Testimony of

NPPD Deputy Under Secretary for Cybersecurity

Phyllis Schneck

Before the

Senate Homeland Security and Governmental Affairs Committee

Regarding

"Strengthening Public-Private Partnerships to Reduce Cyber Risks to Our Nation's Critical Infrastructure"

March 26, 2014

Chairman Carper, Ranking Member Coburn, and distinguished Members of the Committee, it is a pleasure to appear before you today to discuss the Department of Homeland Security's (DHS) work to improve the cybersecurity of critical infrastructure. We view cybersecurity as key to the larger goal of infrastructure security and resilience. Therefore, DHS takes a holistic, cross-sector view of cybersecurity as a risk management decision that needs to be part of the executive discussion in organizations of all sizes across government and industry. America's national security and economic prosperity are increasingly dependent upon critical infrastructure that is at risk from a variety of hazards, including attacks via the Internet. In this spirit, today I will speak to our cybersecurity mission, implementation of Executive Order (EO) 13636 and delivery of our Critical Infrastructure Cyber Community (C^3, pronounced "C-Cubed") Voluntary Program, which promote cybersecurity for critical infrastructure to enhance their shared security and resilience.

DHS Vision for Cybersecurity

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 National Cybersecurity and Communications and Integration Center (NCCIC) the source of a "weather map" for global cyber indicators and activity.

We are working to further enable the NCCIC to receive information at "machine speed."[1] This new capability will begin to enable networks to be more self-healing, as they use mathematics and analytics to mimic restorative processes that occur biologically. 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 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.

We can increase the availability of information flow through stakeholder engagement, constant trust-building to optimize the information shared voluntarily and better use of current authorities. At the

[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.

core of this effort, we also must continue to ensure that privacy and civil liberties protections are baked in to everything we do and we do this primarily by focusing on the sharing of cyber threat information that is non-attributable and anonymized to the greatest extent feasible.

To develop a National Oceanic and Atmospheric Administration-like capability in dynamic data aggregation to a "weather map" will require a significant leap forward from our current efforts sharing information at human speeds with mostly manual processes. DHS seeks machine-speed information sharing with a broad set of partners, which will require an internal data management system that provides real-time situational awareness from which people and tools can extract information. Some of 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.

The programs that DHS has created provide a sound foundation for the above vision. 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. We continue to believe 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.

Implementing Presidential Directives

In February 2013, the President signed EO 13636 on Improving Cybersecurity Critical Infrastructure and Presidential Policy Directive (PPD)-21 on Critical Infrastructure Security and Resilience. These presidential policy documents direct Federal agencies to use their existing authorities and increase partnership with the private sector to provide better protection for the computer systems and networks that are critical to our national and economic security. Critical infrastructure security and resilience requires partnership between public, private, and non-profit sectors, and a clear understanding of the risks we face. To that end, EO 13636 and PPD-21 emphasizes an integrated approach to promoting critical infrastructure cybersecurity. DHS's role is to bring together all stakeholders—government officials and business leaders, security professionals and infrastructure owners and operators—to facilitate information-sharing and support adoption of standards and best practices to reduce and manage cyber risk.

Strengthening the security and resilience of critical infrastructure against growing and evolving cyber risks requires a layered approach. DHS actively collaborates with public and private sector partners every day to improve the security and resilience of critical infrastructure while responding to and mitigating the impacts of attempted disruptions to the nation's critical cyber and communications networks and to reduce adverse impacts on critical network systems. Thus, to implement the EO and PPD 21, the Federal Government has actively sought the collaboration, input and engagement of all our partners.

Cybersecurity Framework & Voluntary Program

EO 13636 directed the National Institute of Standards and Technology (NIST) to develop a Cybersecurity Framework, based on standards and industry best practices for improving cybersecurity and promoting cyber risk management. The EO also directed DHS to establish a voluntary program for critical infrastructure cybersecurity, to serve as a Federal coordination point for cybersecurity resources and support increased cyber resilience by promoting use of the Framework. The C^3 Voluntary Program is an innovative public-private partnership that is critical to DHS. DHS leads this program as part of its mission of continuing outreach and collaboration with the civilian federal government, state, local, tribal and territorial governments and private sector. C^3 helps to align critical infrastructure owners and operators with existing resources that will assist their efforts to manage their cyber risks, including through use of the Framework. The C^3 Voluntary Program also facilitates forums for knowledge sharing and collaboration. It provides access to free and readily available technical assistance, tools, and resources to strengthen capabilities to manage cyber risks, and opportunities to exchange opinions with peers and other partners in the critical infrastructure community.

As an example, one resource in the C^3 Voluntary Program is the Cyber Resilience Review, a no-cost assessment tool that helps organizations of all sizes review the strengths and weaknesses of their cyber systems through a self or facilitated risk-assessment. DHS has already facilitated more than three hundred of these assessments, helping organizations identify and address weaknesses in their systems.

Support to Partners

State, local, territorial, and tribal (SLTT) governments are some of our frontline stakeholders and can serve as a force multiplier in the national effort to protect critical infrastructure. DHS works with these partners, including through SLTT associations such as the National Association of State CIOs and the National Governors Association, to both strengthen the security and resilience of their critical networks, and better protect the public from constantly evolving cyber threats. However, due to challenging budgetary environments, states and territories often lack the resources to obtain advanced security tools. To help address this critical gap, DHS recently forged a cooperative agreement with the Center for Internet Security (CIS) Multi-State Information Sharing and Analysis Center to provide state-of-the-art managed security services to states and territories in conjunction with their use of the NIST Cybersecurity Framework. As part of this agreement, CIS will provide Managed Security Services, funded by DHS, to states and territories in 2014. These services include intrusion detection, intrusion prevention, netflow analysis and firewall monitoring – all things that support critical elements of the Framework. While states and territories must retain full authority and ownership over their networks, and manage those networks commensurate with the risk, these services, and the use of the Framework are critical tools to assist reaching that goal.

DHS is also working to promote use of the Cybersecurity Framework to other groups of entities, such as small and medium businesses (SMB). These entities store significant amounts of sensitive data, from customer information to critical intellectual property, yet may lack the education or resources to properly protect this data or critical systems they manage. Under the C^3 Voluntary Program, the Department has issued a request for information (RFI) to ask industry about the market of affordable cybersecurity solutions and the specific challenges that SMB may face in managing cyber risk. We are encouraged by the initial response from many industry stakeholders and look forward to continuing this effort.

Incentivizing Cybersecurity

While the strongest motivation for use of the Cybersecurity Framework is increased security and resilience of an entity's networks, EO 13636 also directed DHS, along with the Departments of Treasury and Commerce, to evaluate incentives to further encourage participation in the DHS Voluntary Program. This work led to the identification of eight incentive areas that are being analyzed among Federal departments and agencies as well as industry stakeholders. They include cybersecurity insurance, grants, process preferences, liability limitation, streamlined regulations, public recognition, cost recovery for regulated industries, and cybersecurity research and development. Some of the recommended areas are direct incentives, while others are indirect such as cyber insurance. Also, some can be implemented with current authorities or as part of the C^3 Voluntary Program, while others, such as liability limitation, may require legislative action.

Based on feedback from stakeholders, agencies have further defined the scope and path forward for each area. For example, based on further analysis, the cost recovery incentive area has been revised to "support for prudent cybersecurity investments and opportunities for utilities".

Independent of added incentives, DHS hopes that our partners in critical infrastructure will consider use of the Framework as an effective way to manage cyber risks consistent with their business needs. These incentives may provide helpful and positive reasons encouraging participation of in the C^3 Voluntary Program and use of the Framework to manage cyber risks.

Continuing Need for Congressional Support

While securing cyberspace has been identified as a core DHS mission since the 2010 QHSR, the Department's view of cybersecurity has evolved to include a more holistic emphasis on critical infrastructure which takes into account risks across the spectrum. In a time of constrained resources, we must ensure that our efforts achieve the highest level of security as efficiently as possible. To achieve success, however, it is vital that funding requested in the President's budget for NPPD be maintained and preserved, not only for cybersecurity programs but also those that tie in physical world security with networked systems. The Committee has always been a supportive partner in our cybersecurity efforts, including the recent confirmation of NPPD's Under Secretary Suzanne Spaulding, and I would ask that now more than ever, this support remains firm.

Furthermore, we must attract the best and brightest to DHS. We have an urgent and exciting mission. I left the private sector because I believe in what DHS can do with the current leadership in NPPD and at the top of our Department. What Government cannot always pay in money, I believe we can offer in mission and the opportunity to solve a giant but exciting problem that involves computers, people, policy and our way of life. I have visited universities with our Secretary and spoken at several student events. There is eager talent out there, and it is ours to lose. Once we attract that talent, we need to be able to hire those people and to improve our processes to not foil our recruitment efforts.

While the Nation's dependence on cyber infrastructure has grown exponentially since the Department's founding, the Administration believes the Department's statutory authorities have not kept pace with evolving technologies and reliance on cyberspace by Federal agencies and critical infrastructure. To enable DHS and other agencies to more effectively and efficiently carry out their existing responsibilities, legislative action is necessary. We ask that such legislation, aligned in principle with the Administration's 2011 legislative proposal, modernize FISMA and reflect the existing DHS role in agencies' Federal network information security policies as well as clarify existing operational responsibilities for DHS in cybersecurity.

Conclusion

Thank you for the opportunity to share with you some of our ongoing work as well as our vision for future capabilities. Our mission to secure critical infrastructure requires continuous collaboration with other Federal agencies, SLTT and private sector partners, and DHS is deeply committed to further this mission.

We will continue to work with our public and private partners to strengthen the security and resilience of our critical infrastructure. We thank the Committee for their support and look forward to building a more secure and resilient future in which cyberspace remains a catalyst for innovation, growth, and prosperity.