Statement for the Record

The Honorable Suzanne E. Spaulding
Under Secretary, National Protection and Programs Directorate

Dr. Phyllis Schneck
Deputy Under Secretary, Cybersecurity and Communications

U.S. Department of Homeland Security

Before the
United States House of Representatives
Committee on Homeland Security

Regarding

Examining the President's Cybersecurity Information Sharing Proposal

February 25, 2015

Introduction

Chairman McCaul, Ranking Member Thompson, and distinguished Members of the Committee, we are pleased to appear today to discuss the President's cybersecurity legislative proposal on information sharing.

In our testimony today, we will highlight the Department of Homeland Security (DHS) National Protection and Programs Directorate cybersecurity role and capabilities, and describe how the President's legislative proposal to facilitate cyber threat indicator information sharing will further our national security, with DHS's National Cybersecurity and Communications Integration Center (NCCIC) as the coordination center to receive and disclose cyber threat indicators to Federal and Non-Federal entities.

The Ongoing Cyber Threat and the DHS Cybersecurity Role

As a nation, we are faced with pervasive cyber threats. Malicious actors, including those at nation-state level, are motivated by a variety of reasons that include espionage, political and ideological beliefs, and financial gain. Increasingly, State, Local, Tribal and Territorial (SLTT) networks are experiencing cyber activity of a sophistication level similar to that seen on Federal networks.

To achieve our cybersecurity mission, the National Protection and Programs Directorate focuses on helping our partners understand and manage cyber risk, reduce the frequency and impact of cyber incidents, and build partner capacity. We share timely and accurate information and analysis to enable private and public sector partners to protect themselves. We provide on-site assistance to Federal agencies and critical infrastructure entities impacted by a significant cybersecurity incident. We provide technology and services to detect and block cyber threats from impacting Federal civilian networks. We enable Federal agencies to more readily identify network security issues and take prioritized action. We enable commercial cybersecurity companies to use classified information so they can better protect their private sector customers. We perform comprehensive consequence analyses that assess cross-sector interdependencies and cascading effects, including the potential for kinetic harm that includes loss of life, and we maintain a trusted environment for private sector partners to share information and collaborate on cybersecurity threats and trends.

DHS's National Cybersecurity and Communications Integration Center

The NCCIC serves as a 24x7 centralized location for the coordination and integration of cyber situational awareness and incident management. NCCIC partners include all Federal departments and agencies; state, local, tribal, and territorial governments; the private sector; and international entities. The NCCIC continues to explore opportunities to expand its liaison capacity from other agencies and the private sector. The NCCIC provides its partners with enhanced situational awareness of cybersecurity and communications incidents and risks, and provides timely information to manage vulnerabilities, threats, and incidents. In 2014, the NCCIC received over 97,000 incident reports, and issued nearly 12,000 actionable cyber-alerts or warnings. NCCIC teams also detected over 64,000 significant vulnerabilities on federal and non-federal systems and directly responded to 115 significant cyber incidents.

The NCCIC actively shares cyber threat indicators to and from multiple sources including private sector partners, the Intelligence Community, Federal Departments and Agencies, law enforcement, State, Local, Tribal and Territorial governments, and international governments. This sharing, which has been taking place for many years, takes many forms including person-to-person interactions on the NCCIC floor, manual exchange of information via e-mail and secure web portals, and more recently via automated, machine-to-machine exchanges in STIX and TAXII protocols. While all of these sharing methods have value, the cybersecurity community has recognized the strategic importance of migrating cyber threat indicator sharing to more automated mechanisms when and where appropriate.

Cybersecurity Legislation

Last year, Congress acted in a bipartisan manner to pass critical cybersecurity legislation that enhanced the ability of the Department of Homeland Security to work with the private sector and other Federal civilian departments in each of their own cybersecurity activities, and enhanced the Department's cyber workforce authorities. Enactment of these bills represents a significant moment for the Department's cybersecurity mission, and this Committee in particular undertook significant efforts to bring the bills to passage. We are thankful for your support and we are deploying those additional authorities with clarity of mission.

Additional legislation is needed. We must take additional steps to ensure that DHS is able to rapidly and efficiently deploy new protective technologies across Federal civilian agency information systems. In addition, carefully updating laws to facilitate cybersecurity information sharing within the private sector and between the private and government sectors is also essential to improving the Nation's cybersecurity. While many companies currently share cybersecurity threat information under existing laws, there is a heightening need to increase the volume and speed of information shared without sacrificing the trust of the American people or the protection of privacy, confidentiality, civil rights, or civil liberties. It is essential to ensure that cyber threat information can be shared quickly among trusted partners, including with law enforcement, so that network owners and operators can take necessary steps to block threats and avoid damage.

The NCCIC plays a critical role in the President's recent legislative proposal because its core mission – as articulated in the National Cybersecurity Protection Act, developed by this Committee and unanimously-passed by the House in December – is to coordinate and serve as an interface for cybersecurity information across the government and private sector.

The Administration's Information Sharing Proposal for Cyber Threat Indicators

Building on the bipartisan cybersecurity legislation enacted last Congress, President Obama visited the NCCIC on January 13, 2015, to announce a proposal for additional legislation to improve cybersecurity information sharing. The President noted, "Much of our critical infrastructure runs on networks connected to the Internet….[a]nd most of this infrastructure is owned and operated by the private sector. So neither government nor the private sector can defend the nation alone. It's going to have to be a shared mission – government and industry working hand in hand, as partners." This partnership entails sharing cyber threat indicators to better enable government agencies and the private sector to protect themselves.

Information sharing, especially of these technical "threat indicators" that can be used to identify and block malicious activity, is the lifeblood of effective cyber defense and response. Pulling together this information allows defenders to identify anomalies or patterns and recognize dangerous activity before it can do significant damage. The goal of the President's proposal is to increase the sharing of this type of information, as quickly as possible, with appropriate protection for privacy and of sensitive information and systems.

Among other things, the Administration's proposal would reduce the risks for private entities to voluntarily share technical cyber threat indicators with each other and the NCCIC by providing protections against civil or criminal liability for such sharing. Equally important, the proposal narrowly defines the threat indicators that will be shared, requires that irrelevant identifying information be minimized from these indicators, and generally requires strong protections for the privacy and confidentiality of personal information. Finally, the proposal calls for the creation of Information Sharing and Analysis Organizations (ISAOs). ISAOs would be information sharing organizations that would help speed information sharing within the private sector and between the private sector and government.

Our goal is to expand information sharing within the private sector, and to build on the existing relationships, processes and programs of the NCCIC to enhance cooperation between the government and private sector. The proposal will help us improve the methods that the NCCIC already uses to share cyber threat indicators, and leverage automation to achieve scalability wherever possible. We look to evolve and expand indicator sharing at the NCCIC from human exchanges, portals, and written reports to automated machine-to-machine communications. Our vision is that this may reduce the time to receive and act on indicators from hours to milliseconds, create consistency in information provided to interagency partners, law enforcement, and the private sector, and free analysts to focus on the threats that require human analysis while expediting detection and blocking of new threats.

NCCIC as the Coordination Center

Cyber threat indicators, which allow government agencies and the private sector to better protect themselves, come from a variety of sources, including: government agencies, private companies, international partners, and ISAOs. Given the variety of formats used – and information that is included – when sharing such information, the government must have a central clearinghouse to ensure that privacy and confidentiality protections are consistently applied and that the right information reaches the right government and private sector entities.

DHS is a leader within the government when it comes to the development and operational implementation of privacy, confidentiality, and civil liberties policies. DHS was the first agency to have statutorily established Officers for Privacy and for Civil Rights and Civil Liberties. From its creation, DHS has built both privacy and civil liberties protections into all of its programs and has dedicated, on-site privacy professionals committed to ensuring that its cyber mission is carried out in a way consistent with our Nation's values. Through statutory protections like Protected Critical Infrastructure Information (PCII), DHS will continue to anonymize the identity of submitters and other proprietary and sensitive information in threat indicator submissions. Moreover, the President's proposal calls for DHS to build upon its existing privacy, confidentiality, and civil liberty procedures by working with the

Attorney General to develop new procedures to appropriately limit Government receipt, use, and retention of threat indicators. Establishing the NCCIC as the primary entry way for cyber threat indicators from the private sector will ensure uniform application of these important privacy and confidentiality protections, while still allowing cyber threat indictors to be shared with law enforcement for the specific purposes identified in the legislation.

NCCIC sits at the intersection of cyber communities, with representatives from the private sector and other government entities physically present on the NCCIC floor and connected virtually. This diverse participation in the NCCIC was cemented by section 226(d) of the Homeland Security Act as added by the National Cybersecurity Protection Act. NCCIC's core mission is to enable better network defense by assessing and appropriately sharing information on the risks to America's critical cyber systems and how to reduce them.

Building Capacity to Accelerate Automated Sharing of Cyber Threat Indicators

The Administration's proposal directs DHS to automate and share information in as close to real-time as practicable with relevant federal agencies, including law enforcement entities, and with ISAOs. For the past three years, DHS has led the development in collaboration with the private sector of specifications – known as STIX and TAXII – which standardize the representation and exchange of cyber threat information, including actionable cyber threat indicators. STIX, the Structured Threat Information eXpression, is a standardized format for the representation and exchange of cyber threat information, including indicators. TAXII, the Trusted Automated eXchange of Indicator Information, is a standardized protocol for discovering and exchanging cyber threat information in STIX. The interagency Enhance Shared Situational Awareness initiative has already chosen STIX as the basis for sharing cyber threat indicators between the Federal cyber centers, ensuring interoperability between these key sources of information.

Through collaboration between DHS and the private sector, there is a solid and rapidly growing base of commercial offerings supporting STIX and sharing indicators via the TAXII, including platforms, network protection appliances and endpoint security tools. While the NCCIC has in-house systems and tools to assist analysts in generating STIX indicators, those indicators are currently analyzed and filtered by human analysts and shared back out with the private sector and Federal partners through manual methods such as e-mail and secure portals. In 2014, the NCCIC began a limited pilot with several organizations to test automated delivery of STIX indicators via TAXII.

To inform our plan for achieving automated cyber threat indicator information sharing, DHS created a working group between a range of DHS offices and the FBI, a critical stakeholder in the NCCIC. We also included experts from our Privacy, Civil Rights and Civil Liberties, and Science and Technology offices, among others, to ensure that our architecture is based on best-in-class technology and is consistent with our values and our respect for Americans' privacy and civil liberties.

Implementation will proceed through four major phases: (1) an initial operating capability phase in which we will deploy a TAXII system that can disseminate STIX cyber threat indicators with increased automation capability, enabling the use of human analysis for the most complex problems and egregious threats; (2) an expanded automation phase in which we will develop and deploy DHS infrastructure that can receive, filter, and analyze cyber threat indicators-- during this phase, we will

promulgate guidance for private sector companies to minimize, redact and tag their data prior to submission to NCCIC, and will complete a Privacy Impact Assessment; (3) a final operating capability phase in which we will fully automate DHS processes to receive and appropriately disseminate cyber threat indicators in a machine-readable format and finalize policies for filtering, receipt, retention, use, and sharing, including regular compliance reviews; and (4) a scaled services capability phase, during which DHS will work to enable agencies that lack sufficient cybersecurity resources or expertise to receive and share cyber threat indicators with the NCCIC in near-real-time by providing a turnkey technical solution to "plug in" to the NCCIC.

DHS Shares Information Widely with Federal Agencies and the Private Sector

Currently, DHS shares information with Federal Agencies and the private sector. DHS takes a customer-focused approach to information sharing, and different types of information require differing response times and dissemination protocols. DHS provides information to detect and block cybersecurity attacks on Federal civilian agencies and shares information to help critical infrastructure entities in their own protection; provides information to commercial cybersecurity companies so they can better protect their customers through the Enhanced Cybersecurity Services program, or ECS; and maintains a trusted information sharing environment for private sector partners to share information and collaborate on cybersecurity threats and trends via a program known as the Cyber Information Sharing and Collaboration Program, or CISCP. This trust derives in large part from our emphasis on privacy, confidentiality, civil rights, and civil liberties across all information sharing programs, including special care to safeguard personally identifiable information.

DHS also directly supports Federal civilian departments and agencies in developing capabilities that will improve their own cybersecurity posture. Through the Continuous Diagnostics and Mitigation (CDM) program, 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. The CDM program provides diagnostic sensors, tools, and dashboards that provide situational awareness to individual agencies, and will provide DHS with summary data to understand relative and system risk across the Executive Branch. DHS is moving aggressively to implement CDM across all Federal civilian agencies, and Memoranda of Agreement with the CDM program encompass over 97 percent of all Federal civilian personnel.

While CDM will identify vulnerabilities and systemic risks within agency networks, the National Cybersecurity Protection System, also known as EINSTEIN, detects and blocks threats at the perimeter of those networks or at an agencies' Internet Service Provider. EINSTEIN is an integrated intrusion detection, analysis, information sharing, and intrusion-prevention system. The most recent iteration, Einstein 3 Accelerated (E3a), supplements EINSTEIN 2 by adding additional intrusion prevention capabilities and enabling Internet Service Providers (ISPs), under the direction of DHS, to detect and block known or suspected cyber threats using indicators.

Conclusion

We are working together to find new and better ways to share accurate, timely data in a manner

consistent with fundamental American values of privacy, confidentiality, and civil rights. While securing cyberspace has been identified as a core DHS mission since the 2010 Quadrennial Homeland Security Review, the Department's view of cybersecurity has evolved to include a more holistic emphasis on critical infrastructure which takes into account the convergence of cyber and physical risk.

Today our adversaries exploit a fundamental asymmetry in our network infrastructure: while nearly all of our systems and networks are globally interconnected, our defensive capabilities are not. This gives the attackers a compelling advantage as they can find and exploit the weak links in our systems from anywhere around the world – at machine speed. By sharing cyber threat indicators in near real-time, we reduce that asymmetry.

As our defensive cybersecurity capabilities become more interconnected, we greatly reduce the likelihood that an adversary can re-use attack infrastructure, tools, tactics, techniques and procedures. In addition, we greatly reduce the time window in which new and novel attacks are effective because the ecosystem shares those indicators and develops a type of "herd immunity," improving defenses as indicators are shared and events are correlated in near-real-time. These two factors do not eliminate all cyber threats, but they hold the promise of significantly increasing the time and resources (both technical and human) that attackers must expend to achieve their goals. Moreover, the STIX data format and the TAXII transport method are increasingly compatible with commonly used commercial information technology (IT) products. This means more entities are able to send indicators automatically to the NCCIC, creating an ecosystem of indicators which will in turn provide greater context to malicious cyber activity and rapidly increase situational awareness per Executive Order 13636, *Improving Critical Infrastructure Cybersecurity* and Executive Order 13691, signed February 13, 2015, *Promoting Private Sector Cybersecurity Information Sharing*.

DHS will continue to serve as one of the government's primary resources for information sharing and collaborative analysis, at machine-speed wherever possible, of global cyber risks, trends, and incidents. Through our leadership role in protecting civilian government systems and helping the private sector protect itself, DHS can correlate data from diverse sources, in an anonymized and secure manner, to maximize insights and inform effective risk mitigation.

DHS provides the foundation of the U.S. government's approach to securing and ensuring the resilience of civilian critical infrastructure and essential services. We look forward to continuing the conversation and supporting the American goals of peace and stability; in these endeavors, we rely upon your continued support.

Thank you for the opportunity to testify, and we look forward to any questions you may have.