Statement for the Record

Dr. Andy Ozment
Assistant Secretary, Cybersecurity and Communications
U.S. Department of Homeland Security

Before the
United States House of Representatives
Committee on Homeland Security
Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies

Regarding
Emerging Threats and Technologies to Protect the Homeland

February 12, 2015

Introduction

Chairman Ratcliffe, Ranking Member Richmond, and distinguished Members of the Subcommittee, I am pleased to appear today to discuss the work of the Department of Homeland Security (DHS) to address persistent and emerging cyber threats to the U.S. homeland.

In my testimony today, I would like to highlight how DHS helps secure cyber infrastructure and discuss a few specific examples of instances in which we prevented and responded to a serious cybersecurity challenge.

The Ongoing Cyber Threat

Growing cyber threats are an increasing risk to critical infrastructure, our economy and thus, our national security. As a nation, we are faced with pervasive threats from malicious cyber actors. These individuals are motivated by a variety of reasons that include espionage, political and ideological beliefs, and financial gain. Certain nation-states pose a significant cyber threat as they aggressively target and seek access to public and private sector computer networks with the goal of stealing and exploiting massive quantities of data.

Some nation-states consistently target Government networks for traditional espionage, theft of protected information for financial gain, and other purposes. Increasingly, State, Local, Tribal and Territorial (SLTT) networks are experiencing nation-state cyber activity similar to that seen on Federal networks. In addition to targeting government networks, there is a growing threat of nation-states targeting and compromising critical infrastructure networks and systems. Such attacks may provide persistent access for potential malicious cyber operations that could lead to cascading effects with physical implications, including injury or loss of life.

DHS Cybersecurity Role

The DHS National Protection and Programs Directorate (NPPD) undertakes its cybersecurity activities within its overarching mission to secure and enhance the resilience of the Nation's critical infrastructure. By leveraging its core capabilities of information and data sharing; incident response and capacity development; vulnerability assessments; and situational awareness, NPPD applies its expertise and resources to assist with building the Nation's resilience to physical and cybersecurity risks.

NPPD works with infrastructure owners and operators and government partners, to provide timely information, analysis, and assessments through its field force and headquarters components. These capabilities are applied to maintain and provide situational awareness, increase resilience, and understand and mitigate risk. Through established partnerships including DHS support from partners in Science & Technology, US Secret Service, and the Domestic Nuclear Detection Office, NPPD leads the national unity of effort for infrastructure security and resilience and builds the capacity of partners across the Nation. NPPD also directly protects Federal infrastructure against both physical and cyber threats and responds to incidents that threaten infrastructure or sensitive information.

NPPD executes this mission through several key responsibilities:

- *First, NPPD informs decision-makers on potential impacts by performing comprehensive consequence analyses that assess cross-sector interdependencies and cascading effects.* NPPD utilizes integrated analysis and modeling capabilities to understand cyber and physical risk and assist with prioritization of infrastructure to ensure resources are focused on protecting the assets or services of greatest significance. This capability also enables NPPD to maintain and provide situational awareness to public and private sector partners about the potential impacts of future incidents and inform investments of various forms in effective preparedness given limited resources.
- *Second, NPPD reduces cyber and physical risks to critical infrastructure through collaboration with Federal agencies, state, local, tribal, and territorial governments and the private sector.* NPPD works with its partners to conduct voluntary critical infrastructure and cybersecurity assessments. These assessments allow partners to better understand their physical and cyber security resilience and vulnerabilities and provide recommendations for how they can improve. At the national level, NPPD leads or contributes to the development of risk management plans and approaches such as the National Infrastructure Protection Plan and the Cybersecurity Framework.
- *Third, NPPD programs promote cybersecurity knowledge and innovation to create a safer and more secure cyber environment.* NPPD enables Federal departments and agencies to address cybersecurity challenges by providing guidance on technology, emerging risks, and best practices. To this end, NPPD partners with the private sector, law enforcement, military, and intelligence communities to identify and mitigate vulnerabilities and threats to information systems before they can cause significant harm.
- *Fourth, NPPD provides direct protection and conducts incident response activities to minimize the frequency and impact of incidents affecting Federal networks and facilities.* NPPD secures and protects the buildings, grounds, and property owned or occupied by the Federal Government, as well as the people on those properties, by conducting Facility Security Assessments, recommending appropriate countermeasures, overseeing a large contract Protective Security Officer workforce, and exercising law enforcement authorities. On the cyber side, NPPD directly protects Federal networks by identifying vulnerabilities through the Continuous Diagnostics and Mitigation (CDM) program and by detecting and blocking threats through the EINSTEIN program. NPPD also responds to cyber incidents affecting Federal networks upon request of the impacted agencies to determine and recommend necessary mitigations.
- *Fifth, NPPD is responsible for ensuring effective telecommunications for government users in national emergencies and for establishing policies and promoting solutions for interoperable emergency communications used on a daily basis across the country at the Federal, State, and local levels.* As the Sector Specific Agency for Communications and for Emergency Services, NPPD protects and strengthens the security, reliability, survivability, and interoperability of the Nation's communications capabilities at the Federal, State, local, tribal, and territorial levels. NPPD serves the first responder community by serving as a board member and providing technical assistance for the initiative to establish a National Public Safety Broadband Network and supports development of standards and best practices for the interoperability of first responder communications. NPPD is also helping lead the transition of public safety

communications from land-mobile radio to broadband and Voice-Over-Internet Protocol (or VOIP). In order to ensure that communications are available to manage and coordinate a major incident, NPPD also assures the provision of National Security and Emergency Preparedness communications by administering the Priority Telecommunications Service (PTS).

DHS Shares Information Widely with Federal Agencies and the Private Sector, and Provides Incident Response

DHS takes a customer-focused approach to information sharing, using information to detect and block cybersecurity attacks on Federal civilian agencies and sharing information to help critical infrastructure entities in their own protection. We provide information to commercial cybersecurity companies so they can better protect their customers through the Enhanced Cybersecurity Services program, or ECS, and we maintain 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 maintains the National Cybersecurity & Communications Integration Center (NCCIC), which 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 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 vulnerabilities on federal and non-federal systems and directly responded to 115 significant cyber incidents.

Protecting Federal Civilian Cyber Infrastructure

DHS 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. NPPD is moving aggressively to implement CDM across all Federal civilian agencies. Memoranda of Agreement with the CDM program encompass over 97 percent of all Federal civilian personnel. An initial award of CDM tools in 2014 to fill immediate capability gaps at participating agencies,

will, in the future, provide DHS with better data to protect the dot gov, and has resulted in $26 million in cost avoidance. The President's 2016 Budget requests $102.7 million for the CDM program. 2015 will be an exciting year for the CDM program: acquisition Groups A and B, covering 7 agencies and over 45% of all federal civilian personnel, will begin to deploy CDM tools starting in the third quarter of Fiscal Year 2015. By the first quarter of Fiscal Year 2016, 25 agencies and over 95% of all federal civilian personnel will have started deploying CDM tools provided by DHS. NPPD is implementing a commercial off-the-shelf, or COTS, technology for the CDM dashboard to provide agencies with a detailed understanding of their cybersecurity risk and enable comprehensive situational awareness across the federal government. The agency-level dashboards will begin deployment in FY15, and the Federal dashboard is expected to reach Full Operating Capability in FY17.

While CDM will identify vulnerabilities and systemic risks within agency networks, the National Cybersecurity Protection System, or EINSTEIN, detects and blocks threats at the perimeter of the network or at the Internet Service Provider. EINSTEIN is an integrated intrusion detection, analysis, information sharing, and intrusion-prevention system. The President's 2016 Budget requests $463.9 million for the EINSTEIN program. Perhaps the best way to understand EINSTEIN is through the analogy of a car attempting to enter a protected perimeter such as a military base. EINSTEIN 1 can be thought of as analogous to a cop on the beat looking for a particular license plate. The system captures key data about Internet traffic entering an agency through basic network flow information. EINSTEIN 2 is akin to a cop who not only sees the license plate but sends an alert to other security personnel to alert them to a potentially prohibited or malicious vehicle. EINSTEIN 2's network intrusion detection system (IDS) technology uses custom signatures, based upon known or suspected cyber threats within federal network traffic. EINSTEIN 3A, or E^3A, is much like a gatehouse that prohibits vehicles whose license plates set off an alert from entering the base. E3A supplements EINSTEIN 2 by adding additional intrusion prevention capabilities and enabling ISPs, under the direction of DHS, to detect and block known or suspected cyber threats using indicators.

NPPD's Office of Cybersecurity and Communications (CS&C) screens all data captured by EINSTEIN1 and EINSTEIN2 sensors to ensure it is analytically relevant to a known or suspected cyber threat. E3A combines existing analysis of EINSTEIN 1 and EINSTEIN 2 data as well as information provided by cyber mission partners with existing commercial intrusion prevention security services to allow for the near real-time deep packet inspection of federal network traffic to identify and react to known or suspected cyber threats. Participating agencies currently have access to their network flow records through participation in EINSTEIN 1 and receive information about their own data specific to their networks in accordance with CS&C's cybersecurity information handling policies and guidelines. E3A is currently deployed and offering DNS and email services to eleven (11) departments and agencies, covering approximately 25% of all dot-gov (.gov) traffic. Forty-six (46) agencies have signed Memorandum of Agreements (MOA) to participate in E3A services covering 90% of all federal civilian traffic. It reduces threat vectors available to actors seeking to infiltrate, control, or harm Federal networks. We look forward to working with Congress to further clarify DHS's authority to deploy this protective technology to Federal civilian systems.

Securing the Homeland Against Persistent And Emerging Cyber Threats

Cyber intrusions into critical infrastructure and government networks can cause significant damage and be perpetrated by increasingly sophisticated actors. The complexity of emerging threat capabilities, the inextricable link between the physical and cyber domains, and the diversity of cyber actors present challenges to DHS and our customers.

Financial Sector Distributed Denial of Service (DDoS) Attacks

Cyber attacks on the U.S. financial sector are often discussed as an area of concern. There were increasingly powerful DDoS incidents impacting leading U.S. banking institutions in 2012 and 2013, and high-profile media coverage of financial sector cybersecurity challenges in 2014. US-CERT has a distinct role in responding to a DDoS: to disseminate victim and potential victim notifications to United States Federal Agencies, Critical Infrastructure Partners, International CERTs, and US-based Internet Service Providers.

US-CERT has provided technical data and assistance, including identifying 600,000 DDoS-related IP addresses and supporting contextual information. This information helps financial institutions and their information technology security service providers improve defensive capabilities. In addition to sharing with relevant private sector entities, US-CERT provided this information to over 120 international partners, many of whom contributed to our mitigation efforts. US-CERT, along with the U.S. Secret Service, FBI and other interagency partners, also deployed to affected entities on-site technical assistance, or "boots on the ground." US-CERT works with Federal civilian agencies to protect USG systems from becoming part of a botnet, since botnets are a tool that cyber criminals use to deflect attribution in DDoS attacks.

During these attacks, our partners in the DHS Office of Intelligence and Analysis, or I&A, provided long-term, consistent threat updates to the Department of Treasury and private-sector partners in the Financial Services Sector. I&A analysts presented sector-specific unclassified briefings on the relevant threat intelligence, including at the annual Financial Services Information Sharing and Analysis Center (FS-ISAC) conference, alongside the Office of the National Counterintelligence Executive and the U.S. Secret Service. At the request of the Treasury and the Financial and Banking Information Infrastructure Committee (FBIIC), I&A analysts provided classified briefings on the malicious cyber threat actors to cleared individuals and groups from several financial regulators, including the Federal Deposit Insurance Corporation (FDIC), Securities and Exchange Commission (SEC), and the Federal Reserve Board (FRB).

Point of Sale Compromises

On December 19, 2013, a major retailer publically 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 (CVV) security codes. The CVV security codes are three or four digit numbers that are usually on the back of the card. Separately, another retailer also reported a malware incident involving its Point of Sale (POS) system on January 11, 2014, that resulted in

the apparent compromise of credit card and payment information.

In response to this activity, NCCIC/US-CERT analyzed malware identified by the Secret Service 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 products tailored to specific audiences.

These efforts ensured that actionable details associated with a major cyber incident were shared with the private sector partners who needed the information in order to protect themselves and their customers quickly and accurately, while also providing individuals with practical recommendations for mitigating the risk associated with the compromise of their personal information. NCCIC especially benefited from close coordination with the private sector Financial Services Information Sharing and Analysis Center during this response.

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. Enactment of these bills represents a significant moment for the Department's cybersecurity mission, and I thank Congress for this action. This Committee in particular undertook significant efforts to bring the bills to passage.

Additional legislation is needed. While many companies currently share cybersecurity threat information under existing laws, there is a heightening need to increase the volume and speed of such information sharing between the government and the private sector – and among appropriate private sector organizations – without sacrificing the trust of the American people or individual privacy, civil rights, or civil liberties. It is also essential that we ensure the integration of threat indicators to provide shared situational awareness. We must connect the dots. Carefully updating laws to facilitate cybersecurity information sharing is essential to improving the Nation's cybersecurity. We also must provide law enforcement additional tools to fight crime in the digital age, create a National Data Breach Reporting requirement, and further clarify DHS's authority to deploy protective technologies to Federal, Executive Branch, civilian systems.

Conclusion

DHS will continue to work with our public and private partners to create and implement collaborative solutions to improve cybersecurity, focused on reducing frequency and impact of high-consequence cybersecurity incidents. We work around the clock to ensure that the peace and security of the American way of life will not be interrupted by malicious actors seeking to exploit our reliance on the Internet and networked technologies. Each incarnation of the cyber

threat has unique traits, and mitigation requires agility and layered security. Cybersecurity is a process of risk management in a time of constrained resources, and we must ensure that our efforts achieve maximize security as efficiently as possible while preserving privacy, civil rights, and civil liberties.

DHS represents an integral piece of the national effort to increase our collective cybersecurity, but we cannot achieve our mission without a foundation of voluntary partnerships with the critical infrastructure community, industry, and our government partners. 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.

DHS will continue to serve as the center of integration, information sharing, and collaborative analysis, at machine-speed wherever possible, of global cyber risks, trends, and incidents. Through our unique role in protecting civilian government systems and helping the private sector protect themselves, DHS can correlate data from diverse sources, in an anonymized and secure manner, to maximize insights and inform effective risk mitigation. We are working to further mature the ability of NCCIC to receive information at machine speed, which will support emerging capabilities of networks to self-heal and to recognize and block threats before they reach their targets. This will in turn diminish the profit model for cyber adversaries and reduce our response time to a cyber incident from days or hours to seconds.

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 continuing to serve the American goals of peace and stability, and we rely upon your continued support. Thank you for the opportunity to testify, and I look forward to any questions you may have.