity education and awareness of the Nation, including students. When combined, the existing DHS/CE&A activities enable DHS to reach, and potentially exceed its goal of educating 1.7 million students in cybersecurity in 10 years. America's students are pursuing various levels of education and DHS/CE&A has made great strides in facilitating these students' pursuit of cybersecurity education and careers; redefining the goal of training 1.7 million students to include all of CE&A's activities accurately captures the reach of the program, its impact on the Nation, and the goal of DHS.

Senator LANDRIEU. But just one page, page 25, it says a person must normally have 1 to 5 years or more experience in IA technology in a related field. You have to have a systems environment, a computing environment. Knowledge applies, basic knowledge of IA concepts, practices, procedures, et cetera, et cetera.

I still think it would be really important for Homeland Security, probably in conjunction with DOD since they've already done it, and the Department of Education, to come up with a basic framework or a specific certification. Maybe we should do this, Senator Coats, with the private sector as well. I'm not sure. But I think at least in my experience, if the goal is to actually educate whatever, 1.5, 1.7, 2.5, you've got to measure it, have a way to measure it, to know if you're achieving it.

I can tell you as chair of this committee, as strongly as I feel in investing in education, I'm not going to invest money in programs that I'm not sure get a result. And I'm going to be holding through the whole Appropriations Committee the other subcommittees responsible, not holding but pressing them to be responsible, for allocating funding in a way that we can have some confidence that after we've allocated it we're actually producing, in partnership with universities, with the private sector, the kind of workforce and warriors we need to protect this country.

So I've run out of my time. I do have many more questions, but since that's been my emphasis I'm going to stay with it. There are other things I want to ask. But I'm going to turn it over to Senator Coats, and we may get a second round of questioning.

CREDIBILITY

Senator COATS. Dr. Schneck, as you know, DHS has been fighting some credibility issues in terms of capability. I was very impressed when I visited the center. You gave a terrific tour relative to what you've been able to accomplish. I think it looks like DHS has turned the corner on this, gaining credibility.

My understanding is that the strategy pretty much involves three things: one, limiting the Internet touch points to trusted Internet connections; establishing an effective perimeter capability; and deploying continuous diagnostics for managing the Federal system activity.

So my question is, generally where do we now stand today with the dot-gov domain relative to meeting these, implementing this strategy?

Dr. SCHNECK. Thank you again for your visit that day. We appreciate that.

On the perimeter side, we are now supporting not just intrusion detection, which is the system, see something come in and notify us; we're now supporting intrusion prevention under the term you may have heard, E3A, to about a quarter of the seats across the U.S. Government. That number will go up as our new service providers come online. For example, the one that supports DHS is just about to come on and will actually be engaging DHS in our own program, drinking our own champagne, as the team likes to say.

And then, continuous diagnostics and mitigation, which I did not have time to mention in my opening remarks, is a way of turning every network into its own ecosystem. So instead of having the team build a binder, a heavy binder every year, to talk about how secure it is, the system constantly measures how healed up it is and how secure it is, so you always know and you're always aware of behavior that's different.

As we grow that system, it'll become more and more like your body's immune system. You don't need to have a conference call to fight a cold. You always know something coming in and you'll be able to see. Because we see, even across the perimeter defense, different behaviors across all of the U.S. Government that can in the future help inform the networks, other agencies that are being protected by the external defense, as well as these internal immune systems, can learn to recognize bad behaviors.

So our vision is not only operational both in the internal, watching the network behavior, and the internal prevention, but also in using that core that makes DHS unique in NPPD, not only our core ability to work with our partners in the Secret Service and research and development and HSI and Coast Guard and others, but our ability to bring in inputs from other partners, from trusts through the private sector, to understand what companies are seeing, and to use all that and get it widely disseminated to protect others across the Government and the private sector in real time.

I feel that across the Government we are very much operational. We very much have turned a corner. If I could have one wish, it would be to have been able to act faster on Heartbleed, and that would have been for the statutory clarification so that we wouldn't have had to get letters of authorization for every unique organization that we scan.

RESOURCES NEEDED

Senator COATS. Well, you just began to answer my second question, and that was what resources do you need to get to the point where—I know it's a constantly evolving challenge here from a technological standpoint. But are there resources you need now that could accelerate the process of getting this whole domain in place relative to meeting all these strategies?

Dr. SCHNECK. There are always resources that we could use. So we have made, of course, cuts across all of our high-value programs and, unfortunately, even in education, given the budget picture we were given, to fit that. However, that statutory clarification would help us because it reduces the amount of time it takes us to act. It makes it very clear what our authorities are to help with the information-sharing across the private sector that narrowly targeted liability protection.

I came from industry 8 months ago and that's very helpful to a company because it speaks to the general counsel and says: This is okay to share with Government and protect others, and the company won't get hurt, the breach notification.

But this is the area on the congressional side. On the resource side, we do need more talented people and that means manufacturing them and training and educating them. I'm very, very passionate about that as well. I'm a product of that. And it also means the ability to hire people faster, on-board them with the competitiveness that some other agencies have, that we do not yet; and certainly to engage with the whole unity of effort with the DHS and put more money to this. If we didn't have to cut as much, we'd be able to grow a lot faster, and this is an urgent environment.

DATA BREACHES: GOVERNMENT, PRIVATE-SECTOR RESPONSIBILITIES

Senator COATS. I'm going to ask the second panel this also, but I'd just like to get your take. Relative to—there's been some very high-profile data breaches among retail sellers and the business community. Has that resulted in a significant uptick in terms of inquiries and outreach and willingness to be more engaged in partnership with the Federal Government that you've noticed as a result of those high-profile breaches?

Dr. SCHNECK. I would say absolutely. Number one, the American public is scared. And number two, I met even yesterday—I meet all the time with our sector representatives, our partners in the private sector. I met yesterday with some executives from the financial community, and they want to know how to help; they want to know how to contribute their resources and their knowledge. It's the same across all sectors.

So absolutely, this is the time to get this done.

Senator COATS. My time has expired. Madam Chairman, I just think that's so critical as we move forward, and to my other colleagues also. What we got hung up on before was the reluctance of the private sector to, quote, "trust" that they could coordinate with the Federal Government in a way that would protect their privacy and all that. Now they've seen, I think, the capabilities and the necessity of having that interaction between the Federal and the private sector. I'm glad to hear your answer on that one.

Senator LANDRIEU. Thank you, Senator Coats, for your leadership. You've been working with members of both sides and we think we're making progress, and thank you.

But I do want to come back after Senator Coons and ask you to restate the specific authorization that you lacked, that you said you were able to cobble together, but if you had the authorization, at least in dot-gov, you would have been able to move more quickly. I'll come back to you in just a minute.

Senator Coons.

Senator COONS. Thank you, Madam Chair.

Senator Coats, that is an area of interest for me as well, as a former in-house counsel for a private sector company that faced security challenges much like the ones you've described. I do think we still have undone work in terms of delivering clarity.

Let me focus on that first, if I might. Jurisdictional clarity seems to me particularly important for a cyber event because, unlike a natural disaster, a cyber event could be a crime, a national security event, an act of war. It could possibly be all three at the same time. And governmental objectives might be in conflict, one agency trying to restore power, for instance in an attack on the grid, while another agency is trying to preserve evidence needed to catch the perpetrators and investigate and prosecute the perpetrators.

I am concerned about whether we have clear protocols for industry and Government for that response and clear lines of responsibility so that we can do the restoration work that's needed, but without destroying the Government's capacity to investigate and prosecute. So I'd be interested in whether you feel you have the authority you need to do that today and whether we should be considering some legislation that clarifies Federal roles and responsibilities to grant authority for lead during a cyber attack.

I'm going to ask my questions first and then see if we've got enough time for an answer.

And then second, Dr. Schneck, I just wanted to commend you for your engagement with the workforce and your commitment to being a great role model and leader. I think we're going to hear in the second panel from the University of Maryland. They're doing great work in preparing the cyber workforce. The University of Delaware is also working, as are many other universities.

I do want to hear how you think targeted investments in cyber education are furthering national security and what more we need to do.

Last, the National Guard is a remarkable, nearly unique asset that crosses the civilian and military divides and allows us access for national security and homeland security purposes to a world-class workforce that is trained and funded by the private sector, but because of their either Guard or Reserve role can be accessed in times of emergency or on an ongoing basis. I wondered if you had any comment, Dr. Schneck, as to whether there are initiatives in place to enhance that relationship.

So there are three questions. And, Special Agent Noonan, if we have a moment to talk about IP theft and trade secrets theft in the finish, that would be great as well.

Please, Dr. Schneck.

Dr. SCHNECK. I'm going to talk very fast because my colleagues have very interesting work and I want you to hear that. So very quickly, statutory clarification. We currently have the authority. We work from a patchwork of different laws, including the Homeland Security Act of 2002, that tells us that our response is response and mitigation. That's our role—response and mitigation of cyber threats across Federal, civilian, government, State, local tribal, territorial, and critical infrastructure private sector.

The problem—and I knew this from the other side in the private sector—is that when the lawyers get involved, and to their credit they're protecting the company, and they don't really know if we're supposed to be scanning. This even happened with the Cabinet agencies that we had to scan for Heartbleed to ensure that our citizens who use external-facing Web sites, who use a highly credible piece of software called Open SSL that happened to have a defect—we didn't want them to get hurt.

So as fast as we could, we went door to door and got a letter of authorization from each agency, working with each lawyer, to make sure that we could scan it. That cost us 5 to 6 precious days in some cases, because the whole world knew about this vulnerability and all the information that it could capture while we were lawyering. So had we had the clarification in the law that this was our role, we would have gotten started a lot faster.

CYBER EDUCATION: TARGETED INVESTMENTS

On your second question, I'm happy to follow up after in writing. I just want to leave time for my colleagues. Targeted investments in cybersecurity. I am a big believer in innovation. It's not just that I worked for a Silicon Valley company. It's that my father was a scientist and I like to learn. If we can enable other students to have that and to take on cybersecurity as something that is fun, we get our national and our global leadership back as a country. You target that innovation.

I've spent a lot of time in Silicon Valley talking to venture capitalists and others about the importance of protecting your investment. But if we could target that toward the universities, target our research toward that, as we do with our partners in science and technology and R and D, if we could advance a lot of that, I think that we would move forward both as a country and in cybersecurity.

NATIONAL GUARD

Finally, on the National Guard, that's a DOD asset. However, we believe in collaboration, so we welcome that. As you and I talked before, homeland security is local; the response needs to be local. What we can add is the collaboration. Let them plug into the other areas, whether it's us or Secret Service or HSI or Coast Guard, the other responses. Let that be plug and play. Let us all work together. The added energy will do nothing but help us, and we can learn from them. So it's a welcome asset. It's not one we control, but it's certainly one that could fit right into our input of threat information and certainly those that we would output to and welcome to work with.

Senator LANDRIEU. Senator Coons, thank you so much. You and I think are co-sponsoring a bill related to the role of the National Guard, and I would describe the National Guard as well positioned to be of great help to our country in this particular line of defense, because they have the expertise of the military, but their base is homeland, and they draw from a wide variety of industry by their nature. It's part-time warrior. That is very interesting.

So I look forward, Senator Coons, to continuing to work with you on that possible enhanced partnership.

Senator Cochran.

STATEMENT OF SENATOR THAD COCHRAN

Senator COCHRAN. Madam Chair, I got in a little late, but I'm glad I was here to at least express the appreciation of this committee to our witnesses for helping us better understand what the limitations are and what the opportunities are that we have in Congress for making good quality decisions about Federal regulation, rules, laws, how do you protect privacy. Is there a privacy any more? I guess not.

So it's kind of scary. So you're all we've got. What I'm talking about is that the Federal Government's agencies aren't prepared to police the use of assets and equipment and knowledge and information, and would we want that anyway? These are all big questions, and we thank you very much for coming here and helping us understand that.

DATA BREACHES: DISCOVERY

Senator LANDRIEU. Senator Cochran, thank you for your leadership.

Let me ask, if you don't mind—and if you have an additional question, our time will allow it. The votes have been pushed back slightly.

But I do have a question for Mr. Noonan. One of the most poorly understood facts regarding data breaches is that it's rarely the victim company that first discovers the criminal, in the case that it is criminal—let's assume and I think, Senator Coons, it could be all the above—but a criminal unauthorized access to their networks. Rather, it's law enforcement, financial institutions, or third parties that identify and notify the victim company of the data breach.

Without going into any specifics, this speaks to the importance of timely and trusted information shared between law enforcement and the private sector. We've touched on this, but everyone is now aware, or most everyone, of the situation at Target and what happened when the third party, hired by Target, notified them their systems had been breached, what happened internally in Target. I think just this week someone has stepped aside, because that is still going on.

So could you explain right now in America, who is the one that normally finds out the breach has occurred? And it's usually not the victim, as in this case. It's usually who, a third party, an Internet provider, you guys, ICE, FBI, Secret Service? Who wants to take that?

Mr. NOONAN. Yes, ma'am. From the Secret Service's approach, we have a proactive approach to going after cyber criminals. It's generally a source of information that we're able to obtain, and we obtain it in a number of different ways, whether it's through confidential informants, other sources, undercover operations, or trusted partners within the industry.

We're able to take those data, we're able to crunch those data, and determine where there's a vulnerability and who potentially has been victimized. In many cases, in just this year, we've made notifications to actually two other financial institutions about their compromise. And I'm telling you that if it were not for that notification by law enforcement, the Secret Service, to those two financial institutions, they would not be in business today.

So when we talk about potential——

Senator LANDRIEU. Can you repeat that, please?

Mr. NOONAN. Yes, ma'am. We've made notification to two financial institutions in this year, at which time they didn't know that they had an intrusion. We believe that those institutions would have gone under if it were not for notification to those institutions. They did not lose a single dollar because of that advance warning.

Senator LANDRIEU. And if some of these institutions that would go, could potentially go under, are big enough, you could assume lots of other companies and individuals they could take down with them, correct?

Mr. NOONAN. Yes. The people who we're talking about the cyber criminals, the transnational cyber criminals who have the capability to do this, they're very advanced cyber criminals. They're going after financial institutions. Their motivation is greed. So whatever they can get their hands on to monetize in the criminal underground, that's what they're attacking.

In this particular case—I'm just giving you those two particular examples. There are many other examples. There are other retailers that we've made notification to this year as well that they had potential issues, and we were able to—and you've got to understand, that's an advantage because we're going out ahead of them losing anything and we're allowing them to see and look closer at their systems by information and evidence that we're learning in our other cases to say, "Hey, institution, you have a problem, please look in this arena."

That's where the advantage of law enforcement is in this fight against cyber crime. Law enforcement has a way to go outside the fence, if you will, to determine what the criminal actors are doing. We're able to look at their criminal network. We're able to look at their criminal infrastructure, and sometimes ahead of time determine what they're going to do or what actions they may take, and in doing so we do make notifications to those trusted partners.

Senator LANDRIEU. Does ICE want to have anything to answer or comment on, Mr. Edge?

Mr. EDGE. With regard to the intrusions that we're discussing here, we don't duplicate the efforts that the Secret Service initiates. In fact, if we were to discover such an intrusion, we would contact our counterparts at Secret Service and work with them on the investigative effort that would take place.

We also would assist in the computer forensics analytic portion of it as well. So it's a total team effort here. Most of the work that we're doing in the cyber space is pursuant to the investigative areas in which we work—child exploitation, counterproliferation—where we work very closely with DOD and we communicate very closely with DOD and try to disrupt and dismantle those organizations that are off of our shores, where we can certainly make a difference and prevent them from continuing to affect our country.

Senator LANDRIEU. Okay, thank you all.

I think we're going to move to our second panel. I just want to underscore one additional item. To you, Dr. Schneck: I know that you're aware of the extraordinary contribution Louisiana Tech has played in developing an education program for middle and high schools, also with their college level as well. We were one of the universities that received one of the first grants in the country, and I look forward to continuing to work with you on developing and network of universities and programs that are actually meeting the need that's been expressed.

I thank you, Mr. Edge, for recognizing the HERO Child Rescue Corps Program, very innovative, that U.S. Immigration and Customs is working with Special Operations to use wounded warriors while they are convalescing and are unable to perform their primary function. They're well trained and suited to be warriors on the Internet, and I really think that's using our assets really well and I look forward to continuing to support that effort.

I thank you all and we'll move to our second panel.

NONDEPARTMENTAL WITNESSES

Senator LANDRIEU. As the panel is getting situated and the Clerk is helping to seat them, I wanted to let the members know that Senator Coats and I thought it would be a good idea to have some independent voices at the table to give some critique and some different perspective to the Government agencies and entities. We really want to know if our agencies and entities that we're funding are doing the kind of job that you as experts in the field believe they should be doing.

We know that sometimes you work with these agencies, so sometimes it is difficult to criticize them. But we hope that you will do it constructively, and we hope that you will do so. We want to know what's working in your view, what's not working, what progress we're making in these fields, and what we're not.

We've got I think a very excellent panel. First we have Mr. Mahon, vice president and chief security officer of CenturyLink. I think it's the third largest Internet provider in the country, and I'm very proud that it actually is located in Monroe, Louisiana, and is growing. It started out as a very small telephone company maybe 45, 50 years ago with a handful of employees and now it's multithousands and just really an extraordinary success story.

Scott Bowers, vice president, government relations, Indiana Statewide Rural Electric. Scott, welcome. Mr. Bowers, welcome, and we look forward to hearing from you representing the hundreds and thousands of coops in this country that are part of this effort.

Christopher Peters, vice president of North American Electric Reliability Corporation (NERC)-Critical Infrastructure Protection Compliance, Entergy Corporation. Then I think we have Dr. Katz from UMD Cybersecurity Center. Thank you all very much.

Why don't we start with you, Mr. Mahon, with CenturyLink. But, Dan, did you want to say anything particularly about your witness?

Senator COATS. Well, you talked about his credentials. Scott is just someone that comes from the private sector, but clearly part of the private sector that deals with critical infrastructure. We have these coops all over the United States, as you know. I'm sure you have many in Louisiana. We talk about Duke Energy and we talk about AEP and so forth and so on, but in reaching out to particularly smaller town America and rural America, these coops are absolutely essential, and they're very much part of the grid.

So we need to not only be thinking of the big guys, but also the little guys. That applies on the retail side and the commercial side also. We read about Neiman Marcus and Target and so forth. There are thousands, of not hundreds of thousands, of smaller businesses out there that are providing very necessary services and they are also vulnerable to these kind of intrusions.

So I want to make sure that we cover the whole gamut and not just focus on the people at the top.

Senator LANDRIEU. Thank you so much.

We'll start with CenturyLink.

STATEMENT OF R. DAVID MAHON, VICE PRESIDENT AND CHIEF SECURITY OFFICER, CENTURYLINK

Mr. MAHON. Thank you, Chairman Landrieu, Ranking Member Coats——

Senator LANDRIEU. You have to lean into the microphone and push it right close to you. There you go.

Mr. MAHON. Chairman Landrieu, Ranking Member Coats, and Senator Cochran, thank you for this opportunity to testify before you today.

My way of background, CenturyLink has grown through acquisition and innovation over the course of their history and today is a commercial entity with $18.3 billion in revenue, 13 million customers, 47,000 employees. We are a tier one backbone provider and we have 55 data centers around the world.

It's within this context that I would like to speak to you about cybersecurity risks, and I would like to talk to you in three specific areas. First is the adversary; second, DHS programs that have been successful; and third, developing the next generation workforce.

If I can leave you with one thing today, what I would like to tell you is: Do not think about cybersecurity risks within the context of malware, viruses, or other tactics. What I would ask you to think about is the adversary, the people behind the computers that are breaching our networks and stealing our data.

The CenturyLink security team divides these groups into five very specific areas: nation-state-sponsored; criminal enterprises; hactivists; terrorists and sabotage; as well as the insider threat. It's important to understand this within the context of their objectives and their tactics. Each can vary very differently.

For example, a criminal enterprise that is interested in stealing credit cards will attack point of sale systems with a particular type of malware. That is quite different to defending against a nation-state that is interested in stealing intellectual property, maybe about a smartphone operating system.

The reason that this is important is we at CenturyLink are tasked with protecting our network, our data, and our customers from all of these adversaries, and each one is very different and we require very specific information to develop our protections and countermeasures. What has happened is the context in which we conduct our risk assessments allows us to access open source information to better inform our risk assessments, to help us deploy our capital as we expand and protect our network. But our risk assessments are only as good as the information that is available to us.

The Federal Government is in possession of very sensitive and frequently classified information that could be very helpful to us in our risk assessments as we defend against these bad actors. Two of the programs that at the Department of Homeland Security I feel have become very successful are the Enhanced Cybersecurity Services (ECS) program and the Einstein 3A (E3A) program. In each of these programs DHS came together with corporate America and resolved the traditional hurdles that one encounters, whether they be legal, technical, operational, and most importantly, cultural.

It became very difficult in the early days of developing information-sharing programs to acquire information from the Federal Government because of the context or the fear that they had that corporate America would not be able to protect classified information. On the corporate side, there's always the concern that if we discuss our vulnerabilities with the Federal Government there would be some type of regulatory response to our answers.

Therefore, I believe the value of ECS and E3A has been to bring together the private industry and the Department of Homeland Security and the representative agencies within the Department of Homeland Security to effectively begin to combat cyber crime. I do believe it has to go much further. There is additional information that the Federal Government frequently has around the strategy of these organizations, these nation-states, and even independent actors, that would be very helpful to know if we are going to better protect our networks, our data, and our customers.

Regarding the next generation cyber workforce professionals, I believe it is very important to encourage the Department of Homeland Security to begin with the K–12 educational programs that you may have heard about throughout the country in various capacities. But specifically the STEM programs and other technical programs that first generate the interest is what we need. I think CenturyLink, Louisiana Tech, and the Cyber Innovation Center in Bossier City have become an example of what we can do to better protect the corporate infrastructures as well as the Government infrastructures.

I thank you for your determination to lead DHS in its mission and we look forward to supporting you. Thank you.

[The statement follows:]

Prepared Statement of R. David Mahon

Chairwoman Landrieu, Ranking Member Coats and members of the committee, thank you for the opportunity to testify today on an issue that is of critical importance to national security, the U.S. economy and homeland security. CenturyLink appreciates the leadership role the Department of Homeland Security plays in facilitating the cybersecurity of the nation's critical infrastructure, with the oversight and guidance of this Committee. In today's testimony, I would like to cover three key areas where the fiscal year 2015 budget offers worthwhile opportunities to strengthen the nation's cyber defenses:

—Further improving the quality of public-private information sharing related to cybersecurity;

—Leveraging classified cyber threat information to protect critical infrastructure and the networks of Federal, State and local governments through the Einstein 3 Accelerated and Enhanced Cybersecurity Service programs; and

—Investing in our cybersecurity workforce.

CenturyLink was founded nearly 85 years ago as a small rural telephone company with just 75 paid subscribers and a manual switch in the front parlor of the Williams family home in Oak Ridge, Louisiana. Our recent and rapid evolution through acquisition and innovation to become an $18.3 billion communications, data and cloud company with 47,000 employees, 13 million customers, a Tier 1 Internet backbone, and 55 data centers around the world makes us a prime example of how technology and communications infrastructure are driving our economy.

Effective cybersecurity is now central to everything we do, not only as a provider, but also as a customer of others. That includes our residential and enterprise broadband service, the secure communications services we provide to the Department of Defense, U.S. embassies and Federal Communications Commission, our cloud computing platforms, and the managed security services we provide to critical infrastructure owners.

As the company has grown, we've benefited from excellent State and local support, enabling us to cultivate talent in northern Louisiana and the many local markets we serve in almost every State. This includes developing partnerships with the University of Louisiana—Monroe (ULM), Louisiana Tech University, the Cyber Innovation Center in Bossier City and other institutions. In fact, we are nearing completion of a 250,000-square-foot Technology Center of Excellence on our Monroe headquarters campus that will house an additional 800 innovation professionals devoted to network monitoring, research and development, as well as IT and engineering support to our international service footprint.

In addition to our company-specific cybersecurity and risk management programs, CenturyLink has had a productive experience participating in the public-private partnerships established to share information and work collaboratively on industry-wide security challenges. Our executives serve on the President's National Security Telecommunications Advisory Committee (NSTAC), the Communications Sector Coordinating Council (CSCC), the Communications Information Sharing and Analysis Center (ISAC), and the FCC's Communications Security, Reliability and Interoperability Council (CSRIC), among others. Through these efforts, we supported DHS in the creation of the National Cybersecurity and Communications Integration Center (NCCIC) and CenturyLink maintains a permanent presence on the NCCIC floor.

We support the voluntary, industry-led approach to protecting the security of critical infrastructure networks operated by the private sector, and appreciate the work the National Institute of Standards and Technology (NIST) has undertaken to create the Cybersecurity Framework, as well as DHS's Critical Infrastructure Cyber Community (C^3) Voluntary Program to educate stakeholders and promote the framework's use. CenturyLink has found the Framework useful in affirming many of the practices that we and other larger carriers already had in place. We are also using the Framework as a tool to help our enterprise clients assess their own threat level and implement risk-based cybersecurity protections.

THE CYBERSECURITY THREAT AND INFORMATION SHARING

If I could leave the Committee with one thought about cybersecurity risks, it is this: Don't limit your thinking to only addressing the issues of malware, viruses, denial of service attacks, social engineering, botnets or any of the other tactics used. Instead, think of cybersecurity in terms of the adversaries—the people on the other side of the computer, wherever they may be, who conceive and execute the breaches.

Especially where critical infrastructure is concerned, our adversaries are constantly studying their targets, probing networks, paying attention to the defenses we put up, and searching for the weakest link in the chain—even tracking Federal efforts to promote security. Whether it's hacking the Web site of a technical conference so targeted employees will download malware when they register, or using the compromised systems of an HVAC contractor as an attack vector, they are adaptable. This makes the threat more formidable, but also offers a clue about how to build our cyber defenses.

As a general matter, CenturyLink's security team divides cyber threats into several key groups, each with varying levels of sophistication:

—*Nation-State-Sponsored.*—Which are often the most sophisticated, and generally motivated by economic and political espionage. Combating government-sponsored adversaries requires an advanced information security program. These data breaches can go completely undetected by the victim organization.

—*Criminal Activity, Including Organized Crime.*—These attacks have a wide range of sophistication, and are generally focused on capturing information that can be monetized.

—*Terrorism and Sabotage.*—These are most concerned with doing damage, including physical damage, to the target entities.

—*Hacktivism.*—Generally less sophisticated, these groups will use "soft targets" with less sophisticated information security practices to garner publicity and make their political points.

—*Insider Threats.*—These can be the toughest to guard against because they are "inside the perimeter" of the target itself.

Adversaries tend to cluster around an industry sector, based on the goals they want to achieve. For example, a criminal cartel that wants to exploit consumer credit card information will, perhaps, stand up a network of infected computers and launch a particular type of attack on point-of-sale systems across numerous retailers, using similar malware, attack vectors and tactics for covering their tracks. But a nation-state that wants to exfiltrate confidential technical specs about a smartphone operating system will use a completely different strategy. Especially for the more sophisticated adversaries, the best long-run defense is to build closely coordinated defensive alliances around the targeted industries and our partners in government, and to study our adversaries as closely as they study us.

To draw an analogy, the cat-and-mouse nature of cybersecurity resembles offensive and defensive schemes in the National Football League. Every season, coaches devise new "attacks" to move the ball down the field, whether it's the old "west coast offense" or last year's "read option." If they're successful, defenses that rely on the comfort of understanding past, predictable plays won't be prepared to stop them, at least for a while. But the minute a new offensive scheme succeeds, every defensive coordinator in the league starts working on countermeasures to shut it down. And while the short-term countermeasure might be a zone blitz or a few tough hits on the quarterback, the long-term solution has everything to do with continually studying the game tapes and evolving the defense.

In the world of cybersecurity, we don't have the luxury of watching the "game" every Sunday, but the never-ending need to study the opposition and update defenses is the same. For DHS and the nation's critical infrastructure providers, this means continuously refining the information sharing relationships to get actionable, tailored information to the targeted sectors in as close to real time as possible. This will ultimately lead to automating the information sharing mechanisms that will allow a targeted entity to use the cyber threat information to defend itself without compromising the sources and methods of the information provider. This is as much a cultural challenge as it is a technical one, because the information at issue is so sensitive and the teams are not accustomed to sharing their proverbial playbooks.

In our experience, the DHS leaders are fully aware of the challenge and committed to strengthening the partnerships, but doing so is often an iterative, painstaking process that involves continuously building trust, sophistication and technological capabilities, and we appreciate the Committee's continued support for that mission. In the words of Bear Bryant, "defense wins championships."

ENHANCED CYBERSECURITY SERVICES (ECS) AND EINSTEIN 3 ACCELERATED (E3A)

One of the most critical roles the Department of Homeland Security can play is to leverage the classified cyber threat indicators the Federal Government gathers through law enforcement, intelligence collection and other Government-specific functions to protect private sector critical infrastructure and government networks. This is no small task because the cyber indicators themselves must be protected from our adversaries in an end-to-end secure environment and put to use in the field without compromising the sources and methods that yielded them in the first pace. To do this, DHS has developed two programs:

—Enhanced Cybersecurity Services (ECS) for private sector critical infrastructure providers as well as State and local governments, and

—Einstein 3 Accelerated (E3A) for Federal civilian networks.

With both programs, Internet service providers like CenturyLink, under the direction of DHS personnel, administer intrusion prevention and threat-based protections on traffic entering and leaving the networks of participating organizations. Participation is voluntary, and non-Federal participants in ECS must first be validated by DHS, but those who do participate receive an elevated level of protection from the most sophisticated cyber intruders.

CenturyLink has worked extensively with the Federal Government to develop these programs, and provide important protections against the most advanced threats while educating the Government on practical aspects of providing such services to private industry. Expanding the scale and automating the information gleaned within "circles of trust" is the next critical step in providing effective and time critical cybersecurity protections to Government and critical infrastructure providers.

State and local governments administer many functions that are important to public safety and the protection of critical infrastructure, however, they continue to lag in funding mechanisms. DHS has taken the lead to fill this gap temporarily in their support for MS–ISAC services, but additional funding for additional services such as ECS would help State governments avoid becoming the "weak link" with their Federal partners.

DEVELOPING THE CYBERSECURITY WORKFORCE

CenturyLink appreciates the Department of Homeland Security's leadership on developing the nation's cybersecurity workforce, including its support for teacher training and university research and curriculum development in Louisiana. Especially in the last year, CenturyLink has focused on developing and attracting a broad range of innovation professionals, including engineers, senior IT personnel, product managers, researchers and others to help staff our Technology Center of Excellence, which will open early next year.

Our headquarters are located along the I–20 Corridor that spans northern Louisiana and is home to a number of innovation hubs, including the National Center for Academic in Information Assurance Education at Louisiana Tech University, the Cyber Information Technology program at Bossier Parish Community College, and the Cyber Innovation Center, a research park and nonprofit organization devoted to building the knowledge-based workforce in the region. Computer Sciences Corporation recently announced plans to bring 800 new jobs to the Cyber Innovation Center, and we are hopeful that as businesses step up investment in the region, we can work together to cultivate a world class cyber workforce. We would encourage this Committee and DHS to place a renewed emphasis on workforce development in the cyber arena by addressing the potential shortage of qualified and skilled employees that will be needed.

We also support the National Integrated Cyber Education Research Center (NICERC) at the Cyber Innovation Center, which focuses on curriculum design, professional development, and collaboration in K–12 and college education. NICERC has organized programs to give teachers the training and tools to prepare students for a career in cybersecurity, including problem-solving, critical thinking and communication skills. Of special note, NICERC is the lead technical institution for DHS's Cybersecurity Education and Training Assistance Program (CETAP)—so the teacher-focused cybersecurity education model first developed and implemented by NICERC in Louisiana can benefit school districts across the nation.

CONCLUSION

While the challenge of building a cyber workforce and protecting the nation's critical infrastructure from growing threats is a daunting and multifaceted one, we are encouraged by the commitment of the White House, DHS and this Committee to bring the right resources to bear. We appreciate the determination and attention that Chairwoman Landrieu and the committee members have brought to the issue and look forward to working with you and the authorizing committees as you support and guide DHS in its mission.

Senator LANDRIEU. Thank you very much.

Let's go to you now, Dr. Katz, from the University of Maryland, that's played quite a leadership role in all of this.

STATEMENT OF DR. JONATHAN KATZ, PH.D., DIRECTOR, MARYLAND CYBERSECURITY CENTER, UNIVERSITY OF MARYLAND

Dr. KATZ. Chairman Landrieu, Ranking Member Coats, Senator Cochran: I'm going to talk about workforce development and specifically efforts under way within the University System of Maryland. Developing an adequately prepared cybersecurity workforce is a daunting challenge. Put simply, demand is far outstripping supply. Actually, a great statistic came up earlier with mention of the need to educate 200,000 cyber professionals each year.

Now, a critical question is what is meant by cybersecurity education. From my point of view and broadly speaking, there are really two aspects to be considered here. The first is a general cybersecurity education, not just for computer and technical students, but for everyone. The same way people come in and take English comp or introductory math courses, college students need to be exposed to the basics of cybersecurity and good cyber hygiene.

Second, of course, is to grow a dedicated cybersecurity workforce, professionals that have deep technical knowledge, as well as those with the technical knowledge in core computer science and electrical engineering skills, but also with expertise in the, quote unquote, "softer" areas like economics, policy, and psychology.

I think it's important to keep this in mind when we're talking about numbers of cybersecurity professionals needed, to keep clear that not every cyber professional is going to be the same and not everyone is going to need the exact same background in cybersecurity courses.

Now, the University System of Maryland (USM) has a number of programs in place to augment the existing pipeline of future cybersecurity professionals. University of Maryland institutions are playing their part by not only training dedicated cybersecurity professionals, but also educating the general public on good cybersecurity practices and policies. I'll just mention a few key ways in which USM institutions are helping to combat the shortage in our Nation's cybersecurity workforce. I'll only be able to touch on a few here.

USM institutions awarded approximately 4,400 cybersecurity-related degrees in the 2012–2013 academic year. Four USM institutions are NSA and DHS centers of academic excellence in information assurance education. UMD College Park, with support from Northrop Grumman, launched the Advanced Cybersecurity Experience for Students, or ACES, in 2013. This is the Nation's first undergraduate honors program in cybersecurity and really I think serves as a paragon of the way undergraduate cybersecurity education should be done.

University of Maryland Baltimore County, the Center for Cybersecurity Training, offers numerous courses for skill enhancement and certification opportunities for active professionals. And the University of Maryland College Park is going to be offering a series of online courses on cybersecurity beginning in the fall, again as a way to reach out to the broader public.

In addition to these educational offerings, USM institutions also perform outreach to the wider public to spark interest in the field and to try to grow a pipeline of future cybersecurity professionals. Some examples here include cybersecurity camps for middle school girls and high school students, as well as summer camps for high school STEM teachers, held as part of the DHS-funded cybersecurity education and training assistance program.

Our educational opportunities cannot be created or refined in isolation. USM has numerous cybersecurity programs that are developed with input from industry and Government sources. Sharing information about current workforce knowledge gaps and how best to address them is one of the many ways that USM institutions benefit from our interactions with private industry and the Federal Government.

However, as educators we not only train students in the problems of today, but must also ensure that they can master key fundamentals that will provide the foundation for understanding and remediating the cybersecurity threats of tomorrow.

Federal and private support to continue to grow the future cybersecurity workforce is essential to closing the demand gap for those professionals. Continued or perhaps expanded investment from Federal agencies like the Department of Homeland Security, the National Science Foundation, and the National Security Agency, for example, is critical to sustaining the progress that we've already been making.

Thank you for the opportunity to appear before the subcommittee and I look forward to answering your questions.

[The statement follows:]

Prepared Statement of Dr. Jonathan Katz

Chairman Landrieu, Ranking Member Coats: Thank you for the invitation, and the opportunity to speak to the subcommittee. It is an honor to be here.

As the committee has previously noted, we are continually faced with numerous cybersecurity threats. These threats are not static—in fact, the sophistication of attacks cybersecurity seems to change on a daily basis. New vulnerabilities are uncovered, different attack vectors are employed to exploit a system or a program, and patches for critical operating systems are deployed on a near-constant basis. As director of the Maryland Cybersecurity Center (MC2), I am extremely familiar with the rapidity with which cybersecurity threats continue to evolve, and the challenges that these threats present to the Federal Government, the private sector, and our Nation's academic institutions.

Developing an adequately prepared cybersecurity workforce is a daunting challenge. Put simply, demand for talented cybersecurity professionals is far outpacing the supply. A 2013 (ISC)^2 Global Information Security Workforce Study claims that 56 percent of companies nationwide report a workforce shortage. Maryland alone had more than 18,000 vacancies for cybersecurity jobs, according to a recent Abell Foundation report. And Federal agencies are having difficulty filling cybersecurity roles as well, something highlighted in 2008 and 2010 by the CSIS Commission on Cybersecurity for the 44th Presidency.

The University System of Maryland (USM), which includes 12 campuses, has a number of programs in place to augment the existing pipeline of future cybersecurity professionals. Maryland institutions are playing their part by not only training dedicated cybersecurity professionals, but also educating the general public on good cybersecurity practices and policies.

Below are some key ways in which USM institutions are helping to combat the shortage in our Nation's cybersecurity workforce:

—USM institutions offer a broad range of degrees in cybersecurity-related fields, and approximately 4,400 cybersecurity-related degrees (BS, MS, and PhD combined) were awarded in the 2012–2013 academic year.

—Four USM institutions (UMD, UMUC, UMBC, and Bowie State) are NSA and DHS Centers of Academic Excellence in Information Assurance Education.

—UMD College Park, with support from Northrop Grumman, launched the Advanced Cybersecurity Experience for Students (ACES) in 2013. This is the Nation's first undergraduate honors program in cybersecurity.

—UMBC's Center for Cybersecurity Training offers numerous courses for skill enhancement and certification opportunities.

—Multiple USM campuses offer MS programs in cybersecurity, cyber policy, and/or digital forensics.

In addition to our current educational offerings, USM institutions also perform outreach to the general public to spark interest in the field and communicate cybersecurity best practices. Examples include:

—Cybersecurity camps for middle-school girls and high-school students at UMCP.

—Summer camps for high-school STEM teachers held at UB as part of the DHS-funded Cybersecurity Education and Training Program.

—"Tech talks" given by undergraduate cybersecurity-club members to the broader undergraduate student body.

Educational opportunities cannot be created or refined in isolation. USM has numerous cybersecurity programs that are developed with input from industry and government sources. Sharing information about current workforce knowledge gaps, and how to best address them, is one of the many ways that USM institutions benefit from our sustained and regular interactions with private industry and the Federal Government. However, as educators, we must not only train students in the problems of today, but must also ensure that they master key fundamentals that will provide the foundation for understanding and remediating cybersecurity threats of tomorrow.

Federal and private support to continue to grow the future cybersecurity workforce is essential to closing the "demand gap" for those professionals. Continued—and perhaps expanded—investment from Federal agencies, like the Department of Homeland Security, the National Science Foundation, and the National Security Agency, for example, is critical to sustaining the progress that has already been made.

Again, thank you for the opportunity to appear before the subcommittee. I look forward to answering your questions.

Senator LANDRIEU. Thank you very much.

Mr. Bowers.

STATEMENT OF SCOTT R. BOWERS, VICE PRESIDENT OF GOVERNMENT RELATIONS, INDIANA STATEWIDE ASSOCIATION OF RURAL

ELECTRIC COOPERATIVES

Mr. BOWERS. Madam Chair, Senator Coats: Thank you for the opportunity to address you regarding cybersecurity. I'm here on behalf of Indiana Electric Cooperatives (IEC). Currently, IEC represents 39 electric distribution cooperatives that serve over 1.3 million Hoosiers in 89 of the State's 92 counties. Collectively, our member cooperatives employ more than 1,500 individuals and represent the second largest electric provider in Indiana.

Indiana's electric cooperatives recognize your concerns related to cybersecurity. We have taken steps, often independent of Government regulation, to provide the security and reliability required for our consumers. Due to our construct and the areas we serve, most people do not recognize the leadership role electric cooperative assumed, specifically in the areas of renewable energy sources, energy efficiency, and cybersecurity.

Our 39 distribution cooperatives generally do not own bulk electric system assets. Therefore they focus largely on the reliability and security of their distribution systems, protecting member data, and their data business systems where data is processed and stored.

IEC also represents two generation and transmission cooperatives, or G&Ts, Hoover Energy Rural Electric Cooperative and Wabash Valley Power Association. Both are fully integrated on the NERC compliance registry by applicable function. As such, each G&T is required to comply with approved reliability standards related to cybersecurity, operations, and system reliability.

Today I'd like to specifically recognize the cybersecurity efforts of our two G&Ts. Hoosier Energy maintains a thorough cybersecurity program that protects facilities critical to the reliability of the bulk electric system against a myriad of vulnerabilities. Most notably, Hoosier Energy developed an in-house scanning utility called the Windows Configuration Management Utility (WinCMU) that gives Hoosier Energy complete visibility into its systems and reports any unexpected changes to its security team.

Knowing what is on a system is the most important step in maintaining a secure environment. During a recent audit by NERC, auditors acknowledge this and praised WinCMU and Hoosier Energy for going above and beyond the requirements in NERC's cybersecurity standards. Compliance with these standards is enforced by NERC and the Federal Energy Regulatory Commission (FERC).

In addition to complying with such standards, Hoosier Energy's cybersecurity program mitigates and protects against a wide range of vulnerabilities, including: one, ignorance, indifference, and lack of knowledge of cyber threat protection; two, information exfiltration; three, network-based cyber attacks; four, unmanaged changes to cyber assets and protective systems; and five, direct attacks on cyber assets.

Wabash Valley, IEC's second G&T, has a strong cybersecurity program in place as well. Wabash Valley firmly believes it takes every employee being vigilant to ensure the safety of their people and their assets. Relative to cybersecurity standards, Wabash Valley awaits the implementation of NERC's updated Critical Infrastructure Protection (CIP) Standards Version 5. Wabash Valley worked proactively to develop its cybersecurity plan although it was not required by previous versions of the standards.

Additionally, Wabash Valley engaged an external consultant to assess its CIP program and systems. The consultant determined Wabash Valley's CIP program was thorough and indicated that no changes to its systems were required.

Under previous NERC reporting standards, Wabash Valley established reporting relationships with FBI offices in the four States where it has member cooperatives or facilities. Although no longer required, Wabash Valley continues to keep the FBI or the Joint Terrorism Task Force in the reporting chain for cybersecurity events.

Last, Wabash Valley has established procedures in place for NERC alert system and energy sector ISAC-provided communications and alerts. These communications are reviewed by compliance and technical service personnel to assess a potential threat to the G&T. If applicable, systems are reviewed and, as appropriate, preventive actions implemented.

Moving forward, IEC sees several actions and opportunities where additional focus and improvement benefit access to power. Those include: continued improvement in information-sharing to ensure timeliness and actionability to cyber threats; expanding the number of clearances permitted for cooperative staff and allowing for top secret clearance for select senior-level executive staff; avoiding one size fits all solutions, while also encouraging flexibility; encouraging the continuation and creation of additional partnership opportunities; and improving consistency with the Federal standards application and compliance process.

In closing, IEC believe we are on a good path, but opportunities to improve still exist. Each of us, not just the respective Federal agencies, must assume our individual responsibilities to work constructively, effectively, and, most importantly, in partnership to address both current and future cyber-related threats to the reliability and security of our Nation's electric grid.

Thank you.

[The statement follows:]

PREPARED STATEMENT OF SCOTT R. BOWERS

Indiana Electric Cooperatives (IEC), the Nation's first electric cooperative service organization, represents 39 electric distribution cooperatives that serve over 1.3 million Hoosiers in 89 of the State's 92 counties. Collectively, our members employ more than 1,500 individuals and represent the second-largest electric power provider in Indiana. We serve a diverse expanse of Indiana communities, from rural and farming areas, industrial parks and employment zones to burgeoning suburbs. IEC appreciates the opportunity to provide the following testimony before the Senate Appropriations Homeland Security Subcommittee regarding "Investing in Cybersecurity: Understanding Risks and Building Capabilities for the Future."

Indiana's electric cooperatives played a foundational role in delivering electricity to communities across Indiana 80 years ago. Today, we fuel progress by delivering more than electricity to the communities we serve. We contribute to economic development, community development and youth and education programs across Indiana.

We continue to deliver safe, secure, reliable and affordable electric power across the State, including hard-to-reach rural areas. These same electric cooperatives are at the forefront in the promotion of renewable energy sources, energy efficiency programs and technology, ensuring electric power sources for future generations.

INTRODUCTION

IEC recognizes your concerns related to the issue of cybersecurity. We have taken steps, sometimes independent of government regulation, to provide the security and reliability required and necessary for our consumers. Due to our construct and the areas we generally serve, most people do not recognize the leadership role electric cooperatives have assumed—specifically in the areas of renewable energy sources, energy efficiency and cybersecurity.

IEC has two generation and transmission cooperative (G&Ts) members, Hoosier Energy Rural Electric Cooperative (Hoosier Energy) and Wabash Valley Power Association (Wabash Valley), who provide Indiana distribution cooperatives with wholesale electric power from coal, natural gas and renewable energy sources. Both G&Ts are fully integrated and registered on the North American Electric Reliability Corporation (NERC) Compliance Registry by applicable function. As such, each of Indiana's G&T cooperatives are required to comply with approved Reliability Standards related to cybersecurity, operations and system reliability.

Our 39 distribution cooperatives generally do not own Bulk Electric System (BES) assets. Therefore, they focus largely on the reliability and security of their distribution systems, which brings electricity to homes and businesses, protecting member data and their business systems where the data is processed and stored.

This afternoon, I would like to specifically recognize the cybersecurity efforts of our two G&Ts. I will start by discussing Hoosier Energy's efforts to address the cybersecurity threat.

HOOSIER ENERGY

Hoosier Energy maintains a thorough cybersecurity program that protects facilities that are critical to the reliability of the BES against a myriad of cyber vulnerabilities. Most notably, Hoosier Energy developed an in-house scanning utility called the Windows Configuration Management Utility (WinCMU) which gives Hoosier Energy complete visibility into its systems and reports any unexpected changes to its security team. Knowing what is on a system is the most important step in maintaining a secure environment. During a recent audit by NERC, auditors acknowledged this and praised WinCMU and Hoosier Energy for going above and beyond the requirements in NERC's cybersecurity standards. Compliance with these standards is enforced by NERC and the Federal Energy Regulatory Commission (FERC).

In addition to complying with such standards, Hoosier Energy's cybersecurity program mitigates and protects against a wide range of vulnerabilities including:

—Ignorance, Indifference and Lack of Knowledge of Cyber Threat Protection;
—Information Exfiltration;
—Network Based Cyber Attacks;
—Unmanaged Changes to Cyber Assets and Protective Systems;
—Direct Attack on Cyber Assets; and
—Physical Attack on Cyber Assets.

(See Appendix A for description of these vulnerabilities.)

IEC's other G&T, Wabash Valley, also has a cybersecurity program which includes some similar elements to Hoosier Energy's program. Next, I would like to highlight Wabash Valley's efforts to address the issue of cybersecurity.

WABASH VALLEY

The protection of people and assets are top priorities for Wabash Valley. As technology continues to evolve, cybersecurity threats become more advanced and increasingly difficult to detect and prevent. Wabash Valley firmly believes it takes every employee being vigilant to ensure their personal safety and the safety of Wabash Valley's assets (both physical safety and cybersecurity).

Relative to cybersecurity standards, Wabash Valley, along with other small entities, awaits the implementation of NERC's Critical Infrastructure Protection (CIP) standards, Version 5 (cybersecurity standards). Although not required by previous versions of the CIP standards, Wabash Valley has already developed a cybersecurity plan. In addition, an external consultant was hired by Wabash Valley to perform an assessment on its CIP program and systems. The consultant determined its CIP program was thorough for a small entity and that no changes to systems were required at that point in time.

Under NERC's event reporting standards, applicable entities were required to establish a reporting relationship with the Federal Bureau of Investigation (FBI). Wabash Valley established reporting relationships with FBI offices in all States and cities where it has member cooperatives or plant facilities (Indiana, Ohio, Illinois and Missouri). Although direct reporting of events to the FBI is no longer required by the NERC standard, Wabash Valley feels it is important to continue to keep the FBI or the Joint Terrorism Task Force (JTTF) in the reporting chain for cybersecurity (and other) events. Wabash Valley is part of the FBI's Strategic Partnership with businesses. As such, Wabash Valley receives regular bulletins and communications from the FBI to keep them informed about various situations/threats that could affect the safety and security of company assets and/or personnel.

Through the NERC Alert System and the Electric Sector Information Sharing and Analysis Center (ES–ISAC) housed within NERC, communications and alerts related to various potential threats are provided to our industry. It is part of Wabash Valley's established procedures for these communications to be reviewed by compliance and technical services personnel to assess a potential threat to the G&T. If the threat has potential applicability to Wabash Valley, then systems are reviewed and, as appropriate, preventive actions implemented. If the threat, such as HEARTBLEED, has potential impact for company employees on their computer systems at home, information is communicated to Wabash Valley employees. On a regular basis, the Wabash Valley security officer emails pertinent security topics to staff.

Wabash Valley welcomes the finalization of the cyber and physical security standards in the near future. In the meantime, they will continue to seek proactive measures to ensure the security of all G&T personnel and assets.

So where do we go from here? Beyond just the updating of the CIP standards, there are other actions that can assist us, the owners and operators, in assuring access to power. In talking with both our G&Ts, they shared concerns regarding some areas where they see opportunity for improvement.

INFORMATION SHARING

While we recognize and appreciate that improvement has been made by the Federal Government in the flow and sharing of cyber and physical security related information over time, the need for continued improvement still exists. Our ability to receive timely and actionable information remains a work in progress. The media remains our primary source of threat-related information. By the time information is shared with us from the Federal agencies, it can be too late for us to address the threat. Under our current situation, the damage is already done and we have moved into mitigation mode if we were impacted by the threat. Improving the timeliness of the threat communication would also better position us to take preventive actions on the front end in hopes to fend off or, if penetrated, minimize the impact to our system.

Additionally, expanding the number of "secret" clearances permitted for cooperative staff and allowing for "top secret" clearance for select senior-level executive staff would also be beneficial. This adjustment in security clearance procedures, along with liability protections for information sharing with the Government, would allow for more real-time and actionable information to be shared.

FLEXIBILITY

IEC would strongly encourage Congress and the Federal agencies to avoid enacting "one-size-fits-all" solutions for cyber and physical security. Our member cooperatives share a common mission, core principles and similarities in structure, but they are each independent and unique in the tactics, processes and protocols they utilize to serve their members. By affording Indiana's electric cooperatives that flexibility, each of our member cooperatives would be positioned to deploy the measures, technologies and systems that best fit their operations, assets and efforts to combat cyber and physical threats. In addition, each cooperative would be able to account for implementation costs, which helps maintain affordability, without compromising the security measures.

PARTNERSHIPS

Partnerships have been one of the most beneficial and productive tools used by Indiana's electric cooperatives in addressing the cybersecurity issue. The partnerships that have been most successful for us have generally been cooperative to cooperative based. Indiana's electric cooperatives have also benefited from their relationships with other private organizations, i.e. ACES, through their interactions with their Regional Transmission Organizations (RTO) as well as our national association, the National Rural Electric Cooperative Association (NRECA). While electric cooperatives were born with the assistance of the Federal Government in the 1930s, our approach has generally been to work within the cooperative community or the private sector to find cost effective solutions to the issues facing our industry. These types of partnerships, along with finding additional opportunities to enhance the working relationship between the responsible Federal agencies and our member cooperatives through our members and through the NRECA, should be encouraged as well. The Electricity Sector Coordinating Council (ESCC) is a great example of one of these partnerships. With the ESCC you see individual cooperative G&Ts, as well as participants from the Investor Owned Utilities and Municipal Electric Utilities, and the associated trade associations at a table with the Department of Energy (DOE), FERC, NERC and the Department of Homeland Security (DHS) working together to identify and find solutions.

CONSISTENCY

Due to the multiple levels of government oversight concerning cybersecurity (e.g. FERC, NERC and NERC's regional entities), finding consistency in the compliance process has had its challenges. The vague nature of some of the cybersecurity standards coupled with inconsistencies in the interpretation and auditing of those standards have created challenges with cybersecurity compliance for our member cooperatives. Refining this process to increase consistency and by providing more clarity with the respective standards would help streamline the process, enhance our effectiveness and provide greater certainty to our cybersecurity initiatives.

PHYSICAL SECURITY

While the focus of this hearing was specific to the issue of cybersecurity, IEC would like to briefly address the issue of physical security. There has been increased discussion surrounding this issue due to recent events and IEC acknowledges the importance of protecting our physical assets as well. The current initiative by FERC and NERC to develop physical security standards for critical assets is viewed as a positive step by Indiana's electric cooperatives. There is more to be accomplished with this effort and we welcome the opportunity to engage and provide our perspective throughout the process.

CONCLUSION

My comments today outlining areas of opportunity should not be viewed negatively on the interactions Indiana's electric cooperatives have had to date with the Federal agencies engaged in the cybersecurity arena. Our member cooperatives who work most closely with FERC, NERC, DHS and DOE, to name a few, would agree significant improvements and advancements have been made in all of these areas since the effort began. Our primary message for you today is that we are on a good path, but opportunities to improve still exist. Each of us, not just the respective Federal agencies, must assume our individual responsibility to work constructively, effectively and, most importantly, in partnership to address both current and future cyber-related threats to the reliability and security of our Nation's electric grid.

APPENDIX A: DESCRIPTIONS OF REFERENCED CYBER SECURITY MITIGATED VULNERABILITIES

Ignorance, Indifference and Lack of Knowledge of Cyber Threat Protection

Hoosier Energy's cybersecurity program ensures all levels of the organization are appropriately engaged. Responsibilities are clearly delineated among leadership and those responsible for direct cybersecurity activities.

Training and awareness programs are required for all who have access to cyber assets critical to the reliability of the BES. Training covers why Hoosier Energy's program is important, how it protects us and the relevant responsibilities. In addition, Hoosier performs awareness exercises exemplified by a Spearphishing exercise in 2013 that reduced click-thru rates from 30 percent to 2 percent.

Information Exfiltration

Hoosier Energy maintains an information protection program that identifies and classifies critical information, how it can be shared and with whom it can be shared.

Network-Based Cyber Attacks

Hoosier Energy maintains a separate, isolated network through the use of an electronic security perimeter (ESP) that isolates its critical cyber assets from less secure corporate network and neighboring utility connections. All communication is denied by default. Allowed communications are limited to specific protocols and approved sources from outside the ESP.

Direct Attack on Cyber Assets

Like in the ESP, communication is denied by default at each individual cyber asset.

In addition:

—All relevant security patches are applied judiciously
—Malicious software prevention is installed and kept current
—Strong passwords are required and changed periodically
—Unnecessary physical ports are blocked or disabled

Unauthorized Access and Changes to Cyber Assets and Protective Systems

All access is provisioned on the principle of need-to-know. No access is granted without first successfully completing a background check.

ESP communications are monitored and logged around the clock. Any change in configuration or any attempts at unauthorized access automatically creates an alert.

The WinCMU creates a baseline for each protected cyber asset. The WinCMU performs a daily comparison of the actual configuration and the baseline to systematically identify and alert on unexpected changes.

Physical Attack on Cyber Assets

All critical cyber assets are protected within a physical security perimeter (PSP) with access controlled using key cards, monitoring and logging.

Senator LANDRIEU. Thank you very much for that excellent testimony.

Mr. Peters with Entergy.

STATEMENT OF CHRISTOPHER PETERS, VICE PRESIDENT NERC/CRITICAL INFRASTRUCTURE PROTECTION COMPLIANCE, ENTERGY CORPORATION

Mr. PETERS. Good afternoon, Chairwoman Landrieu, Ranking Member Coats. Let me begin by thanking you for convening this panel and for inviting Entergy to participate. I'm pleased to appear here today to discuss Entergy's point of view on cyber and physical security threats to our system, the benefits of the public-private partnership process, and our experiences to date interfacing with the Electricity Sector Information-Sharing and Analysis Center (ES–ISAC).

By way of background, Entergy Corporation is an integrated energy company engaged primarily in electric power production and retail distribution. For some time now, Entergy has recognized the uptick in cyber and physical threats that have the potential to impact the reliability, safety, and security of our operations and the Nation's power grid. We accord such threats the same attention as we have always given the forces of nature, including ice storms, tornadoes, hurricanes, floods, and extreme heat, all of which can threaten the delivery of safe, reliable power.

Entergy supports a comprehensive strategy to managing our cyber and physical security defenses. This strategy leverages our corporate resources to minimize impacts from intentional and unintentional cyber or physical threats to our energy portfolio.

Importantly, these threats have strong support at the board of director and CEO level, which we believe is essential to implementing an enterprise-wide security program with the right amount of people for a security workforce and sufficient funding of the technologies required to deal with threats and breaches.

The threat landscape is inherently unpredictable and evolving, which is why mastering the fundamentals of cyber and physical security is best the best defense. In most cases attacks exploit lapses in basic operations that have been either ignored or which were not fully deployed.

One priority for Entergy is threat management. When a new threat emerges, Entergy conducts an internal review of our defense in depth plans to validate the existing security control framework and make changes as necessary. Accordingly, increasing physical security threats to energy delivery infrastructures have triggered reviews and updates to our security plans and posture, including the implementation of additional physical security controls in key facilities.

Public-private partnership participation is a key element in our cyber and physical security program and can be a significant force multiplier when leveraged. To strengthen our posture, over the past several years we have participated in a number of public-private programs. Allow me to highlight one program we feel is particularly helpful. Since 2008 Entergy has received and responded to over 40 NERC alerts related to grid security threats from the ES–ISAC. Based on the content of each alert, we quickly assemble cross-functional teams of subject matter experts to evaluate the highlighted vulnerabilities, assess potential impacts, and carry out appropriate mitigation steps.

Entergy considers the ES–ISAC a vital partner in achieving electric sector-wide situational awareness, improving national-level response and coordination, and fostering collaboration among key electric sector stakeholders.

The public-private partnership model is not perfect and will continue to evolve over time to ensure that the private sector can realize maximum value from our federally funded programs and technologies. Every utility must drive the daily transformation of their own cyber and physical security programs to defend against constantly changing threat landscapes.

Before concluding, I'd like to add that Entergy is a strong advocate of regulations and legislation that would bolster information-sharing between public and private entities about cybersecurity risks and events, allowing that the protections are built in for confidentiality and non-recourse. We believe access to information of this kind will help enhance the security posture of utilities.

Thank you again for giving Entergy the opportunity to share its views and I hope you found these comments helpful. We look forward to continuing to work with you in the coming year to ensure strong public-private relationships aimed at better securing the energy sector's critical infrastructure. I'm happy to answer any questions you may have.

[The statement follows:]

Prepared Statement of Christopher Peters

Good afternoon, Chairwoman Landrieu, Ranking Member Coats, and distinguished members of the subcommittee. Let me begin by thanking you for convening this panel and for inviting Entergy to participate. My name is Chris Peters and I am Entergy's vice-president for NERC and Critical Infrastructure Protection compliance, reporting to Entergy's executive vice president and chief operating officer.

I am pleased to appear here today to discuss Entergy's point of view on cyber and physical security threats to our system, the benefits of the public-private partnership process, and our experiences to date interfacing with the Electricity Sector-Information Sharing and Analysis Center (ES–ISAC).

By way of background, Entergy Corporation is an integrated energy company engaged primarily in electric power production and retail distribution. Entergy owns and operates power plants with approximately 30,000 megawatts of electric generating capacity, including more than 10,000 megawatts of nuclear power. We deliver electricity to 2.8 million customers in Arkansas, Louisiana, Mississippi, and Texas. We have approximately 14,000 employees.

For some time now, Entergy has recognized the uptick in cyber and physical threats that have the potential to impact the reliability, safety and security of our operations and the Nation's power grid. We accord such threats the same attention as we have always given to forces of nature, including ice storms, tornadoes, hurricanes, floods, and extreme heat—all of which can threaten the delivery of safe, reliable power.

Entergy supports a comprehensive strategy to managing our cyber and physical security defenses. This strategy leverages our corporate resources to minimize impacts from intentional and unintentional cyber or physical threats to our energy portfolio. Importantly, these efforts have strong support at the Board and CEO level, which we believe is essential to implementing an enterprise-wide security program with the right amount of people for a security workforce and sufficient funding of the technologies required to deal with threats and breaches.

The threat landscape is inherently unpredictable and evolving, which is mastering the fundamentals of cyber and physical security is the best defense: In most cases successful attacks exploit lapses in basic operations that have been either ignored or which were not fully deployed.

One priority for Entergy is threat management. When a new threat emerges, Entergy conducts an internal review of our defense-in-depth plans to validate the existing security control framework and make changes as necessary. Accordingly, increasing physical security threats to energy delivery infrastructures have triggered reviews and updates to our security plans and posture, including the implementation of additional physical security controls at key facilities.

Public-private partnership participation is a key element in our cyber and physical security program and can be a significant force multiplier when leveraged. To strengthen our posture, over the past several years we have participated in a number of public-private programs:

—The Government Forum of Incident Response and Security Team Conference;

—The FBI's Classified Cybersecurity Threat Briefings;

—NERC's GridEx and GridEx II sector-wide exercises;

—DOE's Electricity Subsector Cybersecurity Capability Maturity Model (ES–C2M2) and the Control Systems Cybersecurity Training delivered by Idaho National Labs;

—More than a few DHS' initiatives, including: Monthly Unclassified Nuclear Sector Threat Teleconferences, the Control Systems Cybersecurity Program, the Cyber Security Evaluation Tool (CSET), Classified Nuclear Cybersecurity Threat Briefings at the National Security Agency, the Enhanced Critical Infrastructure Protection Initiative, and the Cyber Storm III exercise; and

—Lastly, Entergy worked closely with NIST and participated in several workshops during the drafting of the Cybersecurity Framework in relation to Executive Order (EO) 13636: Improving Critical Infrastructure Cybersecurity.

Allow me to highlight one program we feel is particularly helpful. Since 2008, Entergy has received and responded to over 40 NERC alerts related to grid security threats from the ES–ISAC. Based on the content of each alert, we quickly assemble cross-functional teams of subject matter experts (SMEs) to evaluate the highlighted vulnerabilities, assess potential impacts, and carry out appropriate mitigation steps. Entergy considers the ES–ISAC to be a vital partner in achieving electric sector-wide situational awareness, improving national-level response and coordination, and fostering collaboration among key electric sector stakeholders.

The public-private partnership model is not perfect and will continue to evolve over time to ensure that the private sector can realize maximum value from federally funded programs and technologies. Every utility must drive the daily transformation of their own cyber and physical security programs to defend against constantly changing threat landscapes.

Before concluding, I would like to add that Entergy is a strong advocate of regulations and legislation that would bolster information sharing between public and private entities about cybersecurity risks and events. Allowing that protections are built in for confidentiality and non-recourse, we believe access to information of this kind will help enhance the security posture of utilities.

Thank you for giving Entergy the opportunity to share its views and I hope you've found these comments helpful. We look forward to continuing to work with you in the coming year to ensure strong public-private relationships aimed at better securing the energy sectors' critical infrastructure. I am happy to answer any questions you may have.

Senator LANDRIEU. Thank you all very much.

Let me begin with a question to each of you, starting with Dr. Katz. If you could recommend in a minute or less something for the Department of Homeland Security to focus on improving their current operations—I agree with Senator Coats that the Department has turned the corner. They have the appropriate, I think, leadership in place on this issue. Lots of initial challenges have been sorted out. But if you could give 1 minute of testimony about what you would suggest Homeland Security do; take the next step in a specific area, whether it's in education, whether it's in collaboration, whether it's in authorization, et cetera, et cetera, what would you say?

Dr. KATZ. From my point of view, I think really focusing on cybersecurity workforce development will be very helpful. I think you hit the nail on the head in the previous panel when you mentioned that the requirements for cybersecurity professionals really need to be laid out precisely, because hearing that 200,000 students a year are needed is not very helpful unless we know precisely what kind of background those professionals need and, really more importantly, without an understanding of the fact that those 200,000 professionals are not all going to be identical. They're going to be people—you're going to need people with different needs and different backgrounds, and breaking that out further and really understanding that would be a big step forward and would allow the Nation's academic institutions to better prepare to meet that need.

Senator LANDRIEU. Yes, and I'm going to continue to press my staff and other staffs and any witnesses. If there is such an effort going on, in a comprehensive, clear way trying to identify that specifically, I'd like to know about it, because I keep looking and haven't found it. For instance, in your testimony you said you've graduated 4,000 in cybersecurity-related fields. Would that include math? Would that include general math or economics, et cetera?

Dr. KATZ. Actually, I believe it's fairly broad, so 4,000——

Senator LANDRIEU. Is very broad, and it's "cyber-related fields." Well, you know, our Nation has a great demand for math teachers that have to go into the classroom to teach traditional math. We can't doublecount. Those are teachers we need for the math classroom. Where are our math graduates going into—this is additional cyber.

I really am going to continue to press on this until I can get a clear understanding to make sure we're moving in that direction. But thank you for that.

What would you say at CenturyLink—and I really appreciate understanding the role that the Internet providers—and there are three main providers, correct, AT&T, Verizon, CenturyLink? Who else would you put on that list?

Mr. MAHON. We would be the top three.

Senator LANDRIEU. Is it fair to say that everybody's business comes through your networks, everybody's?

Mr. MAHON. At one point or another, that's an accurate statement.

Senator LANDRIEU. So one thing to consider is the outward perimeter, that you're it. If your systems can be secure and our Government partnership with the three of you can be very good and solid, together we could do a lot of protection for what's inside of that perimeter, is kind of the way I'm thinking about it. Is that how you talk with Verizon and AT&T, and what would you say to the Department of Homeland Security about that?

Mr. MAHON. Your assessment is correct. What I would say about the Department of Homeland Security is, while they do have very good programs with ECS and E3A, we do need to move it to the next level. The majority of the Homeland Security information-sharing model is a one-size-fits-all. They get broad-based information from other Government agencies, they put it in a format suitable for dissemination across all verticals, all infrastructures, small to large corporations. While that's very helpful, if you are a small to medium-sized company and don't have a sophisticated information security program it is of limited value to the larger corporations, particularly the critical infrastructures.

The analogy that I often use is that you're invited to a wedding and you can bring a gift to the bride. She certainly appreciates it, but she would prefer you go to her wedding registry and select something she really needs.

That's really where we need to go today. We have very specific collection requirements on how to protect our network. We do not have access to all the threat information, and I believe the Government, whether it's through the Department of Homeland Security or other agencies, would be of better assistance to us if we gave them very specific requests to see if they could be fulfilled for information.

Senator LANDRIEU. Thank you. That's very helpful.

Mr. Bowers, what would you say?

Mr. BOWERS. I would say that our exposure to DHS has been fairly limited. Most of what we have done has been primarily through FERC, NERC, and the regional entities that work underneath NERC.

Senator LANDRIEU. The reason for that, just to clarify—you of course know it—is that this grid or this infrastructure is the only mandatory regulated infrastructure, to my understanding, the electric grid, through FERC and NERC. So the other private sector companies that have financial infrastructure or other energy infrastructure are not. And it's been the problem or the challenge, as Senator Coats has pointed out, it's hard to get the groups together to figure that out.

But you in the electric sector are working through it fairly well. I know there have been problems, but would you say that that's generally correct?

Mr. BOWERS. Yes, I would agree with that. We've certainly seen tremendous progress over the 7 years. I think as we've worked with the respective Federal agencies and as they've gotten to know us better, as we've gotten to know them better, it's certainly created a much more productive partnership.

As it relates to funding or areas of emphasis, I'll go back to a couple of things that I mentioned. Obviously, providing funds to help bolster and streamline the information-sharing process. One of the things is being able to get real-time information that is actionable. A lot of times that's not the situation, and I know that's not the goal. The goal is for everyone involved to be able to try to avoid these types of situations, and when they do occur obviously to then mitigate them to the best of our ability.

In addition, I mentioned supporting or the expansion of security clearances. I think that will be beneficial to the information-sharing component. Then also, just as we've continued to work through these various standards, bringing that level of consistency, both in the standards, the interpretation, as well as the auditing consistency, would be areas of emphasis for our perspective.

Senator LANDRIEU. Mr. Peters, and then we'll get to Senator Coats for his questions.

Mr. PETERS. Senator, I think DHS has done a great job at raising awareness around control system security, and it's my understanding that 80 percent of the control systems that are coming on line have been tested for various types of cyber intrusions and basic security features. As we look to upgrade our legacy control systems to next generation, that increased funding and support for R&D for control systems that have advanced cyber features would be very beneficial. I know there's been a tremendous amount of success between DHS, the Idaho National Labs, and various control systems vendors in this area. So I would recommend championing continued support for that area.

Senator COATS. Mr. Mahon, how do you work with the smaller businesses, the community banks, the smaller retails, smaller investment houses, and so forth? Obviously, the bigs—and we just have to look at the response of Target and, say, Neiman Marcus and others—have spent a very considerable amount of money to upgrade their systems, to put more security in place, at very, very considerable cost.

But the smaller entities really can't afford to do that. Yet they have the same vulnerabilities, maybe not to as many people, but to sizable—and Scott, I think I would ask you also. You know, you're serving more rural communities, customers and so forth. How do you find the resources to do what you need to do and keep everybody on an even keel?

Mr. MAHON. Well, the small to mid-sized businesses have concluded, Senator, exactly what you just stated, that the cost of IT and the type of cybersecurity protections they need they cannot afford. One of our lines of products and services is referred to as Managed Security Services. We spend the time with those customers explaining our information security program, the security across our core network, and our Managed Security Services products.

When they look at these types of products they can acquire through companies like CenturyLink, they can frequently make the informed decision that it is better actually to outsource your security to companies like CenturyLink, because we can provide them with subject matter experts and a scale model that they could not have an equivalent model of should they decide to build it on their own.

They are also suffering from the same shortage of professionals in the industry. The larger corporations obviously are able to attract them away with a little bit more sophisticated work in some situations. So they also suffer from workforce development issues.

Senator COATS. Scott.

Mr. BOWERS. Senator, I think it ultimately comes back to what our mission is, and our mission is to provide safe, reliable, and affordable electricity to the members that we serve. I would throw "secure" into that as well, based on the dynamics of the last decade plus.

With that, our distribution cooperatives are our first line. They work very closely with their two G&Ts. The G&Ts take and have more interaction with the Federal Government as it relates to these issues, but with the G&Ts and the distribution cooperatives, they work very closely together to make sure that they are making—that the distribution systems are secure.

Our distribution cooperatives obviously are very concerned about the security of our member personal data. Those are things as foundational of who we are and that we are member-owned. It's very near and dear to us and ultimately to who we are, and we have to make sure that we provide the reliability and security and make those investments, while also trying to balance the affordability aspect on top of that.

Senator COATS. I'll take a response from anybody on the panel. How do you provide for security against insider access, the equivalent of a Snowden, but within the retail sector or the financial sector or whatever here, not the intelligence sector? What types of security procedures and hiring procedures and security clearances and so forth and monitoring that, of course?

We hear today that, as has been indicated, there are just independent actors that somehow want to cause some chaos, whether for personal gain or whether for just the sport of it. How do you monitor all that and ensure that you don't fall victim to something like that?

Mr. MAHON. We have an insider threat program at CenturyLink. It depends upon where you are in the organization. If you're working classified work, you have security clearances and the Government process around that, as you know, is pretty rigorous.

But also, there are other positions within the company that you also have to be super-vigilant around. We have some baseline background checks we do on all employees as they enter the organization. But really the insider threat is just the problem, the fact that they're an insider. So really it becomes more of a training program for your managers and your supervisors to spot concerning behavior, so they understand when someone is performing in a manner that is out of the norm.

These types of events that we frequently see in the media of an insider doing extensive damage, if you were to do an after-action on them you would learn most typically that there were signs of behavior that came to the attention of key supervisors, other employees, or managers. They just either weren't trained to spot it, they didn't realize the significance of it, or they didn't have a way to report it to the appropriate organization that could do something about it.

So there is a very formal insider training program in a lot of corporations like CenturyLink and they are effective. Do you still have problems? Obviously, you can't spot everyone who's an insider. But there are ways to manage those risks to an acceptable level.

Senator COATS. Anybody else want to address that?

[No response.]

Senator COATS. My time has run out and our time I think has run out. We can submit questions for further response, but I want to thank all of you and thank the Chair for convening this hearing, and thank all of you for participating in this. This is a critical issue that we need to get it right, because, as our former Homeland Security Secretary once said, the perpetrators or the criminals, the actors, the States, et cetera, they only have to be successful once; we have to be successful 100 percent of the time in trying to stop all their efforts. So it's a real challenge. I appreciate all of your work in terms of trying to keep us safe from all these cyber attacks and intrusions.

Thank you.

Senator LANDRIEU. Yes, and thank you, Senator Coats, for your leadership. We wanted to conduct this hearing jointly and the Senator provided a lot of background to allow us to do that.

I thank all of our witnesses for your testimony today. I am committed to doing all we can in this subcommittee to continue to focus on these issues.

ADDITIONAL COMMITTEE QUESTIONS

We're going to leave the record open for 2 weeks. Questions should be submitted to the committee staff by close of business Wednesday, May 21.

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

QUESTIONS SUBMITTED TO DR. PHYLLIS SCHNECK

QUESTIONS SUBMITTED BY SENATOR MARY L. LANDRIEU

WORKFORCE DEVELOPMENT

Question. Deputy Under Secretary Phyllis Schneck, has the Secretary decided to reassess all of the cybersecurity education, training, and outreach goals of the Department—including the goal to educate 1.7 million students by 2021?

If so, in what timeframe will the reassessment be completed?

What analysis and method will be used to create a metric that meets the nature of the threat?

Answer. The Department of Homeland Security (DHS) has conducted a reassessment of its combined efforts to provide cybersecurity education, training, and outreach throughout the Nation. The Department determined that it can reach the goal of 1.7 million American students of all ages within the original timeframe through a unity of effort across the Department. The 1.7 million students include participants in a number of programs:

—DHS continues the Integrated Cybersecurity Education Communities (ICEC) project and will extend the grant that supports this project, providing an additional $5 million to the grantee to ensure that the project grows in the summer of 2015.

—DHS continues to support the National Centers of Academic Excellence and Scholarship for Service programs, which collectively reaches over 18,000 students per year.

—DHS sponsorship of cybersecurity competitions, particularly at the high school level, increases the number of students receiving hands-on education in cybersecurity by approximately 12,000 students each year.

—The Federal Virtual Training Environment and Cybersecurity Training Events are available to 125,000 students each year.

—The National Initiative for Cybersecurity Careers and Studies (NICCS) portal directs thousands of Americans across the country to cybersecurity education and training programs each year.

Pertaining to your question on the analysis and methods used to create a metric that meets the nature of the threat: The cybersecurity threat is dynamic and consists of nation-States, criminal organizations, individual actors, and systems degradation. The Department approaches its cybersecurity and its broader critical infrastructure security and resilience missions from a risk management perspective which incorporates associated threats, vulnerabilities and consequences. Under the National Infrastructure Protection Plan (NIPP), the critical infrastructure community evaluates the effectiveness of risk management efforts within sectors and at national, State, local, and regional levels by developing metrics for both direct and indirect indicator measurement.

Within the NIPP structure, sector specific agencies work with representatives from private industry (sector coordinating councils or SCCs)—to bring insight to both sides in each sector. Such measures inform the risk management efforts of partners throughout the critical infrastructure community and help build a national picture of progress toward the vision of the NIPP as well as the National Preparedness Goal. Among other functions, the NIPP evaluation process also includes the collection of performance data to assess progress in achieving identified outputs and outcomes, and assessing progress toward achievement of the national priorities, goals and vision.

DHS also places tremendous value on the effectiveness of our cyber specific programs, and is continuously exploring new ways to increase their impact. A key focus is on the future of cyber threats, and how to quantify mitigations that must be built today in order to be in place when needed later. For example, NPPD is studying the effectiveness of delivering classified indicators through the Enhanced Cyber Security Services (ECS) program to determine the appropriate balance of cost, benefit, and impact per indicator. While this balance can be hard to determine, it is the only technology that can defend at the network perimeter against some of the most crippling threats, such as destructive malware, and is priceless in an instance that could save an entire network or organization from a crippling attack.

PROTECTION OF FEDERAL NETWORKS AND WORKING WITH THE PRIVATE SECTOR

Question. Deputy Under Secretary Schneck, what is the Department doing specifically to look long term at the effectiveness of Einstein, Continuous Monitoring and Diagnostics, and all the rest of the suite of acquisitions and programs to protect networks and plan for major procurements?

How do you know programs are continuing to be innovative?

How is the Department including industry in this planning so that they can also plan long term for investments in solutions?

Answer. Effectiveness of the Continuous Diagnostics and Mitigation (CDM) program is monitored through annual performance targets, performance measures, and quarterly reports. Once the program has entered the operations and maintenance phase, it will conduct annual operational assessments, consistent with applicable DHS requirements and OMB Guidance for Information Technology Business Cases (formerly known as Exhibit 300s).

The National Cybersecurity Protection System (NCPS) program office tracks effectiveness of the ENSTIEN system and the protection it offers through a number of different means. By analyzing intrusion prevention alerts that are generated based on both commercial and Government-provided classified cyber indicators the program office is able to better understand the effectiveness of the information that is being used to take action on malicious traffic. The Cyber Pilot Program (CPP) also works to identify gaps in current capabilities and initiates pilot programs that may bring new value. For example, while signature-based systems will continue to have a place in cyber defense for the foreseeable future, there is recognition that behavioral-based systems are also required as part of defense in-depth. The NCPS Program Office is currently in the process of planning a CPP pilot that is analyzing a behavior-based system in a real-world Department/Agency Security Operations Center (SOC).

As EINSTEIN and Continuous Diagnostics and Mitigation capabilities are deployed across Federal Executive Branch civilian agencies, the Department will continue to measure the impacts of these capabilities on the security posture of Federal agencies. Even facing increased threats, impacts can be reduced using real-time action and the ability to leverage what was learned in each event to protect ourselves and others from future attempts. Furthermore, over the long term, the Department recognizes that the cyber threat landscape evolve quickly and, as such, it will identify pursue cybersecurity solutions that quickly close gaps in network protection.

Overall, CDM and EINSTEIN are designed to fuse together in the future, to create a presence within the .gov for detection of threats at the perimeter and inside each network. That presence manifests in intrusion detection/prevention and CDM capabilities, but also serves as information collection across the .gov. This situational awareness can leverage the power of the fastest computers to correlate events seen on different networks and form intelligence that can mitigate threats that previously would have gone unnoticed.

Pertaining to your question on knowing the programs will continue being innovative: The NCPS and the CDM program are deeply committed to continued innovation. They are structured to be responsive to the constantly evolving and dynamic threat environment by taking advantage of the private sector's business imperative to remain innovative for competitive purposes. Within NCPS, EINSTEIN's Intrusion Prevention Security Service (IPSS) will be deployed as a managed commercial service provided by the major Tier 1 Internet Service Providers. Deploying IPSS as a managed service allows those services to evolve at industry speed based on best commercial practices.

At its inception, the CDM program decided in the interest of efficiency, expediency and effectiveness to pursue commercial best fit in acquiring necessary tools for continuous diagnostics and mitigation. The CDM Tools/Continuous Monitoring as a Service (CMaaS) blanket purchase agreement (BPA) is based on General Services Administration Schedule 70 and includes a process by which the BPA can be updated as new commercial off-the-shelf products become available and are judged to be technically acceptable to meet the requirements of the CDM program. Furthermore, a feature of the BPA requires each of the vendor companies to regularly perform technology refresh of solutions that are proposed and delivered to departments and agencies.

In an effort to ensure that the program has the ability to evolve and adapt to emerging technologies, the NCPS program office has ensured that it has a flexible infrastructure that can accommodate a range of technologies and scale them to meet real world scenarios. For example, in support of the NCPS Block 2.2 Information Sharing capability, the program office has focused initial efforts on deploying the key infrastructure components necessary to support information sharing such as Identity, Credential & Access Management (ICAM), a secure portal to provide a user interface, an enterprise service bus to support data translation between applications, and a Cross-Domain Solution (CDS) to support data exchanges at different classification levels. Additionally, as the number of incidents increase, more data is collected from the incidents themselves and is then correlated and disseminated. This information sharing will reduce impacts due to better real time detection, and our ability to use each event to protect the larger ecosystem.

Information sharing takes two forms: human and machine. Human information sharing includes personal relationships, as well as reports generated from data collected and correlated by NPPD programs that is formed into a human-informative visualization or reports. Information in the form of cyber threat indicators can be sent between machines at Internet speed, so that when a threat targets a site, that site already knows of the threat as it was alerted by an indicator.

Overall, CDM and EINSTEIN are designed to fuse together in the future, to create a presence within the .gov for detection of threats at the perimeter and inside each network. That presence manifests in intrusion detection/prevention and CDM capabilities, but also serves as information collection across the .gov. This situational awareness can leverage the power of the fastest computers to correlate events seen on different networks and form intelligence that can mitigate threats that previously would have gone unnoticed.

Pertaining to your question on how the Department is including industry in the planning: CDM has a long history of collaboration with industry, using technologies developed in private sector and continually reconnecting with their private sector vendors to ensure that the CDM leverages the latest private sector innovations.

Prior to release of the original Blanket Purchase Agreement (BPA), in June and August 2012, the program held industry days to provide insight into the program's upcoming solicitation approach. Once the BPA was established in August 2013, the program conducted additional Industry Days (regarding the next set of solicitations for CDM tools and integration services for up to 60 agencies), training (both overview and hardware asset management), special notices, advanced notices, Web sites and considering other means to ensure active collaboration with industry.

The CDM program actively collaborates with its Agency stakeholders, as well as the 17 vendor companies that hold prime contracts under the BPA. The program has an established Leap Ahead technologies program that conducts outreach with industry to be kept apprised of technological developments as they are made available commercially. The Program is budgeted to manage the procurement and program lifecycle activities to include a BPA recompete starting in fiscal year 2017.

The NCPS Program Office utilizes Requests for Information (RFI) and actively participates in Industry Days at both the Department and program level to keep industry informed. Additionally, NSD's Cyber Pilot Program conducts market research as part of its gap analysis process.

QUESTIONS SUBMITTED BY SENATOR THAD COCHRAN

Question. I think we understand the importance of traditional ranges for testing and exercising with conventional weapons like aircraft, guns, or missiles.

Could you explain to the subcommittee the function and value of developing and utilizing ranges in the cyber domain? Are there ongoing efforts to connect the cyber ranges so that we can test cyber tools on more realistic virtual ranges and perform larger, more high fidelity exercises in the cyber domain?

Answer. Ranges in the cyber domain allow cyber professionals to test system operations and their own skills and abilities. Overall, ranges directly contribute to DHS's commitment to ensuring that operational software and/or hardware systems are validated against both best practices and the systems' compliance with Government requirements. NPPD leads the Federal Government's effort to secure civilian Government computer systems, and work with industry and State, local, tribal, and territorial governments to secure critical infrastructure and information systems. DHS must validate information system security configurations both prior to and after deploying the system in an operational environment. With these requirements in mind, cyber ranges provide a controlled, predictable environment where operational systems can be tested and evaluated against known stressors such as cyber attacks or improper configuration. For example, a simulated environment could be used to conduct user acceptance training and to complete performance and load testing of the National Cybersecurity Protection System (NCPS) applications. This type of environment would inject real-world threat data and measurement instruments, offering a valuable realistic training experience for personnel.

In addition to NPPD programs, operational elements across the DHS enterprise could also leverage a range to validate and test the capabilities of present and future security and forensics products. A range that allows for large-scale testing within an adaptable environment would provide the capability to verify the potential benefits of products and tools before purchase, test tools against new threats, and allow personnel to familiarize themselves with innovative tools.

Pertaining to your question on ongoing efforts to connect to cyber ranges: Yes, the DOD Enterprise Cyber Range Environment Forum has developed a charter to federate the cyber ranges across the DOD enterprise so that tools testing capability can be integrated with the ability to conduct exercises.

Question. 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 Federal Government does not have thresholds for when it would defend non-Federal infrastructure from cyber attacks. The Department, working with public and private sector partners, has identified infrastructure—both public and private—where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security. The resulting list of entities, identified under Executive Order 13636, has been briefed to relevant Congressional Committees and the entities themselves have been notified of their designation.

The statutory definition of critical infrastructure is, "Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." 42 U.S.C. section 5195c(e). Cooperation with these entities and clearly defining lanes of responsibility across the Federal Government are vitally important for our engagement with these entities.

We have heard about the importance of cooperation and clearly defined lanes of responsibility across the Federal Government for our cybersecurity efforts.

Question. What are your respective roles in receiving and sharing threat information with the private sector?

Answer. DHS shares timely and actionable cybersecurity information across its partners and constituents to establish and maintain shared situational awareness.

The types of cyber information DHS shares most often include alerts and warnings, analysis of actor tactics, techniques and procedures to aid in incident detection, indicators of malicious activity and supporting contextual information, best practices, vulnerability information and assessments, and trend analysis.

Working across the department with our cyber capabilities housed in the U.S. Secret Service, Coast Guard, CBP, ICE, and others, DHS has several programs in place to help facilitate the sharing of timely, actionable information to and from the private sector:

—The National Cybersecurity and Communications Integration Center (NCCIC) is a 24×7 center responsible for providing a common operating picture for cyber and communications across the Federal, State, and local government, intelligence and law enforcement communities, and the private sector. The NCCIC is based in DHS's Office of Cybersecurity and Communications (CS&C), a component of the National Protection & Programs Directorate (NPPD). On both a steady-state and emergency basis, it fuses, coordinates, and shares information from its operational elements, including the:

—The U.S. Computer Emergency Readiness Team (US–CERT), which responds to cybersecurity incidents and analyzes information from multiple sources to develop timely and actionable alert and warning products for public and private sector partners.

—The Industrial Control Systems Cyber Emergency Response Team (ICS–CERT), which works to reduce risk to the Nation's critical infrastructure through public-private partnerships and by providing onsite support to private sector industrial control systems owners and operators for protection against and response to cyber threats, including incident response, forensic analysis, and site assessments.

—The National Coordinating Center for Telecommunications (NCC), which leads and coordinates the initiation, restoration, and reconstitution of National Security/Emergency Preparedness (NS/EP) telecommunications services or facilities under all conditions.

—NCCIC Operations and Integration (NO&I), which leverages planning, coordination, and integration capabilities to synchronize analysis, information sharing, and incident response efforts to ensure effective synchronization across capabilities.

—Integrating information from all partners—private and public sectors, including State, local, tribal and Federal, in both the cyber and communications arenas—the NCCIC creates and shares a common operational picture, coordinates response activities, and protects our Nation's critical networks.

—Through the Cybersecurity Information Sharing and Collaboration Program (CISCP), DHS has established a systematic approach to cyber threat information sharing and collaboration between DHS and the 16 critical infrastructure sectors.

—By sharing unclassified cyber threat indicators, DHS enables the detection, prevention, and mitigation of threats. This builds a more holistic understanding of cyber threat activity occurring across the 16 critical infrastructure sectors and across the Federal Government.

—Through these partnerships, CISCP enables information sharing and collaboration with our critical infrastructure partners to share new cyber threat, incident, and vulnerability information This exchange is conducted in near-real time to enhance collaboration and to better understand the threat and improve network defense for the entire community.

—A key aspect of CISCP is its bi-directional information sharing construct. CICSP participants submit indicators of cyber threat activity on their network to DHS that can be shared with other CISCP participants in an anonymized, aggregated fashion. Furthermore, the NCCIC allow cleared sector participants onto the NCCIC floor to ensure close coordination and communication when an event occurs.

Questions Submitted by Senator Lisa Murkowski

Question. The President's Executive Order (EO) 13636 on cybersecurity and its accompanying Presidential Policy Directive (PPD) 21 directed the National Institute of Standards and Technology to develop a voluntary cybersecurity framework in partnership with private industry. As you know, the Energy Policy Act of 2005 established mandatory cyber and physical security standards for the electric industry through the Federal Energy Regulatory Commission/North American Electric Reliability Corporation (FERC/NERC) stakeholder process. Via the FERC/NERC stakeholder process these cybersecurity standards have been continuously updated and revised since the law's enactment to reflect ever-changing cyber threats. The industry is now on CIP Version 5 which includes 12 new requirements and also prioritizes cyber assets.

How does the voluntary framework called for in EO 13636 and PPD–21 interface with the mandatory standards already in place for the electric industry? For example, what if a voluntary measure under the NIST framework conflicts with a mandatory standard?

Answer. Because the Cybersecurity Framework is a voluntary approach, organizations can determine how to best use the Framework so that it meets their business requirements. It is designed to be supplemental, not a replacement for industry regulations. If utilities are currently regulated, or become subject to regulation, then regulations would take compliance precedence and the Framework could be used to supplement these requirements.

Question. What actions are DHS either currently undertaking or planning to undertake to protect the grid (at both the transmission and distribution level) from cyber threats? To what extent is DHS duplicating ongoing grid-protection efforts by FERC, NERC and State public utility commissions?

Answer. The Department's National Protection and Programs Directorate (NPPD) supports critical infrastructure owners and operators in preparing for, preventing, protecting against, mitigating from, responding to, and recovering from all-hazards events, such as cyber incidents, terrorist attacks, and natural disasters. The National Infrastructure Coordinating Center (NICC) and the National Cybersecurity and Communications Integration Center (NCCIC) fulfill this DHS responsibility within the critical infrastructure partnership.

Stakeholders throughout the critical infrastructure community—owners and operators; Federal partners; regional consortia; and State, local, tribal, and territorial governments—can, and do, connect to the NICC and NCCIC. In turn, these centers, along with an integrated analysis function, build situational awareness across critical infrastructure sectors based on partner input and provide information with greater depth, breadth, and context than information from any individual partner or sector.

As a part of the NCCIC's overall cyber coordination and response capabilities, NCCIC operates the Industrial Control Systems Cyber Emergency Response Team (ICS–CERT). ICS–CERT coordinates control systems-related security incidents and information sharing with government, and private sector constituents, including vendors, owners and operators, and international and private sector CERTs. The focus on control systems cybersecurity provides a direct path for coordination of activities among all members of the critical infrastructure stakeholder community as well as representatives from law enforcement. This effort spans all phases of electric power and includes:

—*Standards Development.*—In 2010, ICS–CERT was a key member of the Smart Grid Interoperability Panel, Cyber Security Working Group which helped develop and issue the NIST Guidelines for Smart Grid Cyber Security (NISTIR 7628, September 2010).

—*Cybersecurity Assessments.*—To date, ICS–CERT has directly assisted 50 asset owners in the electric subsector by performing these assessments and providing strategies for improving their defensive posture.

—*Vulnerability Handling and Dissemination of Mitigation Strategies.*—To date, ICS–CERT has addressed over 600 vulnerabilities, many of which affect devices and software used in electric grid control systems.

—*Incident Response Services.*—To date, ICS–CERT has provided incident response services to 114 electric sector organizations by analyzing malware, reviewing digital media from hard drives and log files, and recommending strategies for recovery and preventing future intrusions.

—Training to improve asset owners' cybersecurity skills and practices:

—ICS–CERT provides cybersecurity training to network administrators and control system professionals. Courses in cybersecurity principles and best practices are offered through on-line courses and instructor-led classes.

—*Situational Awareness.*—ICS–CERT provides actionable situational awareness through briefings, alerts, advisories, and indicator bulletins. ICS–CERT conducts both unclassified and classified briefings and disseminates information on the Secure Portal and on its Web site.

Pertaining to your question on the extent DHS is duplicating ongoing efforts by FERC, NERC, and State public utility commissions: DHS is not duplicating efforts with the Federal Energy Regulatory Commission (FERC), the North American Electric Reliability Corporation (NERC), or the State public utility commissions but rather ensuring coordination of efforts. As instructed by Presidential Policy Directive 21, among other authorities, DHS provides cybersecurity information sharing, technical assistance and national coordination to enhance the security resilience of U.S. critical infrastructure. DHS does not directly provide the protection but assists critical infrastructure owners and operators in securing their own systems and coordinating their information sharing across sectors and between different partners.

NCCIC/ICS–CERT coordinates regularly with NERC via the Electricity Sector Information Sharing and Analysis Center (ES–ISAC) to ensure sharing of incident related information and dissemination of information products. This eliminates duplication of effort when triaging threat and vulnerability information. ICS–CERT also partners with FERC to conduct assessments at utilities to ensure consistent messaging and a unified methodology for assessing cybersecurity. In addition, ICS–CERT hosts weekly Secure Video Teleconferences, and conducts monthly information sharing sessions with energy sector stakeholders via both classified and unclassified means, that are attended by the Department of Energy, the non-regulatory Office of Energy Infrastructure Security (OEIS) within the Federal Energy Regulatory Commission (FERC), the Nuclear Regulatory Commission (NRC), the Federal Bureau of Investigation (FBI), NERC and the ES–ISAC.

Question. You testified that NPPD is working with DOE to implement a sustained outreach strategy to energy sector chief executive officers to elevate risk management of evolving physical and cyber threats to the enterprise level.

Please explain more fully. What other sectors has DHS undertaken such an outreach effort with?

Answer. In addition to incident response activities, ICS–CERT and the FBI, in coordination with the Department of Energy (DOE), the Electricity Sector Information Sharing and Analysis Center (ES–ISAC), Transportation Security Administration (TSA), the Oil and Natural Gas and Pipelines Sector Coordinating Council's Cyber Security Working Group, and other partners conducted a series of "Action Campaign" briefings at both the Secret and Unclassified levels to provide further context of a specific threat and to highlight mitigation strategies. The briefing campaign began in June 2013 and covered major markets across the United States. These classified briefings have reached over 750 private sector attendees, many of whom were directly associated with power grid operations. Outreach activities in the form of risk and mitigation briefings play a key role in mitigating risks to critical infrastructure.

While the energy sector was the focus for the action campaign briefings, NCCIC/ICS–CERT has always allowed other cleared sector participants to join these briefings. In addition, ICS–CERT holds regular monthly and quarterly classified and unclassified briefings for the nuclear, manufacturing, chemical, dams, water, transportation sectors.

Question. You testified that "[l]egislation providing a single clear expression of DHS cybersecurity authority would greatly enhance and speed up the Department's ability to engage with affected entities during a major cyber incident and dramatically improve the cybersecurity posture of Federal agencies and critical infrastructure." Such legislation, however, could undermine the mandatory cybersecurity standards we already have in place for the electricity industry as a result of the 2005 Energy Policy Act.

Please comment. Is DHS proposing to usurp the grid protection authorities already granted by Congress to FERC and NERC?

Answer. NERC and FERC have clear functions—one is to increase the functionality and reliability through standards for grid operations and the other is the U.S. regulator of grid owners and operators. The Administration is not seeking to supplant these efforts. Rather it has asked the Congress to codify the existing voluntary cybersecurity technical assistance and mitigation role the Department of Homeland Security (DHS) plays in supporting critical infrastructure.

DHS is neither a regulator nor a standards body for the electric sector, but provides cybersecurity assistance through information sharing and technical assistance on a voluntary basis when requested. DHS, under PPD–21, is responsible for leading and coordinating the national effort to protect critical infrastructure from all hazards, including cyber incidents, by managing risk and enhancing resilience through collaboration with the critical infrastructure community. To achieve this end, DHS works with public and private sector partners, including the Department of Energy, FERC, and NERC, to identify and promote effective solutions for security and resilience to manage the evolving risk environment.

CONCLUSION OF HEARING

Senator LANDRIEU. Without further business, the subcommittee is adjourned. Thank you.

[Whereupon, at 3:30 p.m., Wednesday, May 7, the hearing was concluded, and the subcommittee was recessed, to reconvene subject to the call of the Chair.]