William Noonan

Deputy Special Agent in Charge
Criminal Investigative Division
United States Secret Service

Prepared Testimony

Before the
Committee on Appropriations
Subcommittee on Homeland Security
United States Senate

"Investing in Cybersecurity: Understanding Risks and Building Capabilities for the Future"

May 7, 2014

Good afternoon Chairman Landrieu, Ranking Member Coats, and distinguished Members of the Subcommittee. I appreciate the opportunity to testify on the investments the Department of Homeland Security (DHS) is making in cybersecurity, and the capabilities the Secret Service has and is developing to deter cyber-crime around the world. I am honored to appear today alongside my colleagues from Immigration and Customs Enforcement (ICE) and the National Protection and Programs Directorate (NPPD). While no single agency or department has the personnel and resources to eliminate cyber-threats, DHS brings to the table a strong combination of federal law enforcement experience, established partnerships with the Department of Defense, the Department of Justice (DOJ), state and local governments, international law enforcement and the private sector, as well as a workforce committed to strengthening the security and resiliency of our nation's critical infrastructure.

Cyber-threats impact all aspects of the Secret Service's integrated mission. When the agency was created as an investigative arm of the Department of Treasury in 1865, its purpose was to protect the nation's financial system from the proliferation of counterfeit currency. No one at the time could have foreseen that the Secret Service would one day be responsible for the protection of the President of the United States, let alone that protection would have to take into account the potential for computers to affect physical security. Likewise, no one at the time could have foreseen that financial crimes would encompass computer-based attacks on our nation's financial services sector and would regularly include criminal actors working across international borders to perpetrate complex thefts and money laundering schemes.

The Secret Service traces its investigations into cyber-crime back nearly 30 years, when Congress authored 18 U.S.C. §§ 1029 and 1030 as part of enacting the Comprehensive Crime Control Act of 1984 (P.L. 98-473). That law granted the Secret Service authority to investigate criminal offenses[1] related to the unauthorized access to computers[2] and the fraudulent use, or trafficking of, access devices[3]—defined as any piece of information or tangible item that is a means of account access that can be used to obtain money, goods, services, or other thing of value.[4] As the nation's financial payment systems evolved from paper to plastic to electronic transactions, so too has the Secret Service's investigative priorities. Advances in computer technology and greater access to personally identifiable information (PII), including sensitive financial data, via the Internet have created online marketplaces for transnational cyber-criminals to share stolen information and criminal methodologies.

Over the past four years alone, Secret Service cyber-crime investigations have resulted in over 4,900 arrests, associated with approximately $1.37 billion in fraud losses and the prevention of over $11.24 billion in potential fraud losses. Through continued work with our key partners at DOJ, in particular the local U.S. Attorney's Offices, the Computer Crime and Intellectual Property Section (CCIPS), and the International Organized Crime Intelligence and Operations Center (IOC-2), we are confident we will continue to bring cyber-criminals to justice.

[1] *See* 18 USC § 1029(d) & 1030(d)(1)
[2] *See* 18 USC § 1030
[3] *See* 18 USC § 1029
[4] *See* 18 USC § 1029(e)(1)

Since 2010, in support of the Secret Service's protective mission, special agents trained through the agency's Critical Systems Protection (CSP) program successfully completed more than 657 domestic and five international protective advances. The incorporation of tools and specialized training to reduce the risks associated with a viable cyber-threat during protective operations enhances the Secret Service's ability to provide complete protective coverage at venues visited by the President, Vice President and other Secret Service protectees.

CSP technology provides visibility into the once unknown cyber-environment, which gives the Secret Service the ability to identify cyber-threat actors, as well as mitigate the potential impact of a network attack on a protective venue or on the critical infrastructure that supports the venue. CSP-trained special agents also lead the Critical Infrastructure Protection Subcommittee during National Special Security Events (NSSEs). Through their work with federal, state and local law enforcement, along with the private sector, CSP-trained special agents develop a comprehensive operational security plan to safeguard critical infrastructure and key resources associated with protective events and associated venues.

Based on the Secret Service's three decades of experience investigating cyber-crime, in particular the expertise we have developed with respect to the transnational organized cyber-crime threat to our nation, as well as our more recent efforts to protect the President, Vice President, and NSSEs from a cyber-threat, I hope to provide the Subcommittee useful information on how best to deter and mitigate the threat of these crimes in the future.

The Transnational Cyber-crime Threat

Over the past ten years, the Secret Service has observed a marked increase in the quality, quantity, and complexity of cyber-crimes targeting private industry, in particular the financial services sector. These crimes include network intrusions, hacking attacks, installation of malicious software, and account takeovers leading to significant data breaches affecting every sector of the world economy. The widely reported data breaches of Target, Neiman Marcus, White Lodging, and Michael's are just the most recent, well-publicized examples of this decade-long trend of major data breaches perpetrated by cyber-criminals who are intent on targeting our nation's banks and financial payment systems.

In partnership with the Secret Service, Verizon published their most recent Data Breach Investigations Report (Verizon Report) in 2014 to examine current trends and criminal tactics used to conduct data breaches. The analysis included in the 2014 Verizon Report covered more than 63,000 security incidents, including 1,367 confirmed data breaches occurring in calendar year 2013. The report identified three primary motives for the criminals committing these acts: (1) financial gain; (2) espionage; and (3) activism.

Cyber-criminals, motivated by greed, perpetrated the majority of the breaches studied each of the past five years through the Verizon Reports. These criminals primarily use a combination of sophisticated hacking techniques and the deployment of malicious software to accomplish their objective of obtaining sensitive financial information to use as part of increasingly sophisticated frauds. The victims of the crimes studied in the 2014 Verizon Report span 95 different countries, with 34 percent of all reported incidents affecting financial institutions. The study revealed that point-of-sale (POS) intrusions, like the recently reported events, are primarily attributed to

organized criminal groups operating out of Eastern Europe. More concerning, in 88 percent of POS intrusions, the data is exfiltrated in a matter of minutes. However, in 98 percent of the breaches it took weeks or months to discover the crime.

The increasing level of collaboration among cyber-criminals allows them to compartmentalize their operations, greatly increasing the sophistication of their criminal endeavors as they develop specialized skills to carry out cyber-attacks against the nation's financial and other critical infrastructures. These specialties increase both the complexity of investigating these cases, as well as the level of potential harm to companies and individuals. For example, illicit underground cyber-crime marketplaces allow criminals to buy, sell and trade malicious software, access to sensitive networks, spamming services, payment card data, PII, bank account information, brokerage account information, hacking services, and counterfeit identity documents. These illicit digital marketplaces vary in size, with some of the more popular sites boasting membership of approximately 80,000 users. Within these digital marketplaces, criminals often use various digital currencies to conduct transactions, such as paying for stolen information, requesting various criminal services, or laundering illicit proceeds.

As a part of our cyber-crime investigations, the Secret Service targets the most capable cyber-criminals and the individuals who operate illicit infrastructure that supports transnational organized cyber-criminals. For example, in May 2013, as part of a joint investigation through the Global Illicit Financial Team, the Secret Service shut down the digital currency provider Liberty Reserve. Liberty Reserve is alleged to have had more than one million users worldwide and to have laundered more than $6 billion in criminal proceeds. This case is believed to be the largest money laundering case ever prosecuted in the United States and is being jointly prosecuted by the U.S. Attorney's Office for the Southern District of New York and DOJ's Asset Forfeiture and Money Laundering Section. In a coordinated action with the Department of the Treasury, Liberty Reserve was identified as a financial institution of primary money laundering concern under Section 311 of the USA PATRIOT Act (P.L. 107-56), effectively cutting it off from the U.S. financial system.

The Secret Service has successfully investigated many underground cyber-criminal marketplaces. In one such infiltration, the Secret Service initiated and conducted a three-year investigation that led to the indictment of 11 perpetrators allegedly involved in hacking nine major American retailers and the theft and sale of more than 40 million credit and debit card numbers. The investigation revealed that individuals from the United States, Estonia, China and Belarus successfully obtained credit and debit card numbers by hacking into the wireless computer networks of major retailers — including TJ Maxx, BJ's Wholesale Club, Office Max, Boston Market, Barnes & Noble, Sports Authority and Dave & Buster's. Once inside the networks, those individuals installed "sniffer" programs[5] that would capture card numbers, as well as password and account information, as that information moved through the retailers' credit and debit processing networks.

After the data were collected, the alleged conspirators concealed the information in encrypted computer servers they controlled in the United States and Eastern Europe. The credit and debit

[5] Sniffers are programs that detect particular information transiting computer networks, and can be used by criminals to acquire sensitive information from computer systems.

card numbers were then sold through online transactions to other criminals in the United States and Eastern Europe. The accounts associated with the stolen numbers were "cashed out" by encoding card numbers on the magnetic strips of blank cards. The alleged perpetrators then used these fraudulent cards to withdraw tens of thousands of dollars at a time from ATMs. The illegal proceeds were allegedly concealed and laundered by using anonymous Internet-based digital currencies within the United States and abroad, and by channeling funds through bank accounts in Eastern Europe.[6]

The impact of these criminal acts extends well beyond the companies compromised, potentially affecting millions of people. Cyber-crime directly impacts the our economy by requiring additional investment in implementing enhanced security measures, inflicting reputational damage on American companies, and dealing with the financial losses from fraud—all costs that are ultimately passed on to consumers. Proactive and swift law enforcement action protects consumers by preventing and limiting the fraudulent use of payment card data, stolen PII, or both.

Cyber Investigations

The Secret Service proactively investigates cyber-crime using a variety of investigative means to infiltrate transnational cyber-criminal groups. As a result of these proactive investigations, the Secret Service is often the first to learn of planned or ongoing data breaches and is quick to notify financial institutions and the victim companies with actionable information to mitigate the damage from the data breach and terminate the criminal's unauthorized access to their networks. One of the most poorly understood facts regarding data breaches is that it is rarely the victim company that first discovers the criminal's unauthorized access to their network; rather it is law enforcement, financial institutions, or other third parties that identify and notify the likely victim company of the data breach by identifying the common point of origin of the sensitive data being trafficked in cyber-crime marketplaces.

When the Secret Service identifies a potential network intrusion, the agency contacts the owner of the suspected compromised computer system in order to assess the data breach and to stop the continued theft of sensitive information and the exploitation of their networks. After the victim of a data breach confirms that unauthorized access to their networks has occurred, the Secret Service works with the local U.S. Attorney's office, or appropriate state and local officials, to begin a criminal investigation into the matter.

During the course of these criminal investigations, the Secret Service identifies the malware and means of access used to acquire data from the victim's computer network. In order to enable other companies to mitigate their cyber-risk based on current cyber-crime methods, we quickly share information concerning the cybersecurity incident with the widest audience possible, while protecting grand jury information, the integrity of ongoing criminal investigations, and the

[6] Additional information on the criminal use of digital currencies can be referenced in testimony provided by U.S. Secret Service Special Agent in Charge Edward Lowery before the Senate Homeland Security and Governmental Affairs Committee in a hearing titled, "Beyond Silk Road: Potential Risks, Threats, and Promises of Virtual Currencies" (November 18, 2013).

victims' privacy and confidentiality. The Secret Service shares this cybersecurity information through:

- DHS's National Cybersecurity & Communications Integration Center (NCCIC);
- The Information Sharing and Analysis Centers (ISACs);
- The public, private, and academic partnerships established through our Electronic Crimes Task Forces (ECTFs);
- The publication of joint industry notices; and
- Contributions to leading industry and academic reports like the Verizon Report, the Trustwave Global Security Report, and the Carnegie Mellon CERT Insider Threat Study.

As we share cybersecurity information discovered in the course of our criminal investigations, we also continue our pursuit of the individuals responsible for the crimes. Due to the inherent challenges in investigating transnational crime, particularly the lack of cooperation of some countries with law enforcement investigations, it can take years to apprehend the top tier criminals responsible for cyber-crimes.

Collaboration with Other Federal Agencies and International Law Enforcement

While cyber-criminals operate in a world without borders, the law enforcement community does not. The transnational nature of cyber-crime cases has increased the time and resources needed for successful investigation, arrest and adjudication. The partnerships developed through our ECTFs, the support provided by our Criminal Investigative Division, the liaison established by our 24 international offices, and the training provided to our special agents via the Electronic Crimes Special Agent Program (ECSAP) are all instrumental to the Secret Service's success in these investigations.

To strengthen our ability to investigate transnational cyber-crime, the Secret Service maintains ECTFs in London and Rome, has assigned agents to INTERPOL and EUROPOL, and operates cyber-crime working groups in the Netherlands, Estonia, Lithuania, Latvia, Ukraine, and Germany. The Secret Service also trains numerous international partners on investigating cyber-crime; in the past three years, the Secret Service has trained over 500 law enforcement officials representing over 90 countries in investigating cyber-crimes.

The Secret Service's investigations of transnational crime are facilitated by the dedicated efforts of both the Department of State and the DOJ's Office of International Affairs to execute Mutual Legal Assistance Treaties and other forms of international law enforcement cooperation, in addition to the relationships that develop between Secret Service agents and their foreign counterparts through the above-mentioned working groups and training efforts.

Within DHS, the Secret Service benefits from a close relationship with ICE's Homeland Security Investigations (ICE-HSI). Since 1997, the Secret Service, ICE-HSI (and its predecessor organization, the U.S. Customs Service), and the Internal Revenue Service have jointly trained on computer investigations through ECSAP. ICE-HSI is also a member of Secret Service ECTFs, and has been a valued partner on numerous cyber-crime investigations including the recent take down of the aforementioned digital currency, Liberty Reserve.

To further its cybersecurity information sharing efforts, the Secret Service also has a strong relationship with NPPD, including DHS's NCCIC. As the Secret Service identifies malware, suspicious IP addresses and other information through its criminal investigations, it shares information with the NCCIC which pushes actionable information out to the broader cybersecurity community to protect their systems from harm. The Secret Service continues to build upon its full-time presence at NCCIC to coordinate its cyber programs with other federal agencies. In addition to the close partnership with the NCCIC, the Secret Service also has an effective relationship with NPPD's Protective Security Advisors (PSAs) and Cyber Security Advisors in advancement of our cyber protection activities. Currently, 66 percent of all PSAs are co-located in Secret Service field offices around the country.

Cyber Protection

The Secret Service is world-renowned for the physical protection it provides to the President and Vice President, visiting foreign heads of state and government, the White House and other protected sites, and NSSEs. In order to ensure a secure environment for our protectees, the Secret Service integrates a variety of innovative technologies and maintains a highly skilled workforce.

The Secret Service's protective mission is comprehensive and goes well beyond surrounding a protectee with well-trained special agents and Uniformed Division officers. Over the years, the agency's protective methodologies have become more sophisticated, incorporating such tools as airspace interdiction systems, and enhanced chemical, biological, radiological, and nuclear (CBRN) detection systems through the Operational Mission Support program. As part of the Secret Service's continuous goal of preventing an incident before it occurs, the agency relies on meticulous advance work and threat assessments to identify potential risks to our protectees. Since much of our nation's critical infrastructure is becoming increasingly interdependent, the threat of a cyber-attack directed toward our protective interests cannot be ignored.

The Secret Service's CSP program identifies, assesses, and mitigates risk posed by information systems to persons and facilities protected by the Secret Service. The program supports a full spectrum of protective operations to include domestic and foreign trips, as well as NSSEs. It accomplishes its mission in support of the Presidential, Vice Presidential and Dignitary Protective Divisions by assessing the level of risk caused by the disruption, damage or destruction of process control systems critical to an event or venue. The CSP program implements preventative, detective, and corrective controls to reduce risk from a viable cyber-threat during protective operations. The result is situational awareness of the overall cyber-security environment during protective operations.

For example, since 2012, the Secret Service has deployed cyber protection tools in support of seven of the sixteen DHS designated critical infrastructure sectors. Most recently, during the 2014 State of the Union Address (SOTU), the Secret Service deployed its cybersecurity protection platform to defend critical infrastructure and key resources in the National Capital Region.

Investments in Cybersecurity

The President's FY 2015 budget request for DHS includes $1.25 billion in discretionary spending for cybersecurity activities. The Secret Service's budget request accounts for $100.4 million, or roughly 8 percent of the total amount requested. The majority of this funding is requested under Domestic Field Operations to support the staffing associated with Secret Service cyber-crime investigations; training for our state and local law enforcement partners through the National Computer Forensics Institute (NCFI); training for special agents through ECSAP; and funding for the operational costs associated with our ECTFs. Within the amount requested, funding is also proposed to enhance the CSP program through the Cyber Security Presidential Protection Measures (CSPPM) program; support the staffing associated with international cyber-crime investigations; and continue the upgrades necessary to protect Secret Service data and systems from intrusion or intercept through the multi-year Information Integration and Technology Transformation (IITT) program. For the purposes of today's hearing, I would like to highlight a few of these efforts in more detail:

Cyber Protection Activities

The President's FY 2015 budget request includes a total of $21.3 million for cyber protection, which primarily supports the staffing associated with this activity. Within this amount, the request also includes $3.9 million to enhance the Secret Service's cyber protection capabilities through the CSPPM program. This will enable the Secret Service to train an additional 24 special agents in the ECSAP network intrusion discipline. This training is a prerequisite for special agents to advance to the CSP program to fulfill mission critical assignments in cyber protection. The CSPPM request also includes funding to enhance the CSP's cybersecurity protection platform to improve cyber-resiliency at Secret Service protective venues, including those associated with NSSEs.

National Computer Forensics Institute

The President's FY 2015 budget request includes $4 million for the NCFI, which will enable the Secret Service to train approximately 500 state and local law enforcement officers, prosecutors, and judges on current trends in cybersecurity and the potential obstacles they are likely to encounter during the course of their investigations. Located in Hoover, AL, the NCFI offers state and local law enforcement officers and prosecutors the training necessary to perform computer forensics examinations, respond to network intrusion incidents, and conduct electronic crimes investigations, while judges receive general education in these areas.

Since opening in 2008, the institute has held over 150 cyber investigative and digital forensics courses in 16 separate subjects and trained and equipped more than 3,000 state and local officials, including more than 2,300 police investigators, 840 prosecutors, and 230 judges from all 50 states and three U.S. territories. These NCFI graduates represent more than 1,000 agencies nationwide.

Electronic Crimes Task Forces/Electronic Crimes Special Agent Program

The President's FY 2015 budget request includes $1.8 million for the training and operational costs associated with the Secret Service's ECTF and ECSAP programs. The requested amount in FY 2015 will support equipment purchases and travel expenses for ECTF and ECSAP personnel. In addition to these base funds, the Secret Service usesTreasury Executive Office of Asset Forfeiture (TEOAF) funding to support the ECTF and ECSAP programs.

The Secret Service currently operates 35 ECTFs, including two based overseas in Rome, Italy, and London, England. Membership in our ECTFs includes over 4,000 private sector partners; 2,500 international, federal, state and local law enforcement partners; and 350 academic partners. By joining a Secret Service ECTF, our partners benefit from the resources, information, expertise and advanced research provided by our international network of members while focusing on issues with significant regional impact. For example, the New York ECTF, based in the nation's largest banking center, focuses heavily on safeguarding our financial institutions and infrastructure, while the Houston ECTF works closely with partners such as ExxonMobil, Chevron, Shell, and Marathon Oil to protect the nation's vital energy sector.

Conclusion

Safeguarding and securing cyberspace is a top priority for DHS. As part of that effort, the Secret Service is steadfast in its commitment to protect the President, Vice President, and NSSEs from the threat of cyber-attack, and to protect the nation's financial payment systems by investigating and dismantling transnational criminal organizations involved in cyber-crime. Responding to the growth in these types of crimes, and the level of sophistication these criminals employ, requires significant resources and greater collaboration between law enforcement and its public and private sector partners. Accordingly, the Secret Service is focused on improving our protective and investigative capabilities and techniques, enhancing the training of our special agent workforce through ECSAP, providing training for our state and local law enforcement partners through the NCFI, sharing information with our partners and private industry through DHS's NCCIC while actively investigating cases though our ECTFs, and raising public awareness to deter and mitigate the cyber-threats our nation faces today.