Statement for the Record

Dr. Phyllis Schneck
Deputy Undersecretary for Cybersecurity
National Protection and Programs Directorate
U.S. Department of Homeland Security

“Cybersecurity: Enhancing Coordination to Protect the Financial Sector”

Before the
United States Senate
Committee on Banking, Housing and Urban Affairs
Washington, DC

December 10, 2014

Introduction

Chairman Johnson, Ranking Member Crapo, and distinguished Members of the Committee, I am pleased to appear today to discuss the work of the Department of Homeland Security (DHS) National Protection and Programs Directorate (NPPD) to address persistent and emerging cyber threats to the U.S. homeland.

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*. These set out steps to strengthen the security and resilience of the Nation's critical infrastructure. They reflect the increasing importance of integrating cybersecurity efforts with traditional critical infrastructure protection. The President highlighted the importance of government's role in encouraging innovation and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties. DHS partners closely with owners and operators to improve cybersecurity information sharing and encourage implementation of risk-based standards in order to meet the President's objectives.

In my testimony today, I would like to highlight how DHS helps secure cyber infrastructure and then discuss a few specific examples where we prevented and responded to a variety of cybersecurity challenges.

DHS Cybersecurity Role

Based on our statutory and policy requirements, DHS undertakes three broad areas of responsibility in cybersecurity: (1) we coordinate the national protection, prevention, mitigation, response and recovery in the event of significant cyber and communications incidents; (2) we disseminate domestic cyber threat and vulnerability analyses across critical infrastructure sectors; (3) we investigate cybercrime that falls under DHS's jurisdiction.

DHS components actively involved in cybersecurity include NPPD, the United States Secret Service, the U.S. Coast Guard, U.S. Customs and Border Protection, Immigration and Customs Enforcement, the DHS Office of the Chief Information Officer, the DHS Science and Technology Directorate, and the DHS Office of Intelligence and Analysis (I&A), among others. In all of its activities, DHS coordinates its cybersecurity efforts with governmental, private sector, and international partners.

The DHS National Cybersecurity & Communications Integration Center (NCCIC) is a 24-7 cyber situational awareness and incident response and management center that serves as a centralized location for the coordination and integration of operational elements involved in cybersecurity and communications reliability. NCCIC partners include all federal departments and agencies; state, local, tribal, and territorial governments (SLTT); the private sector; and international entities. The Center provides greater situational awareness of cybersecurity and communications, and takes actions to address vulnerabilities, intrusions, and incidents, including mitigation, information-sharing, and recovery.

The NCCIC is composed of the United States Computer Emergency Readiness Team (US-CERT), the Industrial Control System Cyber Emergency Response Team (ICS-CERT), the National Coordination Center for Communications (NCC), and an Operations and Integration Team. NCCIC operations are currently conducted from three states: Virginia, Idaho, and Florida. During the first eleven months of 2014, the NCCIC has had 108,734 incidents reported to the center, issued over 11,514 actionable cyber-alerts, and had over 219,805 partners subscribe to our cyber threat warning sharing initiative. NCCIC teams have also detected over 87,797 vulnerabilities and directly aided in the mitigation of near 53,624 unique challenges.

Enhancing the Security of Cyber Infrastructure

The NCCIC actively collaborates with public and private sector partners every day, including responding to and mitigating the impacts of attempted disruptions to the Nation's critical cyber and communications networks. DHS also directly supports federal civilian departments and agencies in developing capabilities that will improve their own cybersecurity postures. 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. The CDM program provides diagnostic sensors, tools, and dashboards that provide situational awareness to individual agencies and at a summary federal level. Memoranda of Agreement between government entities and DHS to provide the CDM program's services encompass network security protection for over 97 percent of all federal civilian personnel.

The National Cybersecurity Protection System (NCPS) complements these efforts. A key component of NCPS is referred to as EINSTEIN, an integrated intrusion detection, analysis, information sharing, and intrusion-prevention system. EINSTEIN utilizes hardware, software, and other components to support DHS's protection of Federal civilian agency networks. The program will expand intrusion prevention, information sharing, and cyber analytic capabilities at Federal agencies. EINSTEIN 3 Accelerated (E^3A) gives DHS an active role in defending .gov network traffic. At this time, E^3A provides Domain Name System and/or email protection services to thirty-three departments and agencies. It reduces threat vectors available to actors seeking to infiltrate, control, or harm Federal networks.

Securing the Homeland Against Persistent And Emerging Cyber Threats

Cyber intrusions into critical infrastructure and government networks are serious and sophisticated threats. 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. As the private sector owns and operates over 85% of the Nation's critical infrastructure, information sharing and capability development partnership becomes especially critical between the public and private sectors.

Financial Sector Distributed Denial of Service (DDoS) Attacks

The continued stability of the U.S. financial sector is often discussed as an area of concern, as U.S. banks are consistent targets of cyber-attacks. There have been increasingly powerful DDoS incidents impacting leading U.S. banking institutions in 2012 and 2013 and some high-profile media coverage of financial sector cybersecurity issues in 2014. US-CERT has a distinct role in responding to a DDoS: to disseminate 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 about the source of the attacks, the identity of the attacker, or other associated details. 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 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 ensure that no USG systems are vulnerable to take-over as a part of a botnet, since botnets are a tool that cybercriminals use to deflect attribution in DDoS attacks.

During these attacks, our I&A partners bolstered long-term, consistent threat engagements with 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). Additionally our Science & Technology organization coordinates priority R&D programs in collaboration with the Financial Services Sector Coordinating Council.

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 security codes. The value 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 the 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 publically available and can be found on US-CERT’s website, provides a non-technical overview of risks to POS 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.

Preparing for the Next Cyber Incident

DHS is taking a number of proactive measures to strengthen its partnerships with the financial sector and increase shared understanding of one another's capabilities and cybersecurity response plans and procedures. These efforts include regularly exercising incident response procedures together with interagency and private sector representatives; working collaboratively with financial sector representatives to clarify and streamline processes when requesting technical assistance from the government; identifying barriers to information sharing and ways to reduce those barriers; and implementing automated information sharing between the financial services sector and government by expanding the use of Structured Threat Information eXpression (STIX) and Trusted Automated eXchange of Indicator Information (TAXII) programs, a free method for machine-to-machine sharing of cyber threat indicators.

Also of significant note is our vision and direction moving forward to create broad situational awareness of cyber threats and disseminate warning information ahead of malicious attacks. We recognize the need to change the profit model in cybercrime by making networks more resilient and less appealing and rewarding for adversarial attack or intrusion. Just as the human body achieves resilience by fighting new viruses with biological mechanisms that recognize when the body is under attack, DHS is enabling similar mechanisms for networks using mathematical trend analysis of cyber events. We collect the data needed for this from the government agencies that we protect, with full collaboration from our privacy and civil liberties experts, and are creating a cyber "Weather Map," to help visualize and inform current cyber conditions. 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 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 that resilience to deter many cyber threat actors.

DHS also recognizes that effective incident response requires plenty of practice and close cooperation across government and with the private sector. To prepare for and ensure effective cooperation during a significant event, DHS, in close coordination with the Department of the Treasury, private sector representatives, financial sector regulatory bodies and other federal government partners, has instituted an exercise program to periodically test processes and procedures for responding to a significant cyber incident impacting the financial sector. The exercises help clarify roles and responsibilities, identify gaps in response plans and capabilities, and assist with developing plans to address those gaps. The exercises result in valuable lessons learned and will help improve existing processes and procedures and result in more effective cooperation during an actual incident.

DHS Cybersecurity Authorities

We continue to seek legislation that clarifies and strengthens DHS responsibilities and allows us to respond quickly to vulnerabilities like Heartbleed, a vulnerability in the popular OpenSSL cryptographic software library. Legislative action is vital to ensuring the Department has the tools it needs to carry out its mission. DHS had to go "door to door" securing authorization from federal entities to exercise our authority in responding to Heartbleed. We urge Congress to continue efforts to modernize the Federal Information Security Management Act to reflect the existing DHS role in agencies' Federal network information security policies; clarify existing operational responsibilities for DHS in cybersecurity by authorizing the NCCIC; and provide DHS with hiring and other workforce authorities.

Conclusion

DHS will continue to work with our public and private partners to create collaborative solutions to improve cybersecurity, particularly those that reduce the likelihood of the highest-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 degradation of systems or by opportunist, enemy, or terrorist actors. Each incarnation of threat has some 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 the highest level of security as efficiently as possible.

DHS represents an integral piece of the national work in cybersecurity: we are building a foundation of voluntary partnerships with private owners of critical infrastructure and government partners working together to safeguard stability. 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 risks across the board.

The Department stands to be the core of integration and joint analysis, by machines and by humans, of global cyber behavior, trends, malware analysis and the powerful combination of data that only we can correlate due to our unique role protecting civilian government systems with data that often only the private sector gathers. We are working to further enable the NCCIC to receive information at "machine speed."[1] This capability will begin to enable networks to be more self-healing, as they use mathematics and analytics to better recognize and block threats

[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.

before they reach their targets, thus deflating the profit model of cyber adversaries and taking botnet response from hours to seconds in some cases.

DHS forms a crucial underpinning for ensuring the ongoing protection of our infrastructures, services and way of life. 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.