Testimony of

Dr. Phyllis Schneck
Deputy Under Secretary for Cybersecurity and Communications
National Protection and Programs Directorate

United States Department of Homeland Security
Before the
United States Senate
Appropriations Committee
Subcommittee on Homeland Security

May 7, 2014

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 (FY) 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 FY 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) 24x7 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 FY 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 24x7 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 24x7 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 websites 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 websites 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 FY 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 FY 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 FY 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 (E^3A) 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 FY 2016. With the adoption of E^3A, 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 FY 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 24x7 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 FY 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 cyberalerts 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, US 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 website, 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 FY 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

[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.

response from hours to 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 decision-making 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 FY 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 FY 2015 President's Budget Request for NPPD's cybersecurity efforts. I look forward to any questions you may have.