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
Energy and Commerce Committee
Subcommittee on Commerce, Manufacturing and Trade

February 5, 2014

Introduction

Chairman Terry, Ranking Member Schakowsky, and distinguished Members of the Committee, I am here today to discuss the Department of Homeland Security's (DHS) roles in responding to the recently reported breach of point of sale (POS) systems at two major retailers and the apparent compromise of sensitive personal and financial information that resulted from those breaches. I will also put these actions in the context of DHS's responsibilities to deal with cyber threats to our Nation's financial transaction systems as well as other important elements of critical infrastructure.

During the recent POS system compromises, DHS's National Protection and Program Directorate's (NPPD) strong operational and private sector outreach programs were leveraged to help other retailers secure their systems to prevent future attacks while simultaneously supporting the United States Secret Service's (Secret Service) criminal investigation. The National Cybersecurity and Communications Integration Center (NCCIC) used its unique cybersecurity analysis and mitigation capabilities to coordinate efforts to secure systems against future attacks and provided timely analysis for the Secret Service. Through close coordination among DHS components and other partners, we have not only preserved the integrity of the Secret Service law enforcement investigation, we have provided businesses and users the key information they need to protect themselves and reduce the likelihood of a similar incident occurring in the future.

Today I'd like to review in greater detail how NPPD works daily with our colleagues at the Secret Service and with interagency and cross sector partners to respond to and mitigate this and other cyber incidents. I hope this overview will demonstrate the increasing importance of building and maintaining close relationships between law enforcement officials and network defense experts in order to address both the criminal aspects of malicious cyber activity, as well as to reduce continuing vulnerabilities, protect against future attacks, and mitigate consequences of incidents. The importance of effectively leveraging these complementary missions has been consistently demonstrated over the last several years, and is an increasingly important part of the broader framework used by the government and the private sector to cooperate responding to malicious cyber activity.

A Whole of Nation Approach to Cybersecurity

As the Department has highlighted in previous testimony, cyberspace is woven into the fabric of our daily lives. According to recent estimates, the Internet encompasses more than two billion people with at least 12 billion computers and devices, including global positioning systems, mobile phones, satellites, data routers, ordinary desktop computers, and industrial control systems that run the power plants, water systems, and much more that make up our nation's critical infrastructure. While this increased connectivity has led to significant transformations and advances across our country – and around the world – it also has increased complexity and exposes us to new vulnerabilities that can only be addressed by timely action and shared responsibility. The Nation's economic vitality and national security depend on a safe cyberspace where reasonable risk decisions can be made and the flow of digital goods, transactions, and online interactions can occur safely and securely. No country, industry, community or individual is immune to the threat of a cyber-attack and timely action is required to share necessary information in order to discover, address, and mitigate the ever-growing threat of malicious cyber activity.

Furthermore, no single agency or organization by itself can effectively respond to the rising threat of malicious cyber activity. Now, more than ever, there is a need for a civilian-government capability to engage not only with affected entities but with other critical infrastructure sectors and companies that also are at risk. Successful responses to dynamic cyber intrusions require coordination among DHS, the Department of Justice—including the Federal Bureau of Investigation, Criminal Division, National Security Division, and U.S. Attorneys' Offices—the Intelligence Community, the Department of State, the specialized expertise of Sector Specific Agencies such as the Department of the Treasury, private sector partners – who are critical to these efforts – and state, local, tribal and territorial, as well as international partners, each of which have unique roles to play. In carrying out these activities, NPPD promotes and implements a unified approach to cybersecurity incident response, which enables the efforts of a diverse set of partners. Our incident response activities are synchronized with the comprehensive and timely sharing of cybersecurity information, and done in a manner which ensures the protection of individuals' privacy, civil rights and civil liberties.

The Central Role of the National Cybersecurity and Communications Integration Center

To better manage and facilitate cybersecurity information sharing efforts, analysis, and incident response activities, exemplified by the recent retailer breach, the Department operates the National Cybersecurity and Communications Integration Center (NCCIC), an around-the-clock center where key government, private sector, and international partners all work together. The NCCIC is comprised of four branches: the United States Computer Emergency Readiness Team (US-CERT), the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), the National Coordinating Center (NCC) for Communications, and Operations Integration (O&I). These branches provide the capabilities, skills, knowledge, and partnerships needed to serve as a focal point for coordinating cybersecurity information sharing with the private sector; provide technical assistance, onsite analysis, mitigation support, and assessment assistance to cyber-attack victims; and coordinate the National response to significant cyber incidents affecting critical infrastructure.

While responding to the recent retailer compromises, the NCCIC specifically leveraged the resources and capabilities of US-CERT. US-CERT's global partnerships allow it to work directly with analysts from across multiple sectors and international borders to develop a comprehensive picture of malicious cyber activity and mitigation options. US-CERT's mission focuses specifically on computer network defense, and it is able to apply its full resources to supporting prevention, protection, mitigation, response, and recovery efforts. US-CERT publishes technical and non-technical information products assessing the characteristics of malicious cyber activity and improving the ability of organizations and individuals to reduce their risk.

US-CERT's unique ability to aggregate, analyze, and share diverse sets of information from law enforcement, the intelligence community, the private sector – including information sharing and analysis centers – and international partners through more than 200 CERT partnerships worldwide is critical to NCCIC's information sharing mission. Increasingly, our information sharing activities are undertaken using Structured Threat Information Expression (STIX), which allows for data to be shared at machine speed in a standard, machine readable format.

Current Threat Landscape and Recent Retail Company Targeting

The NCCIC currently sees malicious cyber activity perpetrated by a variety of actors who employ diverse methods to achieve their objectives.

For some time, cyber criminals have been targeting consumer data entered into POS systems. When consumers purchase goods or services from a retailer, the transaction is processed through POS systems, which consist of the hardware (e.g. the equipment used to swipe a credit or debit card and the computer or mobile device attached to it) as well as the software that tells the hardware what to do with the information it captures. When consumers use a credit or debit card at a POS system, the information stored on the magnetic stripe of the card is collected and processed by the attached computer or device.

The data stored on the magnetic stripe is referred to as "Track One" and "Track Two" data. Track One data is personal information associated with the account. Track Two data contains information such as the credit card number and expiration date. In some circumstances, criminals attach a physical device to the POS system to collect card data, which is referred to as "skimming". In other cases, cyber criminals deliver malware which acquires card data as it passes through a POS system, eventually exfiltrating the desired data back to the criminal.

POS systems are connected to computers or devices, and are often enabled to access the Internet and email services. Malicious links or attachments in emails as well as malicious websites can be accessed and malware may subsequently be downloaded by an end user of a POS system.

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. Another retailer also reported a malware incident involving its POS system on January 11, 2014, that resulted in the apparent compromise of credit

card and payment information. A direct connection between these two incidents has not been established.

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 Financial Services Information Sharing and Analysis Center during this response.

Ensuring Robust Privacy and Civil Rights and Civil Liberties Safeguards

Throughout our response to the retailer breaches we followed pre-existing protocols and control measures to protect personally identifiable information (PII) and other sensitive information that could cause harm to individuals or the critical infrastructure entities we provide assistance to. Our top level approach is to minimize the collection, retention, dissemination or use of PII, and other sensitive information that is not relevant to the cyber threat. There are also more detailed standards for handling specific types of information within specific programs and activities, tailored to the specific programs, the types of information handled and the mission requirements.

DHS remains committed to ensuring cyberspace is supported by a secure and resilient infrastructure that enables open communication, innovation, and prosperity while protecting privacy, confidentiality, and civil rights and civil liberties by design.

Public Outreach

It is important to note that the NCCIC is only one part of NPPD's overall effort to create a more secure cyberspace through working with private and public sector partners. NPPD continues to build its capabilities and our relationships by reinforcing the Department's Stop.Think.Connect.™ public awareness campaign, which is a year-round national effort designed to engage and challenge Americans to join the effort to practice and promote safe online practices. The Stop.Think.Connect.™ Campaign, launched during National Cyber Security Awareness Month in October 2010, helps Americans understand and manage the risks that come with living in a connected world. NPPD also works closely with the Secret Service Electronic Crimes Task Forces, leveraging their public/private partnerships, and works closely with other Federal agencies, including Sector Specific Agencies, to share cybersecurity

information with critical infrastructure owners and operators. We are aggressively pursuing the objectives of the Executive Order 13636, Improving Critical Infrastructure Cybersecurity, and Presidential Policy Directive 21, Critical Infrastructure Security and Resilience, to increase the quality, quantity and breadth of public/private sector information sharing, while remaining vigilant on privacy and civil liberties protections. This includes development of the EO 13636-directed voluntary program to support adoption of the NIST Cybersecurity Framework, by owners and operators of critical infrastructure and any other interested entities.

Conclusion

While the Secret Service's criminal investigation into the these activities is on-going, NPPD through the NCCIC and other organizations continues to build shared situational awareness of similar threats among our private sector and government partners and the American public at large. At every opportunity, the NCCIC and our private sector outreach program publish technical and non-technical products on best practices for protecting businesses and customers against cyber threats and provide the information sharing and technical assistance necessary to address cyber threats as quickly as possible.

Increased connectivity has led to significant transformations and advances across our country – and around the world. Our daily lives, economic vitality, and national security depend on the cyberspace. DHS, through NPPD programs and partnerships, including the NCCIC and its central role, is working to outpace the cyber threat in order to maintain security and thereby foster innovation that has resulted from this interconnectedness. I appreciate the opportunity to speak with you today about the progress that the NCCIC has made in response to an ever evolving cyber threat and the road ahead for future improvements to our nation's cybersecurity.