Testimony of

Andy Ozment
Assistant Secretary for Cybersecurity and Communications
National Protection and Programs Directorate

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

April 15, 2015

Introduction

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

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

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

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

Protecting the Federal Government

Across the Federal Government, each department and agency is responsible for managing its own cybersecurity. However, under the Federal Information Security Modernization Act

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

CDM: Helping Federal Agencies Understand and Manage Cyber Risk

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

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

The CDM Federal Dashboard will provide DHS with summary data to understand relative and system risk across the Executive Branch. Local agency dashboards will provide each agency with detailed information into its specific, prioritized risks. Both dashboards will use commercial off-the-shelf technology. The agency-level dashboards will begin deployment in FY 2015, and the Federal dashboard is expected to fully deploy by FY 2017.

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

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

Another tool utilized by NPPD to fulfill its mission is EINSTEIN 3 Accelerated (E^3A). E^3A is a perimeter defense tool: a first line of defense against cyber threats for Federal civilian Departments and Agencies. E^3A can be considered a set of security gates on the Federal

Government's traffic, located at the handful of Internet Service Providers (ISPs) that are used by almost every Federal civilian agency to access the Internet. DHS has completed building E^3A checkpoints at two ISPs: therefore, agencies that currently use these two ISPs to connect to the Internet are now able to obtain E^3A protection. These security gates only apply to traffic transiting to and from Federal civilian executive branch agencies. A Privacy Impact Assessment (PIA) for E^3A was published by DHS in 2013 to publicly document how privacy protections have been integrated into the E^3A process. This PIA is available through the Department's publicly-facing website.

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

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

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

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

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

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

Enhancing Information Sharing to Reduce the Frequency and Impact of Cyber Incidents

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

An example of the NCCIC's support to and collaboration with the private sector was the effort to mitigate Distributed Denial of Service (DDoS) incidents impacting U.S. banking institutions in 2012 and 2013. During the DDoS attacks, the NCCIC disseminated technical data and assistance—including 600,000 DDoS- related Internet Protocol (IP) addresses and supporting contextual information—to Federal agencies, critical infrastructure partners, international

partners, and US-based ISPs. This information helped financial institutions and cybersecurity service providers improve their defensive capabilities and detect or block threats before financial services were impacted. In addition to sharing with relevant private sector entities, the NCCIC shared information with over 120 international partners, many of whom contributed to our mitigation efforts. The NCCIC, along with the U.S. Secret Service, FBI and other interagency partners, also deployed to affected entities to offer on-site technical assistance.

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

Helping the Private Sector and SLTT Governments Manage Risk

NPPD helps the Nation's infrastructure owners and operators protect themselves by offering our customers risk assessments and assistance via the Critical Infrastructure Cyber Community (C3) Voluntary Program. NPPD assists all 16 critical infrastructure sectors with risk management activities, including supporting the use of the NIST Cybersecurity Framework for Critical Infrastructure (the Framework). NPPD is requesting additional resources in support of the Framework to allow the C^3 Voluntary Program to double the number of cybersecurity risk assessments provided to critical infrastructure owners and operators. These assessments provide critical infrastructure owners and operators with invaluable information about their cybersecurity posture in relation to the Framework, and they offer concrete areas for improvement. This budget request will extend the reach of the C^3 Voluntary Program, promote adoption of the Framework, and build the security and resilience of the nation's critical infrastructure.

Separately, NPPD is requesting $16.901 million for the Enhanced Cybersecurity Services (ECS) program. ECS has similar capabilities to E^3A. However, unlike E^3A, it is available to validated critical infrastructure companies and SLTT customers. ECS shares sensitive unclassified and classified cyber threat indicators with qualified Commercial Service Providers (CSPs) that then use that data to protect their ECS customers. All payment and contractual relationships occur between an ECS customer and their service provider devoid of any DHS involvement. The Federal Government deals directly with the CSPs and not their end customers. The Federal Government's role is limited to ensuring CSPs meet the program security requirements for receiving sensitive unclassified and classified Government Furnished Information, providing timely and vetted cyber threat information to the qualified service providers, and receiving anonymous, aggregated data back from the service providers about the number of malicious activities detected by their ECS systems. Through their respective CSPs, ECS customers can decide whether any data is shared back to the Department. The privacy and civil liberties considerations for the program are detailed in the ECS PIA available on DHS's publicly-facing website and in a Privacy and Civil Liberties assessment mandated by Executive Order 13636 and made publicly available on the DHS Privacy Office website. This budget request will fund additional cybersecurity analysts to provide new threat and network analysis, and it will expand the ECS program to an increased number of CSPs.

Congressional support

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

- The National Cybersecurity Protection Act of 2014, which provides explicit authority for DHS to provide assistance to the private sector in identifying vulnerabilities and restoring their networks following an attack, and establishes in law the NCCIC as a Federal civilian interface with the private sector.
- The Federal Information Security Modernization Act of 2014, which statutorily establishes DHS authority to administer the implementation of Federal information security policies, develop and oversee implementation of binding cybersecurity directives, provide technical assistance to other agencies through US-CERT, and deploy cybersecurity technology to other agencies upon their request.
- Two bills that help DHS continue to recruit, hire, and retain the best and brightest cybersecurity workforce. In FY 2016, NPPD is requesting $16.238 million to support cybersecurity pay reform as part of DHS' efforts to improve its cybersecurity workforce.
- Separately, apart from our cybersecurity authorities, a four-year authorization for the Chemical Facility Anti-Terrorism Standards (CFATS) program, which significantly improves our ability to work with the private sector on security at high-risk chemical facilities.

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