Testimony of

Larry Zelvin
National Cybersecurity and Communications Integration Center Director
National Protection and Programs Directorate
U.S. Department of Homeland Security

Before the
United States House of Representatives
Committee on Homeland Security
Subcommittee on Counterterrorism and Intelligence and Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies
Washington, D.C.

May 21, 2014

Introduction

Chairman King, Chairman Meehan, Ranking Member Higgins, Ranking Member Clarke, and distinguished Members of the Committee, I am pleased to appear today to discuss the Department of Homeland Security (DHS) National Protection and Programs Directorate (NPPD) and the National Cybersecurity and Communications Integration Center (NCCIC) efforts to assess 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*, which set out steps to strengthen the security and resilience of the Nation's critical infrastructure, and reflect the increasing importance of integrating cybersecurity efforts with traditional critical infrastructure protection. The President also highlighted that it is important for government to encourage efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties. DHS partners closely with critical infrastructure owners and operators to improve cybersecurity information sharing and encourage risk-based implementation of standards and guidelines in order to strengthen critical infrastructure security and resilience.

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

Enhancing the Security of Cyber Infrastructure

Based on our statutory authorities, and in response to policy requirements, DHS coordinates the national protection, prevention, mitigation of, and recovery from significant cyber and communications incidents; disseminates domestic cyber threat and vulnerability analysis across various sectors; and investigates cybercrimes under DHS's jurisdiction. DHS has a unique responsibility in securing federal civilian systems against all threats and hazards. 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, and the DHS Office of Intelligence and Analysis (I&A), among others. In all of its activities, DHS coordinates all of its cybersecurity efforts with public, private sector, and international partners.

The DHS National Cybersecurity & Communications Integration Center (NCCIC) is a 24x7 cyber situational awareness and incident response and management center that serves as a centralized location where operational elements involved in cybersecurity and communications reliance coordinate and integrate cyber security efforts. NCCIC partners include all federal departments and agencies; state, local, tribal, and territorial governments (SLTT); the private sector; and international entities. NCCIC's activities include providing greater understanding of cybersecurity and communications vulnerabilities, intrusions, incidents, mitigation, and recovery actions. 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 seven months of Fiscal Year (FY) 2014, the NCCIC has received 31,593 reports of incidents, detected over 28,000 vulnerabilities, issued over 4,006 actionable cyber-alerts, and had over 252,523 partners subscribe to our cyber threat warning sharing initiative.

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. In FY 2014 so far, the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) has provided over 161 alerts, bulletins, and other products to the ICS community warning of various threats and vulnerabilities impacting control systems, tracked 85 unique vulnerabilities affecting ICS products, conducted 41 assessments across critical infrastructure sectors, and deployed the Cyber Security Evaluation Tool to 2,412 critical infrastructure owners and operators to assist in performing their own cybersecurity self-assessments against known control systems standards.

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, 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 actions for these issues based on potential consequences or likelihood of exploitation by adversaries. The CDM program provides diagnostic sensors, tools, and dashboards that provide situational awareness to individual agencies, as well as general situational awareness at the federal level. Memoranda of Agreement with the CDM program encompass over 97 percent of all federal civilian personnel.

Complementing these efforts, the National Cybersecurity Protection System (NCPS), a key component of which is referred to as EINSTEIN, is an integrated intrusion detection, analysis, information sharing, and intrusion-prevention system, utilizing hardware, software, and other components to support DHS's mandate to protect Federal civilian agency networks. In FY 2014 and beyond, the program will expand intrusion prevention, information sharing, and cyber analytic capabilities at Federal agencies. EINSTEIN 3 Accelerated (E^3A) currently provides Domain Name System and/or email protection services to a total of seven departments and agencies, and we are working with our service providers to bring coverage to the rest of the executive branch. However, this process has been significantly delayed by the lack of clear authorities for DHS. E^3A gives DHS an active role in defending .gov network traffic and significantly reduces the threat vectors available to malicious actors seeking to 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 all of our customers. Because the private sector owns and operates a significant percentage of the Nation's critical infrastructure, information sharing becomes especially critical between the public and private sectors.

Heartbleed

The Department recently learned of a serious vulnerability, known as "Heartbleed," a weakness in the widely-used OpenSSL encryption software that protects the electronic traffic across two-thirds of the Internet and in scores of electronic devices. Although new computer "bugs" and malware crop up almost daily, this vulnerability is unusual in how widespread it is, the potentially damaging information it allows malicious actors to obtain, and the length of time before it was discovered.

NCCIC learned of the of the Heartbleed vulnerability on April 7, 2014. Less than 24 hours later, NCCIC released alert and mitigation information on the US-CERT website. In close coordination with the Departments of Defense and Justice, as well as private sector partners, the NCCIC then created a number of compromise detection signatures for the EINSTEIN system that were also shared with additional critical infrastructure partners. DHS worked with civilian agencies to scan their .gov websites and networks for Heartbleed vulnerabilities, and provided technical assistance for issues of concern identified through this process. The NCCIC and its components also began a highly active outreach to cyber researchers, critical infrastructure owners, operators, and vendors, federal, and SLTT entities, and international partners to discuss measures to mitigate the vulnerability and determine if there had been active exploits.

Once in place, DHS began notifying agencies that EINSTEIN signatures had detected possible activity, and immediately provided mitigation guidance and technical assistance.

The Administration's May 2011 Cybersecurity Legislative Proposal called for Congress to provide DHS with clear statutory authority to carry out this operational mission, while reinforcing the fundamental responsibilities of individual agencies to secure their networks, and preserving the policy and budgetary coordination oversight of the Office of Management and Budget and the Executive Office of the President. While there was rapid and coordinated Federal government response to Heartbleed, the lack of clear and updated laws reflecting the roles and responsibilities of civilian network security caused unnecessary delays in the incident response.

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 (i.e., the three or four digit numbers that are usually on the back of the card). Separately, another retailer 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 shared through non-public, secure channels with industry partners to enable their protection efforts. When possible, NCCIC's goal is always to share information broadly, including by producing products tailored to specific audiences.

These efforts ensured that actionable details associated with a major cyber incident were shared quickly and accurately with the private sector partners who needed the information in order to protect themselves and their customers, 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 (FS-ISAC) during this response.

Energy Sector

In March 2012, DHS identified a campaign of cyber intrusions targeting natural gas pipeline sector companies with spear-phishing e-mails that dated back to December 2011. The attacks were highly targeted, tightly focused and well crafted.

ICS-CERT kicked off an "Action Campaign" in partnership with the Federal Bureau of Investigation, Department of Energy (DOE), Electricity Sector –Information Sharing and Analysis Centers, Transportation Security Administration, and others to provide classified briefings to private sector critical infrastructure organizations across the country. In May and June 2012, DHS deployed onsite assistance to two of the organizations targeted in this campaign: an energy company that operates a gas pipeline in the U.S. and a manufacturing company that specializes in producing materials for pipeline construction. ICS-CERT and the Federal Bureau of Investigation (FBI) provided 14 briefings in major cities throughout the United States to over 750 personnel involved in the protection of energy assets and critical infrastructure.

ICS-CERT, in coordination with DOE and the Federal Energy Regulatory Commission (FERC), has also started an initiative dubbed "SAFEGUARD" to assess the cybersecurity of major energy sector asset owners (e.g., electric and gas utilities, petroleum companies) to proactively understand the state of security. Customized services include cybersecurity assessments, network architecture reviews, network scanning to look for static indicators and indicators of adversary persistence and anomalies, and control systems network traffic visualization.

Our I&A colleagues have increased outreach to the Energy Sector, providing expertise on malicious capabilities and intentions of emerging cyber threat actors targeting the sector, including in unclassified forums. I&A leveraged partnerships with DHS and other Federal experts, including colleagues at DOE, to provide threat briefings to CEOs, CIOs, CISOs, and other private and public sector leaders. These included engagements with the leadership and members of the American Petroleum Institute, alongside NPPD partners and National Security Staff colleagues, and a joint briefing with the FBI to the Federal Energy Regulatory Commission.

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. DDoS incidents impacting leading U.S. banking institutions in 2012 and 2013 and periodically in 2014 have gotten more powerful as the DDoS campaign has persisted. 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 in order to help financial institutions and their information technology security service providers improve their defensive capabilities. In addition to sharing with the relevant private sector entities, US-CERT has provided this information to over 120 international partners, many of whom have contributed to our mitigation efforts. US-CERT, along with the FBI and other interagency partners, has also deployed on-site technical assistance to provide in-person support. US-CERT works with federal civilian agencies to ensure that no U.S. Government systems are infected with botnet software that launches DDoS attacks andto increase the U.S. Government's domestic and international sharing and coordination efforts with public and private sector partners.

During these attacks, our I&A partners bolstered long-term and consistent threat engagements with the Department of Treasury and private sector partners throughout the Financial Services Sector. I&A analysts presented numerous sector-specific unclassified briefings on the relevant threat intelligence, including at the annual FS-ISAC conference, alongside the Office of the National Counterintelligence Executive and the U.S. Secret Service. Additionally, 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).

Conclusion

DHS is committed to creating a safe, secure, and resilient cyber environment while promoting cybersecurity knowledge and innovation and protecting confidentiality, privacy, and civil liberties in collaboration with our public, private, and international partners. We work around the clock to ensure that the peace and security of the American way of life will not be interrupted by opportunist enemies or terrorist actors. Each incarnation of threat has some unique traits. Mitigation requires agility and adaptation. Cybersecurity is not an end-state, but a continuous process of risk management.

We continue to believe that carefully crafted information sharing provisions, as part of a comprehensive suite of cybersecurity legislation, are essential to improving the Nation's cybersecurity, and we will continue to work with Congress and the White House to achieve this objective. We continue to seek legislation that clarifies and strengthens DHS responsibilities and allows us to respond quickly to vulnerabilities like Heartbleed. We continue to seek legislation that incorporates privacy, civil liberties and confidentiality safeguards into all aspects of cybersecurity; strengthens our critical infrastructure's cybersecurity by further increasing information sharing and promoting the adoption of cybersecurity standards and guidelines; gives law enforcement additional tools to fight crime in the digital age; and creates a National Data Breach Reporting requirement.

DHS plays an integral role in promoting national cybersecurity: we are building a foundation of voluntary partnerships with private owners of critical infrastructure and government partners working together to safeguard stability. We form a crucial underpinning for ensuring the ongoing continuation of services. We work through information-sharing, threat and indicator technical tools, sector-specific outreach, on-site technical assistance, education and awareness campaigns, and other mechanisms—in other words, we use a multidimensional approach that provides layered security. We look forward to continuing the conversation and continuing to serve the American goals of peace and stability, and we hope for your continued support.