DECEMBER 10, 2014

CYBERSECURITY: ENHANCING COORDINATION TO PROTECT THE FINANCIAL SECTOR

U.S. SENATE, COMMITTEE ON BANKING, HOUSING AND URBAN AFFAIRS

ONE HUNDRED AND THIRTEENTH CONGRESS, FIRST SESSION

HEARING CONTENTS:

COMPILED FROM:

http://www.banking.senate.gov/public/index.cfm?FuseAction=Hearings.Hearing&Hearing_ID=1632c6b0-843f-4b9b-9df2-0a5322324070

** Please note: Any external links included in this compilation were functional at its creation but are not maintained thereafter.*

JOHNSON HOLDS HEARING ON CYBERSECURITY

December 10, 2014

WASHINGTON – Today, Senate Banking Committee Chairman Tim Johnson (D-SD) held a hearing titled "Cybersecurity: Enhancing Coordination to Protect the Financial Sector."

Below is Chairman Johnson's statement as prepared for delivery:

I call this hearing to order.

For my last hearing as Banking Committee Chairman, I am focusing on an issue that will require action in the next Congress and beyond.

Responsible management of cyber risks by financial institutions is important for consumer protection, financial stability, privacy, and national security. Not only are financial institutions frequent targets of cyber crime, they are uniquely interconnected with major sectors of the economy. Cyberattacks may cause damage to the financial system without directly attacking a bank, including through third party providers.

Earlier this year, I held a hearing on the role of financial regulators in ensuring that institutions protect consumer information. Since then, we have seen one of the biggest data breaches in history at JPMorgan. We must ensure that consumers have confidence in the financial system, and that hard work is done by industry and government together to prevent data breaches before they occur and respond quickly and in coordination when breaches do occur.

However, data breach is only one piece of the cybersecurity puzzle. That is why Ranking Member Crapo and I asked federal and state banking regulators and Treasury to provide information about each agency's protection of our financial system from cyberattacks. I am entering each agency's response into the record and I expect the regulators' continued vigilance on cybersecurity.

Safeguarding cyberspace has become increasingly complex as our lives become more entwined with technology. Technological innovation in financial services, such as mobile payments, peer-to-peer lending, and cloud computing, can facilitate improvements in the consumer experience and economic growth. However, these innovations highlight the crucial need for sound cybersecurity policy, as many of these products are outside of the regulated financial sector.

I have asked today's witnesses to discuss each of their roles in responding to cyber threats and how to improve information sharing. Law enforcement, the intelligence community, Treasury, and financial regulators each may have different missions, but in addressing cybersecurity concerns they all must be united in what some call a "whole government" approach. I look forward to hearing more about cross-sector risks to the financial system, challenges facing small

financial institutions, and how effective your partnerships with the private sector have been in improving cybersecurity practices.

Cybersecurity is one of the most important issues facing the financial system. I urge all of the witnesses today, as well as policymakers in the next Congress, to act quickly to address cybersecurity concerns.

Before I turn to Ranking Member Crapo for the last time, I want to say one more time to him and his staff: Thank you for being such good partners as we sought to run our committee in a civil, bipartisan way. To my other colleagues on this Committee, it has been a pleasure working with all of you over many years.

I now turn to Senator Crapo for his opening statement.

CRAPO STATEMENT AT CYBERSECURITY HEARING

December 10, 2014

WASHINGTON – U.S. Senator Mike Crapo (R-Idaho), Ranking Member of the Senate Banking, Housing and Urban Affairs Committee, today delivered the following remarks during a Banking Committee hearing

Thank you, Mr. Chairman. This morning, we are holding what may be the final Banking Committee hearing chaired by Chairman Johnson.

Mr. Chairman, let me reiterate what a pleasure it has been to work with you. You and I have had a great working relationship for many years. It has been a privilege to serve with you in the Senate, on this Committee and as Chairman and Ranking Member for the past two years, and I wish you the best of luck in the future.

Today, we have gathered to discuss cybersecurity in the financial sector. A "60 Minutes" segment that aired last week called 2014 "the year of the data breach." One recent study estimated that sixty percent of companies overall have experienced a breach in the last two years. This includes a number of high-profile breaches in which hackers have stolen personal and financial information from millions of consumers.

These breaches can result in frustrating experiences for consumers, including obtaining new credit or debit cards, monitoring accounts for fraudulent activity and the disruption of pre-authorized payments. Additionally, financial institutions, especially community banks and credit unions, face significant costs in reissuing cards and covering losses.

The financial sector itself is also a primary target for hackers because, as some have pointed out, "that's where the money is." The largest banks are under constant attack every day and spend hundreds of millions of dollars per year on cyber defense. What many may not realize is that the cost of defending against cyber attacks is remarkably disproportionate compared to the cost of attacking.

Hackers can purchase tools to exploit vulnerabilities for a just few hundred dollars, while firms must spend upwards of a million dollars or more to defend against specific cyber attacks. The costs and burdens on smaller financial institutions to defend against attacks can be enormous. JP Morgan Chase, the nation's largest bank by assets, was attacked this summer, when hackers stole personal information from 76 million households and 7 million small businesses. While this is certainly concerning, I am encouraged that despite spending weeks inside JP Morgan's systems, the criminals reportedly were unable to steal any financial account information.

Maintaining a strong perimeter defense is one essential component of cybersecurity; minimizing damage if hackers get inside is another. The impact of a major cyber attack against our financial

system would be dire; in the words of Treasury Secretary Lew, "successful attacks on our financial system would compromise market confidence, jeopardize the integrity of data and pose a threat to financial stability."

Many of your agencies have made cybersecurity a priority, and I applaud you for doing so. In addition, the financial industry has devoted substantial resources to protecting its information systems, and is widely viewed as one of the most advanced sectors in terms of prioritizing cybersecurity. Today, I hope to learn more about how the federal government is partnering with industry to ensure that our financial system is protected from cyber threats.

What is the government's process for obtaining threat information and delivering it to the private sector? How can we improve this process to get the information where it needs to go more quickly?

It is good that cybersecurity is getting attention from so many different agencies and offices and working groups. While positive steps are being taken, we must make sure the process has not become so complicated that it slows down the outflow of information and hinders coordination. Law enforcement, the Departments of Treasury and Homeland Security, the Intelligence Community and banking regulators must all work together effectively to maximize the speed of information sharing and to minimize the risk of and damage from cyber attacks. I also hope to learn about the work being done by the FFIEC's cybersecurity working group, and how that will inform exam procedures and policies moving forward.

Thank you, Mr. Chairman, for holding this hearing, and I look forward to hearing testimony from each of the witnesses.

*****EMBARGOED FOR DELIVERY*****

U.S. Senate Committee on Banking, Housing, and Urban Affairs
Hearing on Cyber Security - December 9, 2014
Director Brian Peretti

Prepared Testimony

Chairman Johnson, Ranking Member Crapo, and distinguished Members of the Committee, it is a pleasure to appear before you today to discuss the cybersecurity of the financial sector. As Director of Treasury's Office of Critical Infrastructure Protection and Compliance Policy (OCIP), my role is to support the security and resiliency of the critical virtual and physical infrastructure that enables financial sector operations, and cybersecurity has been a central focus of our office for several years.

Over this time, I've seen cybersecurity questions that were once thought of as a "back office" information technology issue now take center stage among senior government leaders, business executives, and the Nation as a whole. I believe this shift reflects the increasingly sophisticated and persistent nature of the cyber threat, which most would say is among the most pressing operational risks that financial institutions face today.

Before I begin, I would like to thank the Committee for focusing attention on this critical issue. At all levels, government and the financial sector have taken significant steps in recent years to enhance information sharing processes, improve baseline security at firms, and develop and test processes for responding to and recovering from incidents. More work is needed, however, and discussions like this can help advance the whole-of-nation, collaborative effort that is needed to respond to these very complex challenges.

History of Treasury's Role

Helping to protect financial sector critical infrastructure from physical and virtual threats is an integral component of Treasury's leadership in financial affairs domestically and globally.

In recent decades, and specifically since the publication of Presidential Decision Directive (PDD) 63 in 1998, Treasury has served as the lead Executive Branch agency liaison with the financial sector for national and homeland security purposes, supporting a national effort to assure the security of the United States' critical infrastructure. Since the early days of this effort, we have recognized that this work absolutely cannot be done without strong collaboration with the private sector, who, as you know, own and operate the bulk of the infrastructure we are discussing. Along these lines, one of Treasury's early efforts in this space was to support the creation and development of the Financial Services Information Sharing and Analysis Center (FS-ISAC) in 1999, which continues to be an important focal point for cross sector collaboration on these issues.

Following the attacks of September 11, Treasury established OCIP, was made chair of the newly formed Financial and Banking Information Infrastructure Committee (FBIIC), and engaged again with industry and government partners to encourage the establishment of the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland

Security (FSSCC), which brings together private sector institutions and organizations to discuss security policy.

Of course the federal government sought to reorganize its efforts to protect critical infrastructure as a whole following 9/11. This included the creation of the Department of Homeland Security (DHS) and its central role in supporting critical infrastructure protection across sectors.

In 2003 Homeland Security Presidential Directive 7 (HSPD-7), superseded PDD-63 and further established Treasury's role as sector liaison by naming Treasury the Sector Specific Agency (SSA) for the banking and finance sector.

Presidential Policy Directive (PPD-21), which revoked HSPD-7, was published in 2013 to advance a national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure. PPD-21 reaffirmed Treasury's role, recognizing its sector expertise and day-to-day engagement in building and reinforcing the security and resiliency partnership between the public and private sectors.

At the same time that PPD-21 was published, the President issued Executive Order (EO) 13636, which was focused specifically on cybersecurity. EO 13636 sought to specifically address the growing cyber threat to critical infrastructure by enhancing partnership with the owners and operators of critical infrastructure to improve cybersecurity information sharing and collaboratively develop and implement risk-based standards.

In response to PPD-21 and EO 13636, the Treasury has continued to expand its focus on increasing the security and resiliency of the financial services sector. Cybersecurity now ranks as one of Treasury's top priorities.

Building Partnerships to Reduce Risk

We at Treasury have found it necessary to coordinate closely with other government agencies and the private sector in order to keep pace with the growing volume and sophistication of cyber-attacks.

In addition to routine one-on-one communications with federal and state financial regulators at the staff- and principal-levels, Treasury coordinates financial sector cybersecurity efforts through the FBIIC. This committee of federal and state financial regulators meets monthly.[1] Meeting agenda topics range from removing information sharing impediments and enhancing incident response planning, to discussing best practices for cybersecurity policies, procedures, and controls. Between meetings, staff work to advance key initiatives, share details of new cyber incidents, and disseminate actionable information about those incidents to financial institutions.

Given recent threats and incidents, and to sharpen the attention of the financial regulators on cybersecurity, last summer, under the leadership of Secretary Lew and Deputy Secretary Bloom

[1] The 18 committee members include representatives from Treasury, the federal banking regulators, the federal market regulators, and associations representing state banking, insurance, and securities regulators.

Raskin, FBIIC launched regular principal-level meetings of the committee. While staff-level meetings focus on operational and tactical issues, the principal-level meetings concentrate on strategic, policy-level issues around cybersecurity and other critical infrastructure matters.

Additionally, Treasury appreciates its collaboration with the Federal Financial Institutions Examination Council (FFIEC), through which federal banking and credit union agencies coordinate and share information, and looks forward to continuing to work closely with the FFIEC on cybersecurity and other issues.

To coordinate policy development and shared situational awareness, Treasury leadership and staff regularly meet with officials of other cabinet departments, law enforcement organizations, and the intelligence community, including the Department of Homeland Security, Federal Bureau of Investigation, the United States Secret Service, and the National Security Agency. These meetings take place in bilateral settings as well as various group meetings, including the National Security Council Staff led Cyber Interagency Policy Council (IPC).

Our coordination with the private sector primarily takes place through the FSSCC and the FS-ISAC and regional coalitions. Additional coordination occurs through individual institutions as well as trade organizations such as the Financial Services Roundtable's BITS division, the American Bankers Association, the Clearing House, the Securities Industry and Financial Markets Association (SIFMA), Credit Union National Association, the National Association of Federal Credit Unions, and the Independent Community Bankers of America.

Collaborative efforts to respond to cyber risk also depend on strong partnership between the public and private sectors.

Our coordination efforts between the public and private sector on financial sector cybersecurity efforts focus on three areas:

- Facilitating the sharing of timely, actionable information regarding cyber threats and incidents with a view toward limiting attacks and stopping contagion across systems, networks, and institutions;
- Assisting with effective, prompt response and recovery from cyber incidents to reassure the public and protect public and private assets; and
- Promoting best practices around cybersecurity controls that help operators of financial systems prevent attacks from succeeding and help minimize the damage from any successful attacks.

Information Sharing

Sharing technical and strategic information about cyber incidents and threats is one of the most effective tools that the government has to support the mitigation of cyber incidents and improve the operational resiliency of the financial sector.

Sharing cybersecurity information is critical to enhance firms' ability to protect their networks and systems from malicious cyber activity, limit the impact of cyber incidents that have already occurred, and establish shared awareness of cyber threats so government and the private sector can respond rapidly to significant incidents.

The primary challenges that currently exist in information sharing are related to growing the network of institutions and government agencies that contribute to collective information sharing, increasing the speed of sharing and processing of cyber-threat information, improving the value of information by contributing more information derived from classified sources to private sector companies, and addressing legal concerns of private sector companies that inhibit them from engaging in robust information sharing.

The financial sector has invested significant resources in developing robust information sharing mechanisms, primarily through the FS-ISAC. This Information Sharing and Analysis Center is a model for what can be accomplished by the private sector, and we in the government should look to further encourage the growth of the FS-ISAC and ISACs in other sectors.

We commend Tom Curry for his leadership and note the FFIEC's recommendation from last month that all firms consider participating in the FS-ISAC. Treasury supports firms' consideration of participation in such information sharing organizations. The FS-ISAC has seen a tremendous surge in membership over the last year. Affirmative support by the financial regulators will support further growth of such important institutions.

In order to improve the speed of information sharing, and therefore its effectiveness, Treasury supports the FS-ISAC's move towards automated information sharing through the adoption of Structured Threat Information eXpression (STIX) and Trusted Automated eXchange of Indicator Information (TAXII). These information sharing protocols, on which DHS has been a leader, minimize the lag between discovered threats and deployed defenses.

In order to ensure that the sector is receiving the best possible information from all government sources, Treasury works closely with other agencies to identify and declassify information that may be of use to private sector firms. To this end, I have established a team within my office, the Financial Services Cyber Intelligence Group (CIG), which works with interagency and private sector partners to provide timely and actionable information, including threat indicators, to the financial services sector. Treasury supports the efforts set forth under section 4 of EO 13636. DHS' National Cybersecurity and Communications Integration Center deserves a special commendation for its continuing work in facilitating the efficient and beneficial exchange of information between government agencies and the private sector.

Treasury also recognizes that federal financial regulators have unique authorities and relationships with financial institutions. To capitalize on this, Treasury encourages efforts by the financial regulators to develop strategies for regulatory agencies to utilize unique relationships and authorities to improve information sharing and enhance situational awareness.

Incident Management

To improve incident management, Treasury believes that roles and responsibilities for different entities must be more clearly defined and regularly tested and refined. In order to best prepare for cybersecurity incidents, government agencies and private sector entities must work together to develop response protocols that clearly delineates roles and responsibilities.

Within the financial sector, Treasury has worked closely to support the development of sector-wide response protocols, including the FS-ISAC's all-hazards response plan and the FSSCC's cyber response framework. Additionally, protocols must be developed by individual private firms and coordinated across sectors.

And these protocols must be integrated and regularly updated to maintain relevance and effectiveness. They must also take into account interconnections across sectors and be inclusive of all relevant critical infrastructure.

Similarly, exercises are necessary to improve incident response plans and develop "muscle memory" in the organizations and with the personnel responsible for managing incident response. Treasury has partnered with DHS and the FSSCC to develop an exercise program focused on the financial services sector. The first joint exercise in this program was held yesterday. By continuing to hold these exercises, and smaller drills along the way, we can collectively hone our preparedness and continuously improve our response mechanisms.

Best Practices

And finally, the federal government can play a unique role in working with industry to support the use and development of standards, guidelines, and best practices on cybersecurity, ensuring that these practices are up-to-date and enable technical innovation. President Obama's EO 13636 called for NIST to develop a framework that would reduce cyber risks to critical infrastructure. Treasury has worked closely with the financial sector regarding how the sector could provide input into the Framework. Over the 12-month period from the issuance of the EO to the roll out of the *Framework for Improving Critical Infrastructure Cybersecurity* (NIST Cybersecurity Framework), the financial sector sent representatives to each of the five NIST workshops, met with NIST and Treasury to discuss sector specific considerations, and provided comment letters on the draft document. Without this time commitment and sharing of knowledge by the financial sector and all of the members from other sectors, interested organizations and the public who devoted time to this subject, the NIST Cybersecurity Framework would not have been completed so successfully.

As it exists today, the NIST Cybersecurity Framework, is a voluntary blueprint that firms of all sizes can use to evaluate, maintain, and improve the resiliency of their computer systems and reduce cyber risk. Treasury continues to encourage financial services firms to utilize the Framework, including by holding business partners, suppliers, and customers accountable to its risk management approach. In particular, efforts by SIFMA to develop auditable standards of the Framework may be beneficial in supporting broad adoption of best practices.

Likewise, recent efforts by financial regulators to promote consistent adoption of best practices across the sector are encouraging. The SEC recently promoted the use of the NIST Cybersecurity Framework and other related NIST standards in the guidance to its final Regulation Systems Compliance and Integrity (Reg SCI). Such consistency is important to promoting shared understanding of cybersecurity risk management and broad adoption of best practices.

Conclusion

While significant progress has been made to improve financial sector cybersecurity, we know that there is more work to be done. We continue to hold ongoing discussions with our government and private sector partners to identify and build a more secure and resilient financial sector. As these efforts progress, we will work with senior policy makers to determine the best courses of action to address the issues that are identified.

I thank you for focusing on this issue and would be happy to take your questions.

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.

For Release Upon Delivery

10:00 a.m., December 10, 2014

TESTIMONY OF

VALERIE ABEND

SENIOR CRITICAL INFRASTRUCTURE OFFICER

OFFICE OF THE COMPTROLLER OF THE CURRENCY

Before the

COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS

UNITED STATES SENATE

December 10, 2014

Statement Required by 12 U.S.C. § 250:
The views expressed herein are those of the Office of the Comptroller of the Currency and do not necessarily represent the views of the President.

Chairman Johnson, Ranking Member Crapo, and members of the Committee, thank you for the opportunity to appear before you today to discuss the important issue of cybersecurity, including our efforts to address cyber threats and vulnerabilities and coordinate information sharing for the benefit of the banking industry, regulatory community, and the financial system overall. There are few issues more important to the OCC and to our country's economic and national security than the risks posed by cyber attacks.

My name is Valerie Abend, and I serve as the OCC's Senior Critical Infrastructure Officer. In collaboration with the agency's supervisory divisions, I lead the agency's cybersecurity and resilience efforts for the national banks and federal savings institutions (referred to collectively as banks) that we supervise. I also currently chair the Federal Financial Institutions Examination Council's (FFIEC) Cybersecurity and Critical Infrastructure Working Group (CCIWG). I have more than 20 years of private and public sector experience in the cybersecurity and critical infrastructure fields. My testimony today will discuss the cybersecurity initiatives the OCC and the FFIEC have taken, the avenues in place to share cybersecurity information, and recommendations where legislation may be helpful to enhance information sharing among financial institutions.

I. Background

We live in a world of rapidly changing technology that impacts financial institutions both in terms of the products and services they offer and the risks that they face. We are long past the time when retail payments occur through face-to-face cash transactions or with paper checks. Instead, consumers increasingly use their cellphones to deposit checks, pay bills, and make purchases at the mall. For most consumers, electronic-based payment mechanisms and electronic banking are a routine part of life, and they may not give much thought to what goes on

behind the scenes to provide the speed, convenience, and security in our payment and settlement systems today. What they may not know is the vast amount of information technology that institutions necessarily rely upon to make this convenience possible. To continue to improve efficiency and offer new products and services, institutions are rapidly adopting new information technology. From connecting personal devices such as tablets and phones to their networks and launching new mobile banking applications, to using cloud computing, banks are adopting new technologies and establishing new connections. Collectively, this dependence on technology and the data that financial institutions create along with the funds they maintain and transmit every day make financial institutions attractive targets for hackers. Unfortunately, new vulnerabilities in both hardware and software are identified daily, making it difficult to protect systems from cyber attacks.

Furthermore, networks that serve the financial industry are global, which means hackers can target banks and other systems from almost anywhere in the world. Financial institutions today face threats from insiders and individuals acting alone, and from international networks of well-organized nation-states, criminals, and so-called "hacktivists" who use cyber attacks to raise awareness and support for their political or social causes.

As the risks evolve, financial institutions must continue to prepare for cyber attacks and how they will identify, mitigate, and respond to them – and regulators must take steps to ensure that they do so.

II. OCC Supervisory Framework and Initiatives

The OCC's supervisory framework is built around four key elements. The first is the OCC's ongoing monitoring and information sharing with other regulators, government agencies, and banks with respect to emerging threats and changes to the risk landscape. The second is the

OCC's development and continual refinement of standards and guidance that set forth supervisory expectations as to how banks and third-party service providers can best safeguard bank and bank customer information. The third key component is the agency's communication of these supervisory expectations to examiners and bank management through training and other forms of communication. The final component of the framework is the implementation of policy through on-site examination of banks and critical third-party service providers to assess their compliance with our supervisory expectations to ensure that they are appropriately managing risks, and when necessary, directing them to take corrective action. Each of these elements is described below.

1) Ongoing Monitoring, Assessment, and Information Sharing

Ongoing monitoring and timely information sharing across the financial sector regarding cybersecurity issues including threats, vulnerabilities and risk mitigation tactics, is a crucial component of our efforts. The OCC conveys risk management practices to banks, including strategies to identify, prevent, mitigate and respond to attacks. During and following a cyber attack, the OCC plays an important role in evaluating the impacts from the attack to determine if they pose a material risk to bank systems and bank customer information. At the same time, the OCC evaluates whether the institutions involved are taking appropriate and timely corrective action.

We encourage banks and service providers to participate with regulators in forums to learn about specific cyber threats in a timely manner. For example, the OCC is a member of both the Financial and Banking Information Infrastructure Committee (FBIIC) and the Financial Services Information Sharing and Analysis Center (FS-ISAC), which are among the financial

sector's public-private partnerships that provide information regarding cyber threats and various means to improve the security and resilience of the financial sector.

OCC examiners also maintain ongoing communication with the banks they supervise. This includes information related to pervasive vulnerabilities and incidents that may cause significant disruption to systems, facilities, or business processes at the bank, its operating subsidiary or affiliate, or at a third-party service provider. Examiners monitor the bank's response to incidents and to reports on threats and vulnerabilities and assess the level of impact and risk to customers, business operations, as well as any system-wide or downstream effects.

The OCC uses a number of mechanisms, based on the nature of the threat or vulnerability and the immediacy of potential impact, to communicate information that may pose a material risk to the banks we supervise. This includes providing examiners with instructions and messages to use in contacting bank management on specific wide-scale vulnerabilities and threats, the risks these may pose to the bank, and actions the bank should take to prevent, detect, and respond to a threat or vulnerability.

2) Supervisory Standards and Guidance

The banking sector is highly regulated and has been subject to stringent information security requirements for decades. The OCC has the authority to require the banks we regulate and their service providers to protect their own systems and bank customer data and to require banks to take steps to identify, prevent, and mitigate identity theft.

For example, following the 1999 enactment of the Gramm-Leach-Bliley Act, the OCC, in conjunction with the Federal Deposit Insurance Corporation (FDIC), the Board of Governors of the Federal Reserve System (FRB), and the National Credit Union Administration (NCUA), published enforceable information security guidelines that set forth standards for administrative,

technical, and physical safeguards that financial institutions must have to ensure the security and confidentiality of customer information. These interagency guidelines require banks to develop and implement formal information security programs that are tailored to a bank's assessment of the risks it faces, including internal and external threats to customer information and any method used to access, collect, store, use, transmit, protect, or dispose of the information. Given the evolving threat and technology environment, the guidelines require a bank's information security program to be dynamic – to continually adapt to address new threats, changes in technology, and new business arrangements. Since banks often depend upon service providers to conduct critical banking activities, the guidelines also address how banks must manage the risks associated with their service providers.

In addition, pursuant to section 114 of the FACT Act, the OCC, FRB, FDIC, NCUA, and the Federal Trade Commission, issued regulations in 2007 titled "Identity Theft Red Flags and Address Discrepancies." These rules require each financial institution and creditor to develop and implement a formal identity theft prevention program that includes policies and procedures for detecting, preventing, and mitigating identity theft in connection with account openings and existing accounts. A bank's program must include policies and procedures to identify, detect and respond to relevant indicators of identity theft, and must be updated periodically to reflect changes in risks to customers and to the institution from identity theft.

Over the years, the OCC on its own, and through the FFIEC, also has published guidance and handbooks that make clear our expectations about acceptable risk management processes and procedures for safeguarding information and managing information technology (IT) risks. This guidance addresses broad subjects such as information security, business continuity planning, and outsourcing technology services. It also focusses on specific areas of risks, such as

authentication of users in an Internet banking environment and effective software patch management. As noted below, this guidance is reviewed continually and updated to take into account evolving risks.

3) Examiner Training and Communicating Expectations

All entry-level OCC examiners receive training on information technology risk management within their first three years of employment. In addition, the OCC has examiners who specialize in IT. These examiners have specialized skills and experience to focus on information security and other technology risks inherent in bank operations. To help these specialists maintain their skills and knowledge, the OCC has an advanced IT training program. This is further augmented through webinars, in-person meetings, and formal and informal networking groups. When the OCC issues new guidance or updates existing guidance, we incorporate it into our training and develop communications so that our examiners can effectively implement these changes through the examination process.

Additionally, the OCC has taken steps to raise awareness of banks about the risks posed by cyber threats and vulnerabilities and to inform them of changes to supervisory expectations. This includes highlighting cybersecurity as an important operational risk that banks must pay close attention to through our public Semi-Annual Risk Perspective reports, releasing bulletins to the industry on topics such as distributed denial of service attacks, and hosting webinars, outreach meetings and roundtable discussions.

4) Onsite Examinations

As part of their ongoing supervision, OCC examiners assess the adequacy of the controls that protect customer information, and bank systems and information. The OCC and the other federal banking regulators also conduct joint examinations of major technology service providers that provide critical services to the banking sector.

Due to the complexity of the largest national banks, the OCC has resident IT examiners onsite who perform ongoing supervision of the banks' IT policies, procedures, and practices. OCC examiners also perform onsite IT examinations at smaller banks every twelve to eighteen months as part of their regular exam. Examiners also follow up on identified concerns or emerging cyber risks during quarterly communications with the banks they supervise, or on a more frequent basis depending on the nature of the concern or risk. The OCC uses information from bank examinations to inform our policies, training, and exam procedures. For example, through our exams, the OCC identified increasing risks and the need for additional guidance for banks on how to manage the complex risks posed by critical third-party relationships. As a result, in 2013, the OCC updated its Third-Party Relationship Risk Management Guidance, which incorporates important expectations for banks to evaluate their third parties' information security, incident response, and management of information systems, as well as the servicers' ability to assess, monitor, and mitigate risks posed by its subcontractors.

III. FFIEC Initiatives

The Comptroller currently chairs the FFIEC, an interagency body comprised of the principals of the five federal banking regulatory agencies – the OCC, the FRB, the FDIC, the NCUA, and the Consumer Financial Protection Bureau (CFPB) – and the FFIEC's State Liaison Committee. The FFIEC is empowered to prescribe uniform principles, standards, and report forms to promote uniformity in the supervision of financial institutions. One of the Council's top priorities is to strengthen institutions' resilience to cyber attacks. Last year, the Comptroller called for – and the Council members concurred in – the creation of the CCIWG to enhance communication among the FFIEC members and to build on existing efforts to strengthen the activities of other interagency and private sector groups with respect to cybersecurity.

The CCIWG serves as a liaison between the members of the FFIEC and the intelligence community, law enforcement, and the Department of Homeland Security (DHS) on issues related to cybersecurity and the protection of critical infrastructure. The working group is empowered to help the FFIEC members collaborate in establishing cyber-related examination policy, developing training programs, coordinating responses to cybersecurity incidents, and managing information-sharing efforts.

The working group has been quite active since its inception. Through its coordination and information sharing with intelligence, law enforcement, DHS, and the Department of the Treasury, the group has drafted several statements to institutions advising firms about the threats posed by ATM cashout schemes, distributed denial of service attacks, and widespread vulnerabilities such as Heartbleed and Shellshock.

One major initiative that the working group launched this summer was the Cybersecurity Assessment, which involved the pilot of a new cybersecurity examination work program at more than 500 diverse community institutions supervised by the OCC, FRB, FDIC, NCUA, and state regulatory agencies. The Cybersecurity Assessment evaluated the complexity of each institution's operating environment, focusing on such factors as the types of connections employed, products and services offered, and technologies used. It also assessed each institution's overall cybersecurity preparedness, with a focus on the following key areas: Risk Management and Oversight, Threat Intelligence and Collaboration, Cybersecurity Controls, External Dependency Management, and Cyber Incident Management and Resilience. The results of the assessment are instructive and will help FFIEC members make informed decisions about how they identify and prioritize actions to enhance the effectiveness of cybersecurity-related supervisory programs, guidance, and examiner training.

Preliminary findings that members agreed would be beneficial to share with institutions were released as *General Observations* and are available on the FFIEC's website.[1] This document highlights some high-level observations and provides questions that boards of directors and chief executive officers (CEOs) of financial institutions should consider when assessing their cybersecurity preparedness. For example, the document encourages institutions to routinely discuss cybersecurity issues in board and senior management meetings to help the financial institution set the tone from the top and build a strong security culture. It also encourages institutions to clearly define roles and responsibilities and assign accountability to identify, assess, and manage cybersecurity risks across the financial institution. While the institutions' leadership is responsible for cybersecurity risk management, employees are typically the first line of defense. As such, the FFIEC also encourages institutions to keep their training programs current and provide them more frequently.

Additionally, the document emphasizes that management should monitor and maintain sufficient awareness of cybersecurity threats and vulnerabilities to help ensure that financial institutions can evaluate and respond to emerging risks. To help build this capability, the FFIEC on behalf of its members issued the statement recommending that institutions of all sizes participate in the FS-ISAC to better understand the risks posed to their institution and to support their risk management program.

Institutions in the pilot assessment implement controls to impede unauthorized access to their systems and have tools in place to detect previously identified attacks. The *General Observations* document stresses that institutions should review and adjust controls when making changes to their IT environment, routinely scan networks for vulnerabilities and anomalous

[1] The FFIEC Cybersecurity Assessment, General Observations document can be accessed at http://www.ffiec.gov/press/PDF/FFIEC_Cybersecurity_Assessment_Observations.pdf

activity, test systems for potential exposure to cyber attacks, and remediate issues when identified. Similarly, the document highlights the importance of identifying the connections an institution has with third-party service providers and ensuring formal controls are in place to secure the ways these providers transmit, access, and store data.

Finally, while we found that institutions have procedures for notifying customers, regulators, and law enforcement when incidents affect sensitive customer information, the document emphasizes that institutions should strengthen their ability to address breaches that may occur by establishing and routinely testing incident response plans throughout the institution. This would include incorporating cyber-attack scenarios into business continuity plans and programs.

In addition to the Cybersecurity Assessment, the CCIWG has made strides in increasing financial institutions and examiners' awareness of cyber threats and vulnerabilities and the actions that management can take to mitigate these risks. During the past year, the working group led a webinar, "Executive Leadership of Cybersecurity" for which over 5,000 community institution CEOs registered, and conducted web-based trainings for over a thousand examiners on cybersecurity issues. Last month, concurrent with the release of the *General Observations* document, the FFIEC, on behalf of its members, released the *Cybersecurity Threat and Vulnerability Monitoring and Sharing Statement*.[2] The statement reiterated members' expectations that management monitor and maintain sufficient awareness of cybersecurity threat and vulnerability information in order to evaluate risk and respond accordingly. In addition, it reinforced the need for all institutions and their critical technology service providers to have appropriate methods for monitoring, sharing, and responding to threat and vulnerability

[2] The FFIEC Cybersecurity Threat and Vulnerability Monitoring and Sharing Statement can be accessed at http://www.ffiec.gov/press/PDF/FFIEC_Cybersecurity_Statement.pdf

information. In addition to recommending institutions to join FS-ISAC, the statement also listed additional government resources that are able to assist financial institutions with identifying and responding to cyber attacks.

IV. Cross Sector Cybersecurity Dependencies and Information Sharing

As noted earlier, ensuring appropriate information sharing is an essential component of the OCC's cybersecurity efforts. The OCC uses information sharing forums, relationships with government agencies, and the supervision process to acquire information on potential and confirmed cyber threats and attacks.

As a member of the FS-ISAC and through our work with the Treasury Department, we receive significant alerts that provide information related to cyber threats, attacks, and vulnerabilities. We also recognize the importance of maintaining relationships with the law enforcement and intelligence communities to share information and keep lines of communication open. The OCC is an active member of the FBIIC, created to improve coordination and communications among a broad array of financial regulators, and chaired by the Treasury Department. These efforts include monthly staff-level meetings and periodic meetings with agency principals. In addition, we attend classified briefings for FBIIC and support the collaborative initiatives of this sector-wide partnership.

The Financial Stability Oversight Council (FSOC) also provides a mechanism to promote collaborative efforts on a range of issues, including cybersecurity issues, and has set forth specific recommendations to advance cybersecurity efforts. The creation of the CCIWG, and some of its activities are directly responsive to the FSOC's recommendations. In its 2014 annual report, FSOC recommended that the Treasury Department continue to work with regulators, other appropriate government agencies, and private sector financial entities to develop the ability

to leverage insights from across the government and other sources to inform oversight of the financial sector and to assist institutions, market utilities, and service providers that may be targeted by cyber attacks. The FFIEC's aforementioned issuances are prime examples of responses to these recommendations. The FSOC also recommended that financial regulators continue their efforts to assess cyber-related vulnerabilities facing their regulated entities, identify gaps in oversight that may need to be addressed, and inform and raise awareness of cyber threats and attacks. As discussed earlier, the FFIEC's Cybersecurity Assessment responds to these recommendations.

The OCC and other banking agencies have a robust process for issuing standards and guidance and supervising the financial sector through our examinations. However, the resiliency of the financial sector is also dependent on other critical sectors, including the telecommunications and energy sectors, which do not operate under a comprehensive supervisory regime like financial institutions. The OCC strongly supports efforts to ensure other sectors have commensurate standards and improved transparency as it relates to the cybersecurity preparedness for these other sectors. In addition, the financial services industry and retailers have interdependencies. We have seen a number of attacks on large retailers in which credit card and other information from millions of consumers was compromised. In response, financial institutions compensate customers for fraudulent charges and replace credit and debit cards, and monitor account activity for fraud at significant cost. This is not easy for any bank, but the burden falls especially heavily upon community institutions. At a cost of $5 or more per card plus fraud related charges, the costs can escalate quickly. We would support efforts to even the playing field between banks and merchants to ensure that both contribute to efforts to make affected consumers whole.

The Treasury Department, as our Sector Specific Agency, has been leading efforts to work more closely with the government agencies responsible for overseeing these other sectors. The OCC supports these efforts and hopes they lead to more in-depth interactions between the financial sector and other sectors with which it closely interacts. For our part, the OCC is a member of a newly formed Cybersecurity Forum for Independent and Executive Branch Agencies. The Forum's objectives are to enhance communication, identify lessons learned, and develop a common understanding of cybersecurity activities through the sharing of best practices and exploring approaches to enhance cybersecurity protections.

V. Recommendations for Congressional Consideration

As we work to safeguard our financial system, we note some areas where Congressional action is necessary to provide parity among the parties impacted in cyber breaches that adversely affect consumers and to facilitate additional information sharing within the banking industry.

1) Parity for Retailers

The recent breaches at large retailers highlight the need for improved cybersecurity for merchants. Enhanced cybersecurity should apply to all industries where customer information is at risk. There should be consistent protections across all industries for securing financial transactions, customer information, and systems. Further, these protections should include appropriate responses to breaches when they do occur. As mentioned previously, when breaches occur in merchant systems, merchants should contribute to efforts to make affected consumers whole.

2) Industry Information Sharing

The OCC believes the existing statutory framework could be improved to encourage information sharing about cyber attacks among institutions. We believe that amending the USA

PATRIOT Act by creating a safe harbor to facilitate and promote the timely sharing of information among financial institutions concerning cybersecurity threats, cyber attacks, and data breaches would create incentives for enhanced information sharing, which would result in increased awareness of potential threats within the banking industry.

3) Other Legislative Proposals

The OCC has reviewed a number of legislative proposals that are pending in Congress to promote and facilitate information sharing concerning cyber threats and attacks among government agencies. The OCC generally supports such legislative initiatives. However, in the case of cyber threat information involving banks, the bills we have reviewed do not require or encourage the DHS, the Department of Justice, or other government agencies to share this information with the appropriate federal banking agency. The federal banking agencies need cyber threat information involving banks to ensure the safety and soundness of both individual banks and the broader financial system. Accordingly, we believe that legislative proposals designed to improve and promote cyber threat information sharing among government agencies should require other government agencies to share information related to banks with the federal banking agencies.

In addition, most legislative proposals designed to promote and facilitate cyber threat information sharing provide that the information shared may not be used for regulatory purposes. This provision could impede our ability to issue cybersecurity guidance or regulations, or to take action to correct deficiencies in cybersecurity risk management.

VI. Conclusion

We have high expectations for our supervised entities in the area of cybersecurity. Financial institutions of all types and sizes must remain vigilant to protect against and mitigate

cyber breaches, and we at the OCC will continue to support banks in this effort. To ensure we stay on top of the evolving threats to the financial services industry, the OCC is committed to refining our supervisory processes on an ongoing basis and to participating in public-private partnerships to help keep abreast of and respond to emerging threats.

The Comptroller has emphasized the importance of communication, collaboration, and cooperation in all aspects of our mission. Nowhere is such communication and collaboration more important than in the realm of cybersecurity, where the threat transcends agency jurisdictions and industry boundaries. Combatting cyber threats and protecting our economic security requires the government and industry to work together for the good of consumers, the industry, and the entire financial services sector.

William Noonan

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

Prepared Testimony

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

December 10, 2014

Good morning Chairman Johnson, Ranking Member Crapo, and distinguished Members of the Committee. Thank you for the opportunity to testify on the ongoing challenge of cyber crime impacting our Nation's financial system. The U.S. Secret Service (Secret Service) has decades of experience investigating large-scale criminal cyber intrusions, in addition to other crimes that impact our Nation's financial payment systems. Based on this investigative experience, I hope to provide this Committee insight into the continued trend of transnational cyber criminals targeting our Nation's financial system for their illicit gain.

The Role of the Secret Service

The Secret Service was founded in 1865 to protect the U.S. financial system from the counterfeiting of our national currency. As the Nation's financial system evolved from paper to plastic to electronic transactions, so too has the Secret Service's investigative mission. Today, our modern financial system depends heavily on information technology for convenience and efficiency. Accordingly, criminals have adapted their methods and are increasingly using cyberspace to exploit our Nation's financial payment system by engaging in fraud and other illicit activities. This is not a new trend; criminals have been committing cyber enabled financial crimes since at least 1970.[1]

Congress established 18 USC §§ 1029-1030 as part of the Comprehensive Crime Control Act of 1984[2] and explicitly assigned the Secret Service authority to investigate these criminal violations.[3] These statutes first established as specific Federal crimes unauthorized access to computers[4] and the fraudulent use, or trafficking of, access devices[5]—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.[6]

Secret Service investigations have resulted in the arrest and successful prosecution of cyber criminals involved in the largest known data breaches, including those of TJ Maxx, Dave & Buster's, Heartland Payment Systems, and others. Over the past five years Secret Service cyber crime investigations have resulted in over 5,940 arrests, associated with approximately $1.53 billion in fraud losses and the prevention of over $11.71 billion in potential fraud losses. Through our work with our partners at the U.S. Department of Justice (DOJ), in particular local U.S. Attorney's Offices, the Computer Crime and Intellectual Property Section (CCIPS), the International Organized Crime Intelligence and Operations Center (IOC-2), the Federal Bureau of Investigations (FBI) and others, we will continue to bring major cyber criminals to justice.

[1] Beginning in 1970, and over the course of three years, the chief teller at the Park Avenue branch of New York's Union Dime Savings Bank manipulated the account information on the bank's computer system to embezzle over $1.5 million from hundreds of customer accounts. This early example of cyber crime not only illustrates the long history of cyber crime, but the difficulty companies have in identifying and stopping cyber criminals in a timely manner—a trend that continues today.
[2] Pub. L. 98-473, §§ 1602(a) and 2102(a), 98 Stat. 1837, 2183 and 2190.
[3] 18 U.S.C. §§ 1029(d) & 1030(d)(1)
[4] 18 U.S.C. § 1030
[5] 18 U.S.C. § 1029
[6] 18 U.S.C. § 1029(e)(1)

The Transnational Cyber Crime Threat

Advances in computer technology and greater access to personally identifiable information (PII) via the Internet have created online marketplaces for transnational cyber criminals to share stolen information and criminal methodologies. As a result, the Secret Service has observed a marked increase in the quality, quantity, and complexity of cyber crimes targeting private industry and critical infrastructure. These crimes include network intrusions, hacking attacks, malicious software, and account takeovers leading to significant data breaches affecting every sector of the world economy. The recently reported payment card data breaches are examples of the decade-long trend of major data breaches perpetrated by transnational cyber criminals who are intent on targeting our Nation's financial payment system for their illicit gain.

The growing collaboration amongst cyber-criminals allows them to compartmentalize their operations, greatly increasing the sophistication of their criminal endeavors as they develop expert specialization. These specialties raise 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. These digital marketplaces often use various digital currencies, and cyber criminals have made extensive use of digital currencies to pay for criminal goods and services or launder illicit proceeds.

Secret Service Strategy for Combating this Threat

The Secret Service proactively investigates cyber crime using a variety of investigative means to infiltrate these 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.

A trusted relationship with the victim is essential for confirming the crime, remediating the situation, beginning a criminal investigation, and collecting evidence. The Secret Service's growing global network of 37 Electronic Crimes Task Forces (ECTF), located within our field offices, are essential for building and maintaining these trusted relationships, along with the Secret Service's commitment to protecting victim privacy. The Secret Service routinely discovers data breaches through our proactive investigations and notifies victim companies with actionable information. For example, as a result of information discovered this year through just one of our ongoing cyber crime investigations, the Secret Service notified hundreds of U.S. entities of cyber criminal activity targeting their organizations.

Additionally, as the Secret Service investigates cyber crime, we discover current criminal methods and share this cybersecurity information broadly to enable other organizations to secure their networks. The Secret Service does this through contributing to leading industry annual reports such as the Verizon Data Breach Investigations Report and the Trustwave Global Security Report, and through more immediate reports, including joint Malware Initial Findings Reports (MIFRs).

This year, UPS Stores Inc. used information published in a joint report by the Secret Service, National Cybersecurity and Communications Integration Center, United States Computer Emergency Readiness Team (NCCIC/US-CERT), and the Financial Services Information Sharing and Analysis Center (FS-ISAC) on the Back-Off malware to protect itself and its customers from cyber criminal activity.[7] The information in this report was derived from a Secret Service investigation of a network intrusion at a small retailer in Syracuse, New York. The Secret Service publically shared actionable cybersecurity information derived from this investigation to help numerous other organizations while still safeguarding sensitive information. As a result, UPS Stores, Inc. was able to identify 51 stores in 24 states that had been impacted, and then were able to contain and mitigate this cyber incident before it developed into a major data breach.[8]

As we share cybersecurity information discovered in the course of our criminal investigation, we also continue our investigation in order to apprehend and bring to justice those involved. 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 finally apprehend the top tier criminals responsible. For example, even after a 2011 indictment, Secret Service agents were not able to arrest Roman Seleznev of Vladivostok, Russia, in an international law enforcement operation until just recently. Mr. Seleznev has been charged in Seattle in a 40-count superseding indictment for allegedly being involved in the theft and sale of financial information of millions of customers. Seleznev is also charged in a separate indictment with participating in a racketeer influenced corrupt organization (RICO) and conspiracy related to possession of counterfeit and unauthorized access devices.[9] This investigation was lead by the Secret Service's Seattle Electronic Crimes Task Force.

In another case, the Secret Service, as part of a joint investigation with U.S. Immigration and Customs Enforcement's Homeland Security Investigations (HSI) and the Global Illicit Financial Team, hosted by IRS-Criminal Investigations, shut down the digital currency provider Liberty Reserve, which was allegedly widely used by criminals worldwide to store, transfer, and launder the proceeds of a variety of illicit activities. Liberty Reserve had more than one million users, who conducted approximately 55 million transactions through its system totaling more than $6 billion in funds. The alleged founder of Liberty Reserve, Arthur Budovsky, was recently extradited from Spain to the United States. Mr. Budovsky is among seven individuals charged in the indictment. Four co-defendants – Vladimir Kats, Azzeddine el Amine, Mark Marmilev, and Maxim Chukharev – have pleaded guilty and await sentencing. Charges against Liberty Reserve

[7] *See* http://www.us-cert.gov/security-publications/Backoff-Point-Sale-Malware
[8] *See* UPS Store's press release *available at* http://www.theupsstore.com/about/media-room/Pages/The-ups-store-notifies-customers.aspx.
[9] *See* http://www.justice.gov/usao/waw/press/2014/October/seleznev.html

and two individual defendants, who have not been apprehended, remain pending. This investigation was lead by the Secret Service's New York Electronic Crimes Task Force.

Legislative Action to Combat Data Breaches

While there is no single solution to prevent data breaches of U.S. customer information, legislative action could help to improve the Nation's cybersecurity, reduce regulatory costs on U.S. companies, and strengthen law enforcement's ability to conduct effective investigations. The Administration has proposed various pieces of cybersecurity legislation, including law enforcement provisions related to computer security, and continues to urge Congress to pass legislation that will strengthen government and private sector cybersecurity capabilities. In particular, we urge Congress to act on legislation that will allow us to keep pace with the rapidly-evolving threats of cyber crime.[10]

Conclusion

The Secret Service is committed to continuing to safeguard the Nation's financial payment systems by defeating cyber criminal organizations. Responding to the growth in these types of crimes, and the level of sophistication these criminals employ, requires significant resources and substantial collaboration among law enforcement and its public and private sector partners. Accordingly, the Secret Service dedicates significant resources to improving investigative techniques, providing training for law enforcement partners, and sharing information on cyber threats. The Secret Service will continue to coordinate and collaborate with other government agencies and the private sector as we develop new methods to combating cyber crime. Thank you for your continued commitment to protecting our Nation's financial system from cyber crime.

[10] This proposal is available at: http://www.whitehouse.gov/omb/legislative_letters/

Department of Justice

STATEMENT OF

JOSEPH M. DEMAREST, JR.
ASSISTANT DIRECTOR
CYBER DIVISION
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE

COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS
UNITED STATES SENATE

ENTITLED

"CYBERSECURITY:
ENHANCING COORDINATION TO PROTECT THE FINANCIAL SECTOR"

PRESENTED

DECEMBER 10, 2014

CYBER DIVISION
FEDERAL BUREAU OF INVESTIGATION

Statement before the Senate Committee on Banking, Housing and Urban Affairs

Assistant Director Joseph M. Demarest, Jr.
Cyber Division, Federal Bureau of Investigation
December 10, 2014

Good morning Chairman Johnson, Ranking Member Crapo, and the distinguished members of this Committee. I am honored to appear before you today to discuss the cyber threats facing our nation, their relation to the financial sector, and the efforts the FBI is taking to identify, pursue, and defeat those threats.

In the course of my brief testimony, I hope to give you a sense of the extent to which today's cyber actors pose new and increasingly complex threats to our country and to the financial sector — a threat that challenges the traditional models of the law enforcement and intelligence communities, where threat actors were previously confined by time, distance, and physical location. Instead, today's cyber actors, from nation states to criminal groups and individuals, find themselves virtually unrestricted in their targets sets and their ambitions, launching attacks from all over the world at literally the speed of light. Today, I hope to convey the many ways that we at the FBI are doing everything in our power to protect the nation, and the financial sector in particular, from these threats.

Cyber Threats Against the Financial Sector: Trends and Implications

Before describing the current cyber threatscape, I'd like to give a brief overview of the FBI Cyber Division, our mission, and how we target the cyber adversaries that threaten this country on a daily basis. In general, the FBI's mission falls into three separate buckets: first, we *identify* the cyber actors perpetrating harm. In the world of cyber crime and cyber espionage, this is often the most difficult step, as cyber threats may hide in plain sight, using various methods to obfuscate their presence, location, and activities. Second, we *pursue* these actors, tracking their activity both online and off. To this end, we utilize collaborative partnerships across the federal government, with international partners and with industry, along with our unique combination of national security and law enforcement authorities, to gather intelligence about the tactics, techniques and procedures of these actors. In short, we find these threat actors and we watch them, gathering intelligence and understanding the motives and the conduct of our adversaries. Lastly, with the aid of partnerships and our unique authorities, we *defeat* cyber adversaries through a full range of methods, including – most importantly, arresting and prosecuting those responsible. The FBI focuses foremost on intelligence led, threat-focused cyber operations which our personnel, analysts, computer scientists, and agents in the field help us achieve every day.

As the members of this Committee are aware, the range of actors who threaten our interests is as complex as it is varied. We face cyber terrorists, who aim to use our reliance upon and use of digital systems to advance their political or ideological goals. We face nation states, who aim to use the

cyber world to conduct espionage, to make preparations for war, and who may even carry out acts of war through cyber means. We face ideology-driven criminals, who may use methods such as denial of service attacks, known as "DDoS" attacks, to further their own ideology or social cause. We face insider threats, whose legitimate access to sensitive information may be used for various illicit ends. Lastly, we face financially motivated groups and individuals, who use a range of methods to enrich themselves at others' expense — and it is this group that I will focus upon most specifically today, though each and every group I just listed may, at times, view the financial sector as a prime target.

As the members of the Committee are also aware, the threat from cyber actors — specifically cyber criminals — continues to garner an increasing share of the media spotlight and continues to advance in sophistication. Recent high-profile attacks, such as those on eBay, Sony, J.P. Morgan Chase, and others, highlight vulnerabilities in some of our nation's largest companies. Regarding the threats to the financial sector in particular, such threats range in complexity, and we continue to work closely with the Secret Service, DHS, and other partners across the government. Point of sale thefts, also known as "POS" scams, for example, are not new, but continue to pose serious threats to the financial services industry. According to Verizon's 2014 Data Breach Investigations Report, the physical installation of a "skimmer" on an ATM, gas pump, or POS terminal to read credit card data has targeted ATMs with an overwhelming specificity — 87 percent of skimming attacks in 2013, for example, were on ATMs. Retail POS scams, where attackers compromise the computers and servers that run POS applications with the intention of capturing payment data, comprise an additional level of sophistication, and can take weeks or even months to be discovered, little less mitigated. The high-profile attack on Target provides one of the more sophisticated examples of retail POS scams, in which, according to open source reporting, 40 million credit card numbers and another 70 million customer records were stolen. Such attacks are not unique to Target — additional data breaches have been reported at Neiman Marcus, Michaels, and P.F. Chang's, among many others.

Vulnerabilities in mobile banking pose another new and highly sophisticated danger, as mobile banking vulnerabilities may exist on mobile devices that are not patched, and malware can be developed to specifically target the use of mobile devices. One example of this type of vulnerability is the Zeus-in-the-Middle malware, a mobile version of the GameOver Zeus malware, which itself was one of the most sophisticated types of malware the FBI ever attempted to disrupt. GameOver Zeus was designed to steel banking credentials that criminals could then use to initiate or redirect wire transfers to overseas bank accounts. All told, the malware infected over 1 million computers worldwide and caused over $100 million in estimated losses. Zeus-in-the-Middle has not caused the same level of damage or losses as GameOver Zeus, but its very existence illustrates the risk posed to mobile platforms, where devices can be infected by malicious apps or via spear phishing emails, and which can then enable cyber criminals to utilize the banking credentials of targeted users on a grand scale. Current open source reporting suggests that Android OS devices remain a prime target for mobile malware — according to the 2014 Cisco Annual Security Report, for example, 99 percent of mobile malware in 2013 targeted the Android platform.

Botnets, which can harness the power of an enormous web of computers for malicious purposes, continue to evolve as well. As I speak, estimates place the total damages caused by botnets at more than $9 billion in losses to U.S. victims and over $110 billion in losses worldwide. Approximately

500 million computers are infected globally per year — translating to 18 victims per second. As botnets become more sophisticated, our techniques must evolve to keep pace. The FBI and our partners may take down one botnet, for example, but coders may alter code and rebuild their bots in fairly short order. The power and scale of botnets is particularly worth noting, as botnets have been used to attack the financial sector through DDoS attacks, and the FBI has been deeply involved in preventing such attacks and in keeping such attacks from inflicting lasting damage. Beginning in September 2012, for example, actors launched powerful DDoS attacks from a botnet, combining the bandwidth of numerous web servers to target major U.S. banking institutions. The FBI worked closely with Department of Homeland Security (DHS) to issue Joint Indicator Bulletins (JIBs) to the U.S. banks, which included thousands of IP addresses that participated in the attacks. The U.S. banks used the IP addresses to better mitigate future incidents, thus helping to ensure their business operations could proceed with less interruption of service to their customers. The JIBs helped reduce the resources available for the threat actors to carry out future DDoS operations and demonstrated the effectiveness of FBI outreach to industry. Throughout this campaign, the FBI held significant outreach efforts to brief bank net-defenders through a series of classified briefs. These briefs, conducted by FBI, DHS, and Treasury representatives, provided bank security personnel the context of the DDoS threat and enabled the banks to share best-practices with their peers in real-time.

From March 2013 to July 2014, the FBI provided approximately 36 classified threat briefings regarding the DDoS attacks to private sector financial institutions and governmental agencies, including DHS, Department of Treasury, the Federal Deposit Insurance Corporation, and the Federal Reserve System. The initial classified briefing, held on March 19, 2013, was attended by over 300 chief information security officers via secure video teleconference from 33 FBI field offices. This type of outreach is far from irregular — based on imminent threats to the financial sector in early 2014, the FBI provided classified threat briefings in March, April, and July 2014 to a total of 145 financial institutions.

We at the FBI, in short, are doing everything in our power to keep pace with the evolving threat against the financial sector. We further our law enforcement mission when we collaborate within the government and across the private sector to prosecute and protect our nation and industries from the devastating consequences of cyber attacks.

Coordination and Information Sharing Across the Government

The FBI and our partners throughout the government have all made significant progress in recent years in collaborating within the cyber domain — and our progress hasn't just been limited domestically, but has occurred at international levels as well. A decade ago, for example, if an FBI agent tracked an Internet Protocol (IP) address to a criminal investigation, and if that IP address was located in a foreign country, this meant the effective end of the investigation. Since that time, however, the FBI has placed cyber specialists in key international locations to facilitate the investigation of cyber crimes affecting the U.S. Recognizing the value of cyber specialists working with key international partners, the FBI Cyber Division stood up a team known as the Operational Coordination Unit's Extraterritorial Operations group to focus on supporting, coordinating, and providing oversight of international cyber national security and criminal intrusion investigations

and operations. This group assesses the global cyber threat environment, developing and executing plans to ensure the assignment of FBI cyber specialists to areas where they are most needed. Such developments, along with technical improvements in our ability to track IP addresses back to their source, has led key actors in the underground economy to recognize the following fact: there are fewer and fewer safe hiding places around the globe for cyber criminals. These criminals may be able to run, capitalizing upon the anonymity and the geographical dispersion of the Internet, but thanks to our efforts, they will not be able to hide for long.

One prime example of the importance of collaboration and coordination is the recent takedown of Silk Road 2.0. Beginning in late December 2013, Blake Benthall, also known by the online handle "Defcon," secretly owned and operated an underground website known as Silk Road 2.0 — one of the most extensive, sophisticated, and widely used criminal marketplaces ever created on the Internet. The website operated on the Tor network, a special network of computers distributed around the world and designed to conceal the IP addresses of the computers that access the network, thereby masking the identities of the network's users. Silk Road 2.0 launched in November 2013 after its predecessor was shut down by law enforcement. Since its launch in 2013, Silk Road 2.0 has been used by thousands of illicit actors to distribute hundreds of kilograms of illegal drugs and other illegitimate goods and services to buyers throughout the world, as well as to launder millions of dollars generated by these unlawful transactions. As of September 2014, Silk Road 2.0 was generating sales of at least approximately $8 million per month and had approximately 150,000 active users. The very existence of Silk Road 2.0 highlights the core concern I'm here to address today: cyber criminals now operate far outside the traditional bounds that confined criminals in past decades, selling banking credentials by the thousands and placing malware on the market for the purposes of DDoS attacks, to cite just two examples of illicit activities that target the financial sector. Whereas last century's bank robbers used an automobile to steal from a handful of banks in a few states in one day — a novel development for the time — today's bank robbers can use the Internet to steal money from thousands of banks across the world in a few hours, all without ever leaving their basement.

Thanks to our coordinated efforts, however, criminal marketplaces like Silk Road 2.0 cannot and will not last for long. The investigation into Silk Road 2.0 was conducted jointly by the FBI and the DHS's Immigration and Customs Enforcement's Homeland Security Investigations (ICE-HSI), illustrating the critical nature of cooperation and information sharing in today's cyber investigations — no government agency, no matter how competent its agents and experts, can operate successfully on its own. We capitalize on our distinct roles and responsibilities within the government to address and prevent cybercrime. Over the course of the investigation into Silk Road 2.0, an HSI agent acting in an undercover capacity successfully infiltrated the support staff involved in the administration of the Silk Road 2.0 website and was given access to private, restricted areas of the site reserved for Benthall and his administrative staff. By doing so, the HSI agent was able to interact directly with Benthall throughout his operation of the website.

On November 7, 2014, the U.S. government seized the Silk Road 2.0 website in the largest law enforcement action to date against criminal websites operating on the Tor network. Benthall was arrested and charged with one count of conspiring to commit narcotics trafficking (carrying a maximum sentence of life in prison and a mandatory minimum sentence of 10 years in prison), one count of conspiring to commit computer hacking (carrying a maximum sentence of five years in

prison), one count of conspiring to traffic in fraudulent identification documents (carrying a maximum sentence of 15 years in prison), and one count of money laundering conspiracy (carrying a maximum sentence of 20 years in prison). The investigation was a key success for the FBI, for ICE-HSI, and for the U.S. government as a whole — and a key illustration of the importance of collaboration and cooperation.

Another example of the importance of collaboration and cooperation, both inside and outside of government, is the vital work the National Cyber Investigative Joint Task Force (NCIJTF) performs on a daily basis. Mandated by the President in 2008, the NCIJTF serves as national focal point for coordinating, integrating, and sharing pertinent information related to cyber threat investigations among 19 federal agencies. The FBI aims to strengthen and solidify the NCIJTF as the cybersecurity center for coordinating cyber threat investigations and disruption operations. The NCIJTF involves senior personnel from key agencies, including deputy directors from the National Security Agency, the Department of Homeland Security, the Central Intelligence Agency, the U.S. Secret Service, and U.S. Cyber Command. Reinforcing the role of the NCIJTF on cross-government cyber threat information sharing and coordination is a key priority for the FBI.

Lastly, the FBI is working to strengthen local and national information sharing and collaboration efforts in support of network defense, intelligence operations, and disruption operations. And I cannot make the following statement frequently enough: the private sector is an essential partner if we are to succeed in defeating the cyber threat our nation confronts. I will discuss in more detail some of our collaboration efforts with the private sector shortly.

Current FBI Efforts to Combat Cyber Threats

The FBI is engaged in a host of efforts to combat cyber threats, from efforts focused on threat identification and sharing inside and outside of government, to our internal emphasis on developing and retaining new talent and changing the way we operate to evolve with the cyber threat. I would like to take this opportunity to highlight a few of the ways we at the FBI are confronting this threat head on.

FBI Liaison Alert System

As I alluded to earlier in my testimony, the threat of botnets provides a good example of how the FBI is proactively working with industry partners to combat cyber threats. To further assist with network defense and mitigation of botnets, the FBI created a document called the FBI Liaison Alert System message, or FLASH. Through the system, the FBI releases high confidence data to the private sector with indicators and alerts related to computer intrusions and DDoS attacks. From April 2013 to July 2014, the FBI disseminated 34 FLASH messages, about 20 of which dealt with threats against the financial sector. The FBI disseminated, among other information, indicators for approximately 115,000 compromised systems in these FLASH messages. These declassified, technical indicators, associated with intrusions, are meant to enable industry partners to be on the lookout for and defend their infrastructure from nefarious traffic on their networks.
The FBI provided these FLASH messages to key partners across affected critical infrastructure sectors, to include: Tier 1 and 2 Internet Service Providers (ISPs), Domain Name Server (DNS) root

server operators, top-level domain (TLD) operators, and Five Eyes partners. When the FBI receives credible information regarding a threat to U.S. critical infrastructure, FBI coordinates with DHS to discuss and deconflict victim notification and mitigation strategies, at times involving other agencies, such as the Department of Treasury, as well.

Guardian Victim Analysis Unit

The FBI's Guardian Victim Analysis Unit (GVAU) is a direct response to the President's 2013 Executive Order 13636, which called for increases in the volume, timeliness, and quality of cyber threat information shared with U.S. private sector entities so that these entities may better defend themselves against cyber threats. To help aid these entities and to enhance private sector information sharing efforts, the FBI established Cyber Guardian, a series of applications that enables actors in and outside of government to share threat information. One Cyber Guardian application is available on a Secret enclave, and two applications known as eGuardian and iGuardian/InfraGard — both operating at the unclassified level — are available to State, Local, Tribal, and Territorial (SLTT) entities, and to the private sector, respectively. The Cyber Guardian applications provide a means for the FBI to rapidly disseminate reports on cyber threat activity, in addition to a platform for coordination and deconfliction of cyber threat information.

The Internet Crime Complaint Center

Established in 2000, the Internet Crime Complaint Center (IC3) is a partnership between the FBI and the National White Collar Crime Center meant to serve as a vehicle to receive, develop, and refer criminal complaints regarding the rapidly expanding arena of cyber crime. During its infancy, the IC3 received approximately 2,000 victim complaints per month. Now the IC3 receives approximately 800 complaints a day, with over 244,000 complaints received to date for the 2014 calendar year. In 2013, the IC3 received 262,813 consumer complaints with losses in excess of $781 million. The IC3 database currently houses more than 3.15 million consumer complaints dating back to its inception in 2000.

The Domestic Security Alliance Council

The Domestic Security Alliance Council (DSAC) is a strategic partnership between the U.S. government and U.S. private industry, formed with the goal of increasing security by enhancing communications and promoting the timely and effective exchange of security information among its constituents. The DSAC advances the FBI's mission of preventing, detecting, and deterring criminal acts by facilitating strong, enduring relationships among its private industry members, FBI headquarters divisions, FBI field offices, DHS headquarters, DHS fusion centers, and other federal government entities.

The National Cyber-Forensics and Training Alliance

The National Cyber-Forensics and Training Alliance (NCFTA) is composed of representatives of industry, academia, and the FBI, all working together to collaborate on combating cyber crime. The NCFTA provides a unique environment for information sharing between law enforcement, private industry, and academia. The NCFTA is a non-profit group whose members include ISPs, banks,

retailers, and a whole host of other industry representatives, along with law enforcement and academia, with a mission to identify cyber threats and share information for mitigation and neutralization purposes. The NCFTA provides a one-of-a-kind opportunity for subject matter experts to address global cyber threats such as botnets, spam, and malware. Because of its non-profit status, the group can share information in a neutral environment, develop a strategic understanding of the threat, and work to address cyber threats collaboratively.

National Industry Partnership Unit

The FBI established an entity known as the National Industry Partnership Unit to develop partnerships through the InfraGard program between the FBI and private sector, academic, and other public entities, to support the FBI's investigative programs. Established in the Cleveland field office in 1996, InfraGard was initially a local effort to gain support from the information technology industry and academia for the FBI's investigative efforts in the cyber arena. InfraGard soon expanded to other FBI field offices, and in 2003 the Cyber Division assumed responsibility for the program. InfraGard and the FBI have developed a relationship of trust and credibility in the exchange of information concerning various terrorism, intelligence, criminal, and security matters. InfraGard members gain access to information that enables them to protect their assets and in turn give information to the government that facilitates its responsibilities in preventing and addressing terrorism and other crimes. This relationship supports information sharing at both the national and local levels, with the aim of increasing the level of information and reporting between InfraGard members and the FBI on matters related to counterterrorism, cyber crime, and other major crime programs.

Charting the Cyber Future

The future cyber threatscape will certainly be complex — based on recent advances in the sophistication of our adversaries, both state and non-state, it is hard to imagine what this threatscape will look like 10 or even 20 years down the road. Nevertheless, we in the FBI pride ourselves on being a forward looking organization, and adapting to the challenges we face. The FBI Cyber Division — our agents, computer scientists, analysts, and personnel — are all working hard to outpace such threats on a daily basis, identifying, pursuing, and defeating our adversaries, wherever in the world they might be.

There are, however, a number of ways that Congress might seek to aid us in our efforts. In particular, I would like to enumerate three concerns that new legislation or amendments to existing legislation could address that would strengthen our ability to combat cyber threats, as follows:

- Updating the Computer Fraud and Abuse Act. The Computer Fraud and Abuse Act (CFAA) constitutes the primary federal law against hacking, protecting the public against criminals who hack into computers to steal information, install malicious software, and delete files. The CFAA was first enacted in 1986, at a time when the problem of cybercrime was still in its infancy. Over the years, a series of measured, modest changes have been made to the CFAA to reflect new technologies and means of committing crimes and to equip law enforcement with the tools to respond to changing

threats. The CFAA has not been amended since 2008, however, and the intervening years have again created the need for the enactment of modest, incremental changes. The Administration has proposed several such revisions to keep federal criminal law up-to-date with rapidly-evolving technologies.

Cyber threats adapt and evolve at the speed of light, and we need laws on the books that reflect the most current means by which cyber actors are committing crimes. Updating the CFAA to reflect these changes would help strengthen our ability to punish, and therefore to deter, the crimes we seek to prevent.

Data Breach Notifications. We believe there is a strong need for a uniform federal standard holding certain types of businesses accountable for data breaches and theft of electronic personally identifiable information. Businesses should, for example, be required to provide prompt notice to consumers in the wake of a certain cyber attacks. Such a standard would not only hold businesses accountable for breaches, but would also assist in FBI and other law enforcement efforts to identify, pursue, and defeat the perpetrators of cyber attacks.

Information Sharing. Although the government and the private sector already share cyber threat information on a daily basis, legislation can enhance the value and benefit of these information sharing relationships. The government and the private sector both have critical and unique insights into the cyber threats we face, and sharing these insights is necessary to enhance our mutual understanding of the threat. Similarly, the operational collaboration required to identify cyber threat indicators and to mitigate intrusions requires the exact type of sharing we seek in the first place. As such, the FBI supports legislation that would establish a clear framework for sharing and reduce risk in the process, in addition to providing strong and straightforward safeguards for the privacy and civil liberties of Americans. U.S. citizens must have confidence that threat information is being shared appropriately, and we in the law enforcement and intelligence communities must be as transparent as possible. We also want to ensure that all the relevant federal partners receive the information in real time.

The bottom line, however, is that current levels of information sharing are insufficient to address the cyber threats we face, specifically with regards to the financial sector. The U.S. is currently facing sophisticated, well-resourced adversaries, and minimum security requirements are needed to harden our critical infrastructure networks. The government and private sector should collaborate to develop these requirements, and we believe that legislation would help to further these ends. There are a host of statutory and regulatory restrictions as well that provide narrowly tailored liability protections for appropriate cyber information sharing. Further, there are a number of regulatory and statutory concerns that private actors may express when it comes to sharing cyber threat information with the government, and new legislation can and should be crafted to address these concerns. The events of the last year, and the continuing high-profile cyber attacks on major American companies, should serve to highlight the need for new engagement against cyber threats on every level possible.

In the absence of the passage of cybersecurity legislation, however, the administration is taking steps in the right direction to ensure that we can share information, in a practical and meaningful way. One such step is Executive Order (EO) 13636, entitled "Improving Critical Infrastructure Cybersecurity" and which I addressed briefly earlier, signed by the President in February 2013 and designed to provide critical infrastructure owners and operators with assistance to address cyber threats and manage risks. The EO calls for the government to collaborate more closely with industry by sharing information about cyber threats and jointly developing a framework of cybersecurity standards and best practices. One of the EO's main goals is to improve government information sharing with critical infrastructure owners and operators regarding cyber threats, including attack signatures and other technical data. The FBI would, however, welcome more active engagement from Congress on these matters. Although the EO is a step in the right direction, robust cybersecurity legislation is still needed. As partners across the government and private sector have explored the ways we can operate, under existing laws, to implement the requirements of the EO, we are well positioned to have a more informed dialogue with Congress, and to improve our ability to address cyber threats.

Conclusion

In conclusion, Mr. Chairman, the FBI is focusing our resources, expanding our presence at the local, national and international levels, and engaging in cooperation with the private sector and intergovernmental collaboration. As the Committee knows well, we face considerable challenges in our efforts to combat cyber crime, and yet we remain optimistic that by identifying, pursuing, arresting and prosecuting these offenders we will defeat our cyber adversaries and continue to succeed in neutralizing these threats. My colleagues at the FBI and I look forward to working with the Committee and with Congress in protecting our nation from the evolving threat posed by cyber actors. Thank you again for the opportunity to appear before you today. I would be happy to answer any questions you may have.