AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. HRG. 113–583

CYBERSECURITY: ENHANCING COORDINATION TO PROTECT THE FINANCIAL SECTOR

HEARING

BEFORE THE

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

ONE HUNDRED THIRTEENTH CONGRESS

SECOND SESSION

ON

EXAMINING THE COORDINATION AND INFORMATION SHARING BETWEEN THE FINANCIAL SERVICES INDUSTRY AND THE SECRET SERVICE, DEPARTMENT OF HOMELAND SECURITY, FEDERAL BUREAU OF INVESTIGATION, THE TREASURY DEPARTMENT, THE FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL, FEDERAL REGULATORY AGENCIES, AND LAW ENFORCEMENT IN IDENTIFYING, MONITORING, AND RESPONDING TO CYBERTHREATS

DECEMBER 10, 2014

Printed for the use of the Committee on Banking, Housing, and Urban Affairs

Available at: http://www.fdsys.gov/

U.S. GOVERNMENT PUBLISHING OFFICE

93–566 PDF WASHINGTON : 2016

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS

TIM JOHNSON, South Dakota, *Chairman*

JACK REED, Rhode Island
CHARLES E. SCHUMER, New York
ROBERT MENENDEZ, New Jersey
SHERROD BROWN, Ohio
JON TESTER, Montana
MARK R. WARNER, Virginia
JEFF MERKLEY, Oregon
KAY HAGAN, North Carolina
JOE MANCHIN III, West Virginia
ELIZABETH WARREN, Massachusetts
HEIDI HEITKAMP, North Dakota

MIKE CRAPO, Idaho
RICHARD C. SHELBY, Alabama
BOB CORKER, Tennessee
DAVID VITTER, Louisiana
MIKE JOHANNS, Nebraska
PATRICK J. TOOMEY, Pennsylvania
MARK KIRK, Illinois
JERRY MORAN, Kansas
TOM COBURN, Oklahoma
DEAN HELLER, Nevada

CHARLES YI, *Staff Director*
GREGG RICHARD, *Republican Staff Director*

LAURA SWANSON, *Deputy Staff Director*
JEANETTE QUICK, *Counsel*
PHIL RUDD, *Legislative Assistant*

GREG DEAN, *Republican Chief Counsel*
JARED SAWYER, *Republican Counsel*
TRAVIS HILL, *Republican Counsel*

DAWN RATLIFF, *Chief Clerk*
TROY CORNELL, *Hearing Clerk*
SHELVIN SIMMONS, *IT Director*
JASON T. PARKER, *GPO Detailee*
JIM CROWELL, *Editor*

C O N T E N T S

WEDNESDAY, DECEMBER 10, 2014

	Page
Opening statement of Chairman Johnson	1
Opening statements, comments, or prepared statements of:	
Senator Crapo	2

WITNESSES

Brian Peretti, Director for the Office of Critical Infrastructure Protection and Compliance Policy, Department of the Treasury	4
Prepared statement	26
Responses to written questions of:	
Senator Crapo	48
Senator Menendez	49
Senator Warner	51
Phyllis Schneck, Deputy Under Secretary for Cybersecurity and Communications, National Protection and Programs Directorate, Department of Homeland Security	6
Prepared statement	29
Responses to written questions of:	
Senator Crapo	53
Senator Menendez	58
Senator Warner	59
Valerie Abend, Senior Critical Infrastructure Officer, Office of the Comptroller of the Currency	8
Prepared statement	33
Responses to written questions of:	
Senator Crapo	64
Senator Menendez	66
Senator Warner	70
William Noonan, Deputy Special Agent in Charge, Cyber Operations Branch, Criminal Investigative Division, Secret Service	10
Prepared statement	39
Responses to written questions of:	
Senator Crapo	75
Senator Warner	76
Joseph M. Demarest, Jr., Assistant Director, Cyber Division, Federal Bureau of Investigation, Department of Justice	11
Prepared statement	41

ADDITIONAL MATERIAL SUPPLIED FOR THE RECORD

Letter to Agencies submitted by Chairman Johnson and Senator Crapo	79
Letter of response submitted by Joint Agencies	81
Letter of response submitted by the Department of the Treasury	83
Letter of response submitted by Federal Deposit Insurance Corporation	85
Letter of response submitted by the National Credit Union Administration	91
Letter of response submitted by the Board of Governors of the Federal Reserve System	97
Letter of response submitted by the Office of the Comptroller of the Currency	102
Letter to the Conference of State Bank Supervisors submitted by Chairman Johnson and Senator Crapo	109
Letter of response submitted by the Conference of State Bank Supervisors	111

Page

Statement submitted by the National Association of Federal Credit Unions 121
Statement submitted by the Securities Industry and Financial Markets Association 123
Statement submitted by the Independent Community Bankers of America 130
Protecting Merchant Point of Sale Systems During the Holiday Season 132

CYBERSECURITY: ENHANCING COORDINATION TO PROTECT THE FINANCIAL SECTOR

WEDNESDAY, DECEMBER 10, 2014

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

The Committee met at 10:04 a.m., in room SD–538, Dirksen Senate Office Building, Hon. Tim Johnson, Chairman of the Committee, presiding.

OPENING STATEMENT OF CHAIRMAN TIM JOHNSON

Chairman JOHNSON. 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 cybercrime, they are uniquely interconnected with major sectors of the economy. Cyber attacks 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 cyber attacks. I am entering each agency's response into the record and I expect that regulators continue 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 cyberthreats and how to improve information shar-

ing. 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 the many years.

I now turn to Senator Crapo for his opening statement.

STATEMENT OF SENATOR MIKE CRAPO

Senator CRAPO. Thank you, Mr. Chairman, and I appreciate your kind remarks. I share the same feelings that you have indicated with regard to not only our work together, but our staff, and I have developed great friendships with all of you. I appreciate that.

This morning, we are holding what may be the final Banking Committee hearing that will be chaired by you, and I just have to reiterate what a pleasure it has been to work with you. You and I do have a great working relationship and it has been a privilege to serve with you in the past in a number of contexts, but in this Congress as Chairman and Ranking Member, and I wish you the best of luck in the future.

Chairman JOHNSON. Thank you.

Senator CRAPO. 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 60 percent of companies overall have experienced a breach in the last 2 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 preauthorized 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 is where the money is. The largest banks are under constant attack, every day, and spent 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 just a 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.

JPMorgan Chase, the Nation's largest bank by assets, was attacked this summer when hackers stole personal information from 76 million households and seven million small businesses. While this is certainly concerning, I am encouraged that despite spending weeks inside JPMorgan's system, 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 Secretary Lew, successful attacks on our financial system would compromise market confidence, jeopardize the integrity of the data, and pose a threat to financial security.

Many of your agencies have made cybersecurity a priority and I applaud you for that. 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 cyberthreats. 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 be sure that 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, and intelligence community, and banking regulators must all work together effectively to maximize the speed of information sharing and to minimize the risk of damage from cyber attacks.

I hope to learn, also, 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 the testimony of each of our witnesses today.

Chairman JOHNSON. Thank you, Senator Crapo.

Are there any other Members who would like to give a brief opening statement?

[No response.]

Chairman JOHNSON. I would like to remind my colleagues that the record will be open for the next 7 days for additional statements and any other materials you would like to submit.

Now, I will introduce our witnesses. Brian Peretti is Director for the Office of Critical Infrastructure Protection and compliance Policy at the U.S. Department of the Treasury.

Phyllis Schneck is Deputy Under Secretary for Cybersecurity and Communications for the National Protection and Programs Directorate at the Department of Homeland Security.

Valerie Abend is the Senior Critical Infrastructure Officer for the Office of the Comptroller of the Currency.

William Noonan is Deputy Special Agent in Charge of the Cyber Operations Branch of the Secret Service's Criminal Investigative Division.

Joseph Demarest, Jr., is Assistant Director of the Cyber Division at the Federal Bureau of Investigation.

I would like to ask the witnesses to please keep your remarks to 5 minutes. Your full written statements will be included in the hearing record.

Mr. Peretti, you may begin your testimony.

STATEMENT OF BRIAN PERETTI, DIRECTOR FOR THE OFFICE OF CRITICAL INFRASTRUCTURE PROTECTION AND COMPLIANCE POLICY, DEPARTMENT OF THE TREASURY

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

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 of 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.

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. Presidential Policy Directive 21 was created in 2013 to advance a national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure. This Directive reaffirms Treasury's role as the sector-specific agency for financial services, recognizing its financial services expertise and the value of its day to day engagement with financial institutions in building and enhancing security and resiliency partnerships.

PPD–21, along with the President's 2013 Executive Order on cybersecurity, forms the basis for Treasury's mission to protect critical infrastructure from cyber incidents. This work depends on strong partnerships with others in Government and industry. To focus our work, we collaborate closely with other Government agencies and the private sector. To coordinate with Government, we chair the Financial and Banking Information Infrastructure Committee, a committee of 18 Federal and State regulators, and participate in interagency discussions chaired by the White House. To coordinate with the sector, we work with the Financial Services Sector Coordinating Council, which brings together private-sector institutions, trade associations, and individual firms to discuss security and resiliency policy.

Now that I have described who we work with, I would like to spend the remainder of my time today talking specifically about the substantial outcomes of our work.

First, I would like to highlight our work to promote cybersecurity information sharing. Sharing technical and strategic information about cyber instances and threats is one of the most effective tools that the Government has to support the mitigation of cyber instances and improve the operational resilience of the financial sector. In order to ensure that the sector receives the best 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 Sector Cyber Intelligence Group, which works with the interagency and private-sector partners to provide timely and actionable information, including threat indicators, to the financial services sector.

The financial services 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 Government should look further to encourage the growth of the FS–ISAC and ISACs in other sectors.

The President's Executive Order 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 this sector could provide input into the framework. Today, the NIST Cybersecurity Framework is a voluntary blueprint that firms of all sizes can use to evaluate, maintain, and improve the resilience of their computer systems and reduce cyber-risk.

Treasury continues to encourage financial service firms to utilize the framework, including by holding business partners, suppliers, and customers accountable to the risk management approach. In particular, efforts by SIFMA by develop auditable standards of the framework may be beneficial in supporting broad adoption of best practices.

Finally, to improve incident management, Treasury believes the roles and responsibilities for different entities must be more clearly defined and regularly tested and refined. In order to prepare for cybersecurity instances, Government agencies and private-sector entities must work together to develop and refine response protocols that clearly delineate roles and responsibilities.

Similarly, exercises are necessary to improve incident plans and develop muscle memory in the organizations with the personnel responsible for managing the incidences. 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 preparedness and continually improve response mechanisms.

In conclusion, while significant progress has been made to improve financial sector cybersecurity, we know 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 policymakers to determine the best course of action to address these issues as they are identified.

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

Chairman JOHNSON. Thank you.

Dr. Schneck, please proceed with your testimony.

STATEMENT OF PHYLLIS SCHNECK, DEPUTY UNDER SECRETARY FOR CYBERSECURITY AND COMMUNICATIONS, NATIONAL PROTECTION AND PROGRAMS DIRECTORATE, DEPARTMENT OF HOMELAND SECURITY

Ms. SCHNECK. Good morning, Chairman Johnson, Ranking Member Crapo, and distinguished Members of the Committee. I am very pleased to be here today to talk with you about the role of DHS in cybersecurity, the way we work with these critical issues with the financial sector.

Secretary Johnson always reminds us that cybersecurity is a part of homeland security, and we are fortunate within the Department of Homeland Security to not only have where I am, with the National Protection and Programs Directorate, a non-law enforcement piece focused on the protection and resilience of critical infrastructure, which includes cybersecurity and communications, but also law enforcement with Homeland Security Investigations as well as the U.S. Secret Service, some of the finest law enforcement investigators on the planet for financial crimes.

So, I speak with you today from the National Protection and Programs Directorate on the non-law enforcement side and the role that we play. If you look at our National Cybersecurity and Communications Integration Center, which I will call the NCCIC, that is the core of cyber awareness, information coming in from victims, from partners, from vendors, from all of our interagency partners, whether it is the FBI, the intelligence community, from our in-house law enforcement, from Secret Service, from Homeland Security Investigations, all of our private-sector partners, all the State and local.

Twenty-four-seven, all this information is coming in. We see something, say something. Just like the aviation industry, we learn from every event, whether people go out and help somebody stay online, we learn from that and it protects everybody else, or whether the programs we have to protect the Government in, as you said, perimeter defense, those collect data with the full collaboration with privacy and civil liberties. We collect as much data as we are allowed to understand, just as weather forecasters do, what we need to do to have information propagated ahead to protect the next victim. We do that for Government and private sector, as our programs look at perimeter defense for Government agencies as well as internal, and we are also able to protect private sector with Government data.

We also house the United States Computer Emergency Readiness Team, or the U.S.–CERT, people that get on airplanes to keep people online, fix and respond. Our role is to respond and mitigate cyberthreat, make sure people stay online, whether it is systems that keep the lights on, the water running, or cyber systems in general. We also have the Industrial Control System CERT housed

in Idaho Falls which looks at those very control systems that do keep physical infrastructure alive. So, those electronic systems that can be breached and are being targeted, keeping those online.

If we look at what is important here, it is speed. Our adversary enjoys an agility that we do not have. My background is in high-performance computing and cryptography, but also really looking at how you build intelligence and situational awareness, and it was my job at my previous company, a large cyber provider, to do the information sharing and to lead for the company when we shared information with Government and law enforcement. And, I learned there this is a very complex issue and what we can do to help build resilience and help change the profit model for the adversary and make that much smaller, make this not worth their time, is to mitigate faster. This is about speed.

And, the way we can balance that is if the NCCIC and our ability to respond as a Government, as a whole of Government, if you use the civilian non-law enforcement side to ingest the cyber activity, as we are doing, and the first place to report, we can then begin the mitigation while people work with their lawyers to figure out how to work with law enforcement. They are equally important. We must prosecute bad guys, but we also have to make sure that we do not waste time in the middle with the lawyers on the law enforcement side so the companies can work with them and have that understood. We have to make sure we are already mitigating in real time.

So, the financial sector has done a lot of work to help us use real time, as they call it, or machine time protocols, faster than the attacks, to help networks be smarter about what is coming to them. Those can already be working while law enforcement is then deciding how they want to prosecute the case, because we want that civilian non-law enforcement reporting. Then we fan out all the data to the Secret Service, Homeland Security Investigation, FBI, intelligence community, and vendor partners that sit within the NCCIC.

But, we have already started the mitigation, and it is this very speed that the FISMA modernization will help us to achieve, as well, helping us to clarify in statute the authority that we have to defend these networks and ensure that that, again, that mitigation has already started. And, I do thank the Senate for passing a version of this bill that could help us get there.

I also want to point out what is important in our vision is the situational awareness, understand what is happening right now in cybersecurity, collect that data, work with private-sector partners, work with the financial sector, leverage the great work that this sector has build in trust, in automated machine-to-machine communication, in getting to the bottom of legal issues so that we can all talk and, again, enjoy the agility that usually the adversary only enjoys and enable this to work cross-sector. And, to do that, we also have to get to the small to medium business and use that Executive Order 13636 and our voluntary framework to enable best practices in cybersecurity to then enable all of this information sharing to get to those companies, as well, so that we can learn from them.

In conclusion, we need to continue the great work that the financial sector has done such a tremendous job on with us as a whole of Government, and I look forward to more partnership and to any questions you may ask.

Chairman JOHNSON. Thank you.

Ms. Abend, please proceed with your testimony.

STATEMENT OF VALERIE ABEND, SENIOR CRITICAL INFRASTRUCTURE OFFICER, OFFICE OF THE COMPTROLLER OF THE CURRENCY

Ms. ABEND. Chairman Johnson, Ranking Member Crapo, and Members of the Committee, I am pleased to be here today to discuss the important issue of cybersecurity and what the OCC and the Federal Financial Institutions Examination Council has been doing to address cyberthreats and vulnerabilities. These efforts include information sharing for the benefit of the banking industry, regulatory community, and the financial system overall.

But, first, I want to thank Chairman Johnson for his many years of leadership in the financial services arena and wishing him well in his future endeavors.

There are few issues more important to the OCC and to our country's economic and national security than the risks posed to financial institutions by cyber attacks. We live in a world of rapidly evolving technology in which consumers store information in the cloud, pay bills with their computers, and use their cell phones to make purchases at the mall. However, these conveniences have also introduced new vulnerabilities into the financial system, making it more difficult to protect financial institutions and customer information from cyber attacks.

As risks evolve, financial institutions must adapt. Our job as regulators is to ensure that institutions we supervise do everything possible to identify and manage vulnerabilities to these cyberthreats and our ability to response.

To meet that objective, the OCC's supervisory framework includes ongoing monitoring and information sharing with other regulators, Government agencies, and banks regarding emerging threats and changes to the risk landscape. It also includes development and continual refinement of standards and guidance that set forth our expectations as to how banks should safeguard their systems and their customers' information, including at their third-party service providers.

To complement these efforts, we are committed to maintaining a cadre of highly trained IT examiners. While all OCC examiners receive training on information technology risk management, we also cultivate examiners with specialized skills and experience to focus on the evolving information security and other technology risks in bank operations. Our examiners assess bank compliance with our supervisory expectations to ensure that they are appropriately managing risk, and when necessary, directing them to take corrective action.

Comptroller of the Currency Tom Curry chairs the FFIEC, and one of the Council's top priorities is to strengthen the resilience of regulated institutions to cyber attacks. Under the Comptroller's leadership, the FFIEC created the Cybersecurity and Critical Infra-

structure Working Group. The Working Group helps the FFIEC members collaborate on cyber-related examination policy, training programs, coordination of responses to cybersecurity incidents, and information sharing and awareness efforts.

The Working Group has been quite active since its inception. In addition to sponsoring awareness and training webinars, it has drafted statements advising financial institutions about the variety of specific threats and vulnerabilities, including the Heartbleed and Shellshock vulnerabilities and attacks on ATMs.

The FFIEC, on behalf of its members, also recommended that all institutions join the Financial Services Information Sharing and Analysis Center, a public–private partnership which provides information about current threats and vulnerabilities.

A major initiative of the Working Group was to pilot a cybersecurity examination work program at more than 500 community institutions. This cybersecurity assessment evaluated the operating environment for each institution and assessed its overall level of preparedness. The results of the assessment will help FFIEC members make informed decisions about how they prioritize actions to enhance the effectiveness of cybersecurity-related supervisory programs, guidance, and examiner training. The results are summarized in a General Observations document that provides observations and questions that banks, boards of directors, and CEOs should consider when assessing their cybersecurity preparedness.

The Comptroller has emphasized the importance of communication, collaboration, cooperation in all aspects of our mission, but nowhere is communication and collaboration more important than in the realm of cybersecurity, where the threats transcend agency jurisdictions and industry boundaries. The OCC is an active member of several information-sharing bodies. We also recognize the importance of maintaining relationships with law enforcement and intelligence communities to share information through open lines of communication. We use information-sharing forums, relationships with Government agencies, and information from our exams to inform our supervision.

Finally, the recent breaches at large retailers highlight the need for improved cybersecurity for merchants. When breaches occur in merchant systems, we believe that merchants should contribute to efforts to make affected consumers whole so that banks, particularly community institutions, do not disproportionately shoulder the cost. Additionally, financial institutions share dependencies with other sectors, such as telecommunications and energy, and as such, we support efforts to ensure commensurate standards for those important critical infrastructures.

In closing, we are committed to refining our supervisory processes and to participating in a range of information-sharing forums to keep abreast of and respond to cyberthreats. Combating 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.

Thank you, and I would be happy to answer your questions.

Chairman JOHNSON. Thank you.

Mr. Noonan, please proceed with your testimony.

STATEMENT OF WILLIAM NOONAN, DEPUTY SPECIAL AGENT IN CHARGE, CYBER OPERATIONS BRANCH, CRIMINAL INVESTIGATIVE DIVISION, SECRET SERVICE

Mr. NOONAN. Good morning, Chairman Johnson, Ranking Member Crapo, and distinguished Members of the Committee. Thank you for the opportunity to testify with interagency partners regarding the ongoing threat of cybercrime to our Nation's financial services sector.

Chairman Johnson, while the Secret Service has only testified a handful of times before this Committee in recent years, we all appreciate the work you have done on behalf of American consumers and the financial services industry. We wish you the best in retirement.

The founding mission of the Secret Service is to protect our Nation's financial payment system from malicious activity. As it has evolved from paper to plastic to now digital information, so, too, has the Secret Service's investigative mission. Today, financial transactions of all types depend heavily on information technology. As such, criminals motivated by greed have adapted their methods and are increasingly using cyberspace to exploit these systems to engage in fraud and other illegal activities.

The wealth accrued by the world's most skillful cybercriminals is staggering. Some have become multimillionaires through their criminal endeavors and are not stopping there. Cyber investigative programs are being outpaced by criminals who reinvest their illicit proceeds to support their malicious cyber activity.

Despite substantial investments in cybersecurity by our leading financial institutions, we continue to see many fall victim to cybercriminals. In considering all the high-profile cyber incidents over the last year, it is clear that defense alone is inadequate. Proactive law enforcement investigations are essential in Combating these threats.

The Secret Service has observed transnational cybercriminals who, over the past 10 years, have grown into highly capable adversaries. They command botnets consisting of millions of computers. They routinely compromise highly secure computer networks. And, they accomplish increasingly profitable operations. Last year, we witnessed an unlimited ATM cash-out operation that was unprecedented in scope. The operation involved a cybercriminal organization which stole $40 million in less than 11 hours through a synchronized effort executed across 24 countries. Rich off the money they have stolen from Americans, our Nation faces increasing risk that sophisticated cybercriminals may coordinate their unique skill sets and apply their combined expertise to conduct cyber attacks against our critical infrastructure.

Achieving a different outcome drives our work at the Secret Service. We focus on proactively investigating the most capable cybercriminals. To defeat these transnational groups, we target their criminal infrastructure and leaders. For example, last year, the Secret Service shut down the digital currency platform Liberty Reserve for allegedly running a $6 billion money laundering scheme. Prior to its shutdown, the currency had more than 5.5 million user accounts and approximately 55 million transactions. The founder of Liberty Reserve, Arthur Budovsky, was extradited from

Spain to the United States in October. Mr. Budovsky is among seven individuals charged in the indictment. Four other codefendants pled guilty and are awaiting sentencing.

In addition, this past year, the Secret Service worked with a key law enforcement partner to apprehend one of the primary masterminds alleged to be behind a series of unlimited ATM cash-out operations, including the one I previously mentioned. Since his arrest, there has not been another successful operation of this kind. These arrests prove that transnational cybercriminals are not beyond the reach of U.S. law enforcement. Over the past 5 years, the Secret Service arrested nearly 6,000 cybercriminals and prevented nearly $12 billion in potential fraud losses.

The Secret Service actively shares information to disrupt cybercriminal schemes. This year, as a result of information discovered through just one of our ongoing cybercrime investigations, we notified over 200 U.S. organizations of cybercriminal activity targeting their networks. These include retailers, financial institutions, Government agencies, IT companies, health care providers, and military agencies.

Our work does not stop with victim notification. The Secret Service also widely shares actionable cybersecurity information through our close partnerships with the Department of Treasury, the Department of Justice, and DHS's National Cybersecurity and Communications Integration Center. This is in addition to our work with industry groups like the FS–ISAC, Financial Services Roundtable, and the Business Executives for National Security.

Through the dedicated efforts of our special agents, our Electronic Crimes Task Forces, and our public and private-sector partners, the Secret Service will continue its efforts to counter the growing threat posed by cybercriminals.

Thank you for the opportunity to testify on this important topic, and I look forward to your questions.

Chairman JOHNSON. Thank you.

Mr. Demarest, please proceed with your testimony.

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

Mr. DEMAREST. Last, but certainly not least, the FBI.

[Laughter.]

Mr. DEMAREST. Good morning, Ranking Member Crapo and distinguished Members of the Committee. And to Chairman Johnson, I, and we in the FBI, thank you, sir, for your long and distinguished service to the American people. Thank you, sir.

I am honored to appear before you today to discuss cyberthreats 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 testimony this morning, 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 specifically, a threat that challenges traditional models of law enforcement and the intelligence communities. Today's cyber actors, from Nation-States to criminal groups and individuals, find

themselves virtually unconstrained by time, distance, and physical location.

I would like to start with a brief overview of the Cyber Division of the FBI. In general, our mission falls into three separate but primary buckets. First, we identify the cyber actors perpetrating the harm and the role of cybercrime and cyber espionage. This is often the most difficult step, as cyberthreats use various methods to attempt to hide virtually in plain sight.

Second, we pursue these actors, tracking their activity both online and off. We utilize collaborative partnerships across the Federal Government, with international partners, and certainly 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 by using a variety of cutting-edge techniques to locate them no matter where they are on the planet.

Last, with the aid of partnerships and our unique authorities, we defeat the cyber adversaries through a full range of methods, from prosecution to disruption, here and abroad.

As the Members of this Committee are aware, the threat from cyber actors continue to advance in sophistication. I would like to spend the rest of my brief testimony highlighting a few of the ways the FBI, along with our partners here in Government and in organizations like the Securities Industry and Financial Markets Association, SIFMA, the Financial Services Sector Coordinating Council, FSSCC, the Financial Services Information Sharing and Analysis Center, FS–ISAC, and the Financial Services Roundtable are collaborating with each other and with the private sector to protect the Nation and the financial sector, in particular, from cyberthreats.

Specifically, I would like to talk about botnets and the criminal underground which harness the power of enormous webs of computers for malicious purposes and the FBI's efforts to address them through Operation Clean Slate.

As I speak, since 2001, 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 to date. Approximately 500 million computers are infected globally per year, translating to 18 victims per second. Botnets are continually used to attack the financial sector through "denial of service" attacks, or DDoS attacks, and the FBI has been deeply involved in keeping such attacks from inflicting lasting damage.

Beginning in September of 2012, for example, actors launched powerful DDoS attacks from a botnet to target major U.S. banking institutions. From March 2013 through July 2014, the FBI conducted approximately 36 classified threat briefings regarding the attacks on private-sector financial institutions and Government agencies, including DHS, Department of Treasury, the FDIC, and the Federal Reserve. The initial classified briefing held in March 2013 was attended by over 300 chief information security officers. This type of outreach is now the norm for us. We share by rule, not exception. Based on imminent threats to the financial sector in early 2014, the FBI provided classified threat briefings in March, April, and July to a total of 145 financial institutions.

Further, the FBI worked closely with DHS to issue a Joint Indicator Bulletin, or Bulletins, or JIBs, as they are affectionately called internally, to the U.S. banks, which included thousands of IP addresses that participated in the attacks. Throughout this campaign, the FBI held significant outreach efforts to brief bank net defenders through a series of classified briefings. These briefings, conducted by FBI, DHS, and Treasury representatives, provided the bank security personnel the context of the DDoS threat and enabled the banks to share best practices with their peers in real time.

To further assist with network defense of botnets, the FBI created a document called the FBI Liaison Alert System Message, or FLAS. Through this system, the FBI releases high-confidence data to the private sector with indicators and alerts related to computer intrusions and DDoS attacks. From April of 2013 through July of this year, the FBI disseminated 34 FLAS messages, about 20 of which dealt with threats directly focused on the financial sector. The FBI disseminated, among other information, indicators for approximately 115,000 compromised systems in these messages.

We at the FBI, in short, are doing everything in our power to keep pace with the threat against the financial sector and our Nation. Our agents, computer scientists and analysts, and professional staff are all working hard to outpace the threats on a daily basis by identifying, pursuing, and defeating our adversaries wherever they may be in the world. The FBI and our partners throughout the Government have all made significant progress in recent years in collaborating within the cyber domain and we look forward to working with the Committee and Congress in protecting our Nation from these evolving threats.

I thank you again for this opportunity and I look forward to your questions. Thank you.

Chairman JOHNSON. Thank you all for your testimony. I will now ask the clerk to put 5 minutes on the clock for each Member.

Director Schneck, we have heard that cyber attacks often have impacts on more than one critical infrastructure sector. What is DHS doing to facilitate information sharing and best practices among sectors? Are there other sectors that are particularly important to coordinate with the financial services sector?

Ms. SCHNECK. Thank you, sir, and I also regret that my first time talking to you in this forum is my last, but thank you——

Chairman JOHNSON. Yes.

Ms. SCHNECK. So, a great question. One of the reasons, I believe, that we exist in our NCCIC, that National Cybersecurity Coordination, Communication, Integration Center, is really to look at how we take these attack attempts and how we take the data that we see and we take the actual attacks and make sure that not only we respond and mitigate quickly, but that we share that information out across sectors, because we are all connected. If we had to figure out whether finance was more important than electricity or water or gas, we would have a hard time doing that because they are all so interdependent, and you also add a complexity that a lot of the signaling systems, the electronics that control circuits opening and closing to make, literally, decisions—whether water comes

out of a valve or nuclear or electric—all of that is, in many cases, the same equipment across the sectors.

We work very hard through our Industrial Control Systems CERT and our regular computer emergency response teams and our interagency partners, our internal partners, everybody, and all of the trusted private-sector relationships to gather data and science and technology to understand two things. One is, how do we bring information in faster, and how do we analyze it, make real actionable intelligence out of it, and how do we push it out faster.

So, bringing it in comes from trust and then automated mechanisms, so people and machines. When machines see something wrong behaviorally, they tell us, and this is all designed with privacy and civil liberties baked in. The other piece is with people, and as we work closely with sectors such as financial industry as well as electric and water and all of the others, I think the finance sector, and I gave credit earlier, is very important, because they had set a standard of the level of trusted relationship going back 15 years. They have been leaders in this.

The Financial Services ISAC, Information Sharing and Analysis Center, that was mentioned earlier has taken great strides in providing ways, free of charge, for others in the private sector and Government to attach their software, whatever they may be using, to protocols or ways that we can protect other sectors and other companies with information that we know in the NCCIC. So, if we keep all the information and analyze it and look at trends, just as weather forecasters do, our job now is to get it out as quickly as possible so that our networks are resilient, and without having seen it before, a piece of the network can understand a behavior that is wrong, just like your body's immune system recognizes a cold that you may not have had before. And, working with our interagency partners and working with trust and advancements with the financial sector and others, we make other sectors stronger.

There are many sectors that are looking at this, as well as State and local and small to medium businesses, leveraging outreach from the cybersecurity framework. And, we have launched at DHS the C–Cubed VP. It is an acronym, of course, but it is the cyber—Critical Infrastructure Cybersecurity Community Voluntary Program, and that is a long name for we reach out to everybody that will listen to our best practices, that will go to our Web site and see how to judge your resilience, and that will take the information that we have, either ingest it by machine in real time, or by one of the reports that my colleagues have mentioned, or by simply calling us up saying that they need help, because the adversary moves quickly and with an agility we do not have.

Chairman JOHNSON. Thank you.

Ms. Abend, you are Chair of the FFIEC Cybersecurity Working Group. Third-party vendors may pose cybersecurity risks to financial institutions, particularly smaller institutions. What actions are the FFIEC members taking to supervise third-party service providers?

Ms. ABEND. Technology service providers serve an important role to our institutions, particularly in terms of the largest ones that

provide core banking and other critical services to a large number of financial institutions, including community institutions. And, as such, the FFIEC publishes guidance that our examiners use to oversee these institutions, including guidance specifically on the oversight of technology service providers. We use some of our most talented specialized IT examiners at the OCC to supervise these entities jointly with other banking regulatory authorities.

Chairman JOHNSON. Mr. Noonan and Mr. Demarest, last year around the holidays, we learned that one of the country's largest retailers experienced a massive data breach after Thanksgiving. What changes and improvements have been made since last year to protect consumers during the holiday season, and how do you pursue cybercriminals, and would you characterize your investigations as proactive or reactive? Mr. Noonan, let us start with you.

Mr. NOONAN. Yes, sir. Thank you. The Secret Service's approach to going after cybercriminals today is a proactive approach. As we dive into our criminal investigations, we utilize a number of different methods. We look at undercover operations. We have criminal sources. We have confidential informants. And, we are also able to look at the criminals' infrastructure and their communications. And, in doing so, we are able to see potentially where other victims are and make notifications to those companies.

So, in many of today's data breaches that are out there, our notifications are being made to those companies of their potential data breach by law enforcement, by the Secret Service. As a result of that, we work closely with those companies and we are able to draw out important evidence and tactics and trends that the criminal adversaries are using against the victim company. When we do do that, we take that information and we share that across the industry.

So, just this past year, we increased the amount of information that we have put out. Actually, we put out, I think it was eight malware initial finding reports, which are new or different strains of malware, which we put out to industry to better help them in their defenses. In addition to that, we put out seven different industry notices that went out to the whole of industry, and we use that—we take that information, and we are not just putting that out, but our partners at the NCCIC are helping us in disseminating that information out to the whole of Government, out to the rest of industry, and in doing so, we are helping to fortify and protect industry.

Just this November, on November 7, the FS–ISAC along with the Retail Cyber Intelligence Sharing Center and the Secret Service put out a document to help the retailers on how to better protect themselves with the types of crimes that we saw over the past year—point of sale terminal, information theft that were happening through infiltration of different networks. And, it is a pretty robust product that we put out and I would be willing to share it for the record after the hearing.

Chairman JOHNSON. Mr. Demarest.

Mr. DEMAREST. Yes. In exactly the same very proactive or shifting toward a proactive stance, beyond our similar hair styles, Bill and I are very closely fused together today——

[Laughter.]

Mr. DEMAREST. ——yet, you would find—and we talk about major hacks of some of the retailers, too—we are finding great benefit. And, as Bill mentioned, we each do a great job in that proactive stance where we are using undercover operations, source operations, or human operations, current tactical coverages. But, we in the FBI are able also to bring to that the national security authorities. We are able to bring in what we are collecting and working with the intelligence community that may have overlap. Some of our actors, as you know, may serve by day on their own, but may be cooperating with a certain Government Nation or a Nation-State by evening.

So, from that standpoint—and, what we provide is, on joint matters or separate, is providing those industries or at least the targeted sector retail threat indicators. If they are focused or they are for some reason not following the target of either a Nation-State or criminal actors, that information is provided in near real time to the targeted company.

Chairman JOHNSON. Senator Crapo.

Senator CRAPO. Thank you very much, Mr. Chairman.

Mr. Noonan and Mr. Demarest, one question I have is, as your law enforcement agencies in the course of an investigation obtain data that is helpful for the victims of the data breach, it is often important to share this among institutions, as you have indicated, so that other potential victims are alerted and become able to protect themselves. But, is there not an issue, also, with regard to whether in the process of sharing this data the bad actors are notified that they are being investigated or alerted to the possibility that they are about to get caught?

Mr. NOONAN. So, I think it is more important for us in law enforcement, obviously, to share information with the infrastructure we are talking about. Yes, sir, there is always a risk of the actors finding out about an investigation. But, I think it is more important for us together in law enforcement to make that notification to industry to be able to better prevent the occurrence from happening, or to stop the bleeding, if you will.

So, take for example Target. Notification was made to Target in a rather quick period of time, and I think the exposure on Target was only 2 weeks. Had that exposure gone out longer and we not made a notification to the industry, and then within 5 days of us working with Target, we took those industry, the indicators, and we pushed it out to the whole of industry.

So, I believe law enforcement's approach of going out and making notification, working with potential victim companies, is a critical part of the equation in what needs to be done to prevent further instances of data breach and others.

Mr. DEMAREST. Fully concur. Cost-benefit analysis. So, once we do that, we look at what we are doing, those indicators that may potentially compromise current collection. We feel more strongly about sharing that information and closing down those avenues of the actors. The actors, Ranking Member Crapo, you do accurately point out they do a lot of research online, so they find these products that are posted by us, DHS, I will say some of the managed cybersecurity firms' products, the research products that are also done. They will do research on those and then change their tactics.

But, the idea is to frustrate those adversaries, have them cost more in the way of time, resources, and energy to actually devise ways to circumvent what we put in place to block them.

Senator CRAPO. Thank you.

And, Mr. Peretti and Dr. Schneck, the FS–ISAC and the DTCC recently launched a new information-sharing platform called Soltra Edge, which automates information sharing to send out threat information at, as you have said, machine speed rather than human speed. And, as I understand it, Soltra uses the STIX language and the TAXII distribution method, which are protocols developed through DHS-funded projects. As the industry moves forward with automated information sharing, are Treasury and DHS able and ready to send and receive information at the same speed and in the same format as industry?

Mr. PERETTI. So, as we are moving forward—as industry is rolling out these programs—we are developing our systems to mirror that. So, while we are not at the stage yet to be able to share our information, we are formatting our information in that method and we expect to be able to do that as soon as the private sector is able to receive it.

Senator CRAPO. Do you want to add anything, Dr. Schneck?

Ms. SCHNECK. I do. This is one of the most exciting things, I think, to happen to cybersecurity and information sharing. STIX is a way of shipping information and TAXII is a way of—STIX is a language, if you will, what fields are we sending, and TAXII is a way to do it, and Soltra is kind of like a user interface. And, Treasury and the financial sector and the FS–ISAC in particular built this so that anybody can use it, which all of a sudden hooks all of the entities we need to protect with an opportunity to send and receive information. So, the wider your aperture in understanding what is happening in cyber, the better you can understand how you can form a behavior and an analysis of that that might hurt you. So, we are learning as we protect, and this is one enabler.

The other thing on which we are working with Treasury is cyber insurance as a potential building—and the exploration of a potential market to incentivize even the smallest companies to budget for cybersecurity.

Senator CRAPO. Well, thank you.

Let me just—I just have a few seconds left, but let me follow up on that. We have had a lot of discussion here in your testimony and in our questions about the flow of information and making sure that we communicate at machine speed and so forth, but what information are we talking about? What is it that you just described as such an exciting development that we are able to see being transferred and communicated at machine speed?

Ms. SCHNECK. If I may, I will use an example in botnets that was raised a moment ago by law enforcement. Botnets are the ability for the adversary to lease hundreds of thousands of machines to just throw traffic at a network that is not expecting it and literally take them offline.

What we can do with this now is understand, because we see a whole world that we are protecting and being connective through the efforts of the DHS programs and EINSTEIN and continuous diagnostics and mitigation across the Government, enhanced cyber-

security services will use that information to protect the private sector and now the automation will connect us to everybody else, if you will. We can use that intelligence to start to understand which machines are generating this traffic.

And, this is the world I come from in the private sector. This can happen in seconds. We can then provide the addresses of those machines to the ISPs, as an example, and stop the traffic from getting to the organizations that they were targeted to hurt. And, that is just one example, and my saying in that in-house is months to milliseconds.

So, before, and we still do this through trusted relationships with the Secret Service and Homeland Security Investigations and the FBI, we call the ISPs and give them the addresses now, or we email them. As this takes on, the machines will automatically know to block it.

Senator CRAPO. Thank you.

Mr. PERETTI. And, if I can just add on to that for 1 second; and what we do is ask the industry in conferences and meetings, what kind of information they need to be able to better defend their systems. So, instead of us providing information to them that may not be actionable based upon the systems they use, we go out and actually ask them, what kind of information they need. Usually, what they are asking for is IP addresses and malware hashes that they can then run through their systems to see if there are any intrusions or malicious activity going on. So, that is the type of information we are going to keep providing and that dynamic feedback loop between us and industry is really helping to refine the information and the delivery of resources that is more actionable to them to help the network defenders to protect themselves.

Senator CRAPO. Thank you.

Chairman JOHNSON. Senator Warren.

Senator WARREN. Thank you, Mr. Chairman, and since this is likely our last hearing of the year, I want to say to Chairman Johnson and to Ranking Member Crapo, thank you for the very engaged, very open way that you have run this Committee and given us an opportunity to explore so many issues. It has really been terrific. And, I also want to say on Chairman Johnson's retirement that your leadership has always been knowledgeable, thoughtful, principled, and it has been a great honor to serve with you, sir, so thank you.

I want to talk about safety and soundness. In January 2011, Federal Reserve Governor Tarullo gave a speech on regulating systemic risk in our financial institutions and how problems in one financial firm can create risks for overall financial stability. And, I was thinking about an example of two banks, JPMorgan and New York Mellon, settle all triparty repurchase agreements in the market. One-point-six trillion dollars' worth of securities are funded by triparty repos every day. If a cyber attack disrupted the ability of either of those banks to allocate collateral, it could have devastating consequences for securities firms, for money market, mutual funds, major banks, even the liquidity of the United States Treasury.

Now, Ms. Abend, this strikes me as a classic safety and soundness issue. The OCC's safety and soundness analysis requires you

to investigate how sensitive banks are to systemic market risk and how exposed each individual institution is to market risk given particular products and services that it offers. Then OCC regulators give the institution a ranking signifying whether it has adequately addressed each of the risks that are identified.

So, I want to know whether systemic risk from cybersecurity is taken into account in the ranking, and second, whether firms that are not prepared are determined, as determined by the OCC, to have failed to satisfy the safety and soundness guidelines are then treated.

Ms. ABEND. Cybersecurity has been a top priority for the OCC, particularly over the last couple of years.

Senator WARREN. No, I appreciate that. You have made that clear.

Ms. ABEND. And, in that process, we do look at the risk profile of our institutions. As part of the cybersecurity risk assessment, we actually looked at various aspects of their cybersecurity inherent risk profile, which includes technologies that they use, the products and services that they offer, and the connections that they have. And, as part of our OCC examination process, we do assign some of our most talented IT examiners to be resident on-site at our largest institutions.

Senator WARREN. No, I understand that, but the question I was asking is whether or not you take this into account in ranking the institutions and then holding them accountable as part of your safety and soundness analysis.

Ms. ABEND. We do see cybersecurity as a safety and soundness issue and we do look at the risk profile of those institutions——

Senator WARREN. And you put it into the ranking?

Ms. ABEND. I am not actually the expert who conducts that part of the ranking policy, but, what I can say is that we do have a risk-based analysis as to how we determine the risks of our institutions and the level of resources that they get on-site as resident exams.

Senator WARREN. Well, as we all know here, a future cyber attack could paralyze the financial sector with devastating consequences for our economy. No two crises are alike. We want to be out in front on this, and I would really like to know that the OCC is using this as part of their ranking.

Let me ask about another issue. When we talk about cyber attacks that affect our financial institutions, we should remember it is not just the institutions themselves who are at risk. There is a whole chain of organizations. We have talked a little bit about this. There are lots of individuals, institutions that present vulnerabilities, from the merchants to the acquirers to the payments processors and even to the employees. Forbes reported yesterday that 71 percent of employees in a new survey report having access to data they should not see. But, my point is that each and every one of these links in the chain of commerce means millions of people, potentially, are exposed to financial fraud and theft.

Last year's breach at Target, which we have talked about a little bit today, made this abundantly clear. We now know that criminals used one of Target's vendors to breach Target's system by using malware to capture credit card and debit card information. In this case, there was a single point of failure, one vendor who had com-

puters that were authorized to submit billing information to Target, that created a breach that affected the entire chain.

So, Mr. Peretti, how is Treasury monitoring the other entities along the chain, from the retail merchants, to the third-party data processors and software providers, all the way down the line before it gets to the banks, to ensure that they are making the necessary investments in cybersecurity?

Mr. PERETTI. So, what Treasury has been doing has been communicating with financial firms to be able to highlight this risk within the system, to be able to make sure that they are paying attention not only to their own internal systems, but to also all their vendors. One of the ways we have been doing that is to really publicize in this cybersecurity framework, which is a framework to be able to, first, be able to identify how you are doing cybersecurity within your own organization, but then we have been asking firms to be able to use this potentially as a way to be able to look at their outside vendors. Are there——

Senator WARREN. I am sorry. So, your monitoring of the chain is limited to telling the financial institutions to take a look at the chain? Is that what you are saying?

Mr. PERETTI. So, the financial firm's decisions are based upon a risk model in which they look at that. They are able to select their vendors based upon the products and services that they need to be able to deliver the services to their customers. And, so, we try——

Senator WARREN. I think that meant yes. Is that what you were saying?

Mr. PERETTI. What we try to do is deliver the information to them so that they can make appropriate risk management determinations as opposed to telling them which vendors they should or should not use.

Senator WARREN. Oh, I am not talking about telling them which vendors to use. What I am just trying to understand is the process by which you are monitoring—the risk comes in all the way up and down the chain——

Mr. PERETTI. Yes.

Senator WARREN. ——and we obviously know that now. So, the question I was asking about is whether you have any direct monitoring of any part of the chain, and what I think I am hearing you say is you are just telling the financial institutions to be sure to monitor.

Mr. PERETTI. So, Treasury is not a financial regulator.

Senator WARREN. I understand that.

Mr. PERETTI. We have 17 Federal and State financial regulators out there. What we do is provide information to them so that as they do their examination process, that could be incorporated into their examination procedures going forward. So, we do not go out and monitor or survey any of those folks. That is not our role within the sector. We provide that information to the regulators to be able to then use that information within their examination process.

Senator WARREN. Well, I am over my time, but if I can ask just one more question, just a little bit here. Dr. Schneck, how much risk do retailers pose, and particularly small retailers, particularly those who do not have the resources for sophisticated cyber defense?

Ms. SCHNECK. So, thank you. That is a great point, and I would ask to expand it to small to medium business in general.

Senator WARREN. Fair enough. Yes. Expand.

Ms. SCHNECK. So, we think there is a lot of risk, and that is part of why, as Mr. Peretti was mentioning, we do leverage this cybersecurity framework, because it was developed by industry and Government, by scientists from industry with NIST and with DHS, and we use those best practices to bring the discussion of cybersecurity as a risk equation, because most small to medium businesses, at least the last year with whom I have spoken, did not really look at cybersecurity as a main part of their risk equation and we are trying very hard to change that with these massive outreach programs. I have actually gone out West and talked to venture capitalists who start the smallest companies with the best technologies and ask them how they could invest tens of millions of dollars in intellectual property and not think about how to protect it.

So, we are trying to change the paradigm of how we focus on cybersecurity and make it part of how every entity in that chain looks at their risk so that the information that Mr. Peretti gets is more accurate, and we are using these outreach programs as a way to do that, and we are trying to incentivize using cybersecurity with tools such as developing a market for cyber insurance and working closely with Treasury on that. Other areas look at grants, or how do we protect reputation forward, but really making security part of the culture, making it good to share information about a breach, because your experience is very common and can protect a lot of others and that is the kind of intelligence and galvanization that we as a country and community need to do to help Government and industry tackle this and change the profit model for the criminals.

Senator WARREN. Well, good. Well, I very much appreciate that you are trying to shift the paradigm here. I understand the focus on the banks and why that is so important, but we have got to harden our security up and down the line, and I think that we cannot just make this about the banks. It has got to be the whole chain here. So, thank you very much, and thank you, Mr. Chairman.

Chairman JOHNSON. Senator Schumer.

Senator SCHUMER. Well, thank you, Mr. Chairman, and first, I would be remiss if not to acknowledge, I guess this will be the last hearing, unless we have to have one on TRIA or something—I hope not——

[Laughter.]

Senator SCHUMER. ——that you will be chairing the Banking Committee. So, I just wanted to take this opportunity to personally say how much you will be missed. You have been a great voice of reason, a steady tiller on this Committee, and we have done great things under your fair and independent chairmanship, and, of course, we have become close friends. Last night, I got to say a few words, of course, about you at our departing dinner. But, I just want to wish you and Barbara all the best.

And, to my good friend, Mike Crapo, I guess this is your last hearing, we hope, as Ranking Member. I imagine you are moving on to bigger and better things.

Senator CRAPO. We are going to see.

[Laughter.]

Senator SCHUMER. But, I want to wish you well. And, just like Tim, you have been fair and open and a wonderful person to work with, so thank you.

Now, I have a couple of—first, to the matter at hand, whether it is terrorists looking to cause us harm by wreaking havoc on cyber infrastructure, illicit goods being sold over the Internet, or sophisticated criminals hacking into systems of our financial and retail institutions, cybersecurity has never been more important to our safety and economy, and I think it is finally beginning to come into the public consciousness.

A couple of years ago, when a number of chairs here attempted to do a cybersecurity bill, there was resistance from industry. They did not want to share information about breaches. It was sort of like, I thought, almost some of these industry leaders objecting, it was sort of when Churchill asked them to turn out the lights. He asked Britain to turn out the lights during the Battle of Britain. Some people said, "No, I do not want to." I think those days are over. I think that the business community, broadly put, understands the danger here and is far more willing to cooperate than before. And, it is going to become a worse problem before it becomes better, I am afraid.

So, I have a few questions. First, to any of you, is business much more willing to cooperate, to share information about breaches and all these kinds of things than they were a year or two ago? Mr. Peretti.

Mr. PERETTI. Thank you for that question. We have seen a large change within industry to be able to be more forthcoming and open with sharing this information. They understand that the key for this is not only to share the information with law enforcement and the Government, but also with other parties.

Senator SCHUMER. Right.

Mr. PERETTI. This really came about during the DDoS attacks that started to occur back in 2012 in which financial firms saw that they were being attacked, and instead of keeping that information to themselves, they actively shared it with other financial institutions who would potentially be the next one to be attacked.

Senator SCHUMER. And, are they willing to share it with law enforcement and the people at Treasury, Homeland Security? Do you all agree they are much more willing to share information now than before? Does anyone disagree with that?

Mr. DEMAREST. We agree, yes, Senator Schumer. Yes, from the FBI, and I am sure Secret Service will echo the same, and DHS. We find them much more open today to sharing and getting involved earlier for purposes of whether they want to take something to prosecution or criminal or for national security purposes——

Senator SCHUMER. Right.

Mr. DEMAREST. ——to better defend the Nation.

Senator SCHUMER. Sure.

Mr. DEMAREST. So, we find them sharing much more readily.

Senator SCHUMER. Well, I hope this will yield next year an ability to pass some real legislation here. We need legislation. It has been stymied, in part because of the business reluctance of re-

quired sharing of information, and I just hope we will overcome that.

My next question, I think most of us were shocked at the sophistication of the breach on Sony. I know that is not a financial firm, but could happen, and my question was broader than just Sony. Fingers are pointing to North Korea. Now, I do not know what information you folks have about that, but my general question is, it is sort of surprising that a country like North Korea, which is sophisticated in a few areas but not very sophisticated in most, would have such an amazing ability to turn a large company into a knot.

How many other countries have this kind of ability? How serious is country attacks, cybersecurity not so much on Government facilities, but on—which we have to worry about seriously, I am very worried about those—but on other private entities, whether they be in financial, where they could disrupt an economy, or retail, disrupt retail, power, whatever else. Could somebody give me a little analysis there about how serious country threats are?

I think we have all been—our awareness of that has been heightened because of the supposed attack by North Korea. I do not know what level of proof you can give on that yet, or want to, but I am just asking about the country sophistication in doing this, not just U.S., Russia, China, which we hear about all the time, but next level countries.

Mr. DEMAREST. Senator Schumer, I will start. So, I will not touch on the attribution piece because we are still working very, very hard at that.

Senator SCHUMER. Right. I understand.

Mr. DEMAREST. I will say it is a model of cooperation with Sony, Sony executives, in how this is brought about. The event occurred, and within hours, you find teams from the FBI and the interagency actually on ground and working with Sony and their managed cybersecurity provider, for Mandiant.

The level of sophistication is extremely high, and we can tell based on our investigative efforts to date, organized and certainly persistent. So—and when we talk about, you know, generally speaking, about Nation-States that have this capability, you could pick the top three or four off the top of your head that have the ability when we talk about computer network attack capability, and one predominately out of the Middle East that we are also very concerned about.

Senator SCHUMER. Yes.

Mr. DEMAREST. So, generally speaking, it is of concern, because in speaking with, I will say, with Sony and, separately, their managed cybersecurity provider, the malware that was used would have slipped, it probably would have gotten past 90 percent of the net defenses that are out there today in private industry, and I would challenge to even say Government.

Senator SCHUMER. Wow. Does every—so, I know you mentioned a big Middle East country, which I would assume is Iran, and you do not have to comment. But, what I was asking, is there a next level of countries that have almost as sophisticated a level, an ability to attack as U.S., China, Russia, Iran?

Mr. DEMAREST. So——

Senator SCHUMER. Because, that was frightening. I think it was frightening to people, the specter that it might have been North Korea that did this, and said, Lord knows, anyone can do this.

Mr. DEMAREST. We have watched countries over the past 2½, 3 years actually evolve and develop greater capability and skill.

Senator SCHUMER. So, this is becoming more and more of a problem, and I imagine, and this is Dr. Schneck more than anything else, it is a geopolitical problem as well as an economic problem.

Ms. SCHNECK. I think it is an everything problem. This is—and I am going to take this from a slightly different angle——

Senator SCHUMER. Sure.

Ms. SCHNECK. ——from a non-law enforcement angle. In our world, in the National Cybersecurity and Communications Integration Center, and for DHS, the non-law enforcement piece, to protect——

Senator SCHUMER. Yes.

Ms. SCHNECK. ——everyone and our stakeholders, it—attribution is almost a distraction. For us, it is how do we understand—malware is simply a set of instructions that have the ability to allow me to execute my will on your machine, which means I turn your lights out, I kill your machine, I take your business down, whatever I want, or I sit there and watch what you do and send it out back home and learn what you are doing and resell it.

What I worry about and what our team worries about is that the increasing sophistication is available to anyone. It is really not about what country or what about—it is about, how can they acquire it. It is for sale in the underground. You can get sophisticated sets of instructions that will do this, and it is very much like what I will call the antibiotic resistant strain. The better we get, and we have to get better, but the better the adversaries get——

Senator SCHUMER. Yes.

Ms. SCHNECK. And that is why my push for speed, because the one thing they cannot do is behaviorally make the Internet stronger.

Senator SCHUMER. In some ways, it is a little like nuclear weapons. You not only worry that these countries can make them, but who they sell them to, which might not be a country.

Ms. SCHNECK. Correct.

Mr. NOONAN. Senator Schumer——

Senator SCHUMER. Does anyone—just one final question, with your indulgence, Mr. Chairman, since I am the last one here—and I will call on you, Mr. Noonan—but, does anyone doubt the need for stronger legislation on this, aside from all the good efforts that you are doing? Raise your hand if you think we need legislation of some sort. Everybody. Let the record show all hands were raised.

[Laughter.]

Senator SCHUMER. You have the last word, Mr. Noonan.

Mr. NOONAN. I am sorry. Your comments about Nation-State actors. I think with the FBI and the Secret Service and the experience that we have together on going after a number of the different sophisticated criminal groups, Dr. Schneck mentioned how some of this information and some of these tactics are available at the criminal underground level, too. Just this year, we discovered a criminal tool that was available to the criminal underground for

the simple price of $3,000 which could DDoS many, many different companies, many different countries, if you will, at a huge, huge rate. I think it was 36 gigs of DDoS power it would do for a simple $3,000 for sale on the criminal underground. So, the complex criminal actors that we are looking at that are doing a lot of these intrusions have the skills and the sophistication that far exceed a number of different Nation-States, too. So, the criminal threat is a significant threat and it is scary about how much of that technology exists today, just for sale on the criminal underground.

Mr. DEMAREST. Senator Schumer, we could make you a hacker in 30 minutes, based on the tools that are currently available in the underground——

Senator SCHUMER. I refuse the offer.

[Laughter.]

Mr. DEMAREST. Let the record reflect.

Senator SCHUMER. I want to show you the phone I use, just in case. You may want to revise your remarks here.

[Laughter.]

Senator SCHUMER. Thank you, Mr. Chairman.

Chairman JOHNSON. Thank you.

Does Senator Warren or Senator Schumer have a follow-up?

Senator SCHUMER. No, thank you.

Chairman JOHNSON. I want to thank our witnesses for testifying today and for all their work on this important issue.

This hearing is adjourned.

[Whereupon, at 11:18 a.m., the hearing was adjourned.]

[Prepared statements, responses to written questions, and additional material supplied for the record follow:]

PREPARED STATEMENT OF BRIAN PERETTI

DIRECTOR FOR THE OFFICE OF CRITICAL INFRASTRUCTURE PROTECTION AND COMPLIANCE POLICY, DEPARTMENT OF THE TREASURY

DECEMBER 10, 2014

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 cyberthreat, 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 cyberthreat 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 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 cyberthreats 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 cyberthreats 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 cyberthreat information, improving the value of information by contributing more

[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.

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's 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 sectorwide 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 consider-

ations, 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 policymakers 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.

PREPARED STATEMENT OF PHYLLIS SCHNECK

DEPUTY UNDER SECRETARY FOR CYBERSECURITY AND COMMUNICATIONS, NATIONAL PROTECTION AND PROGRAMS DIRECTORATE, DEPARTMENT OF HOMELAND SECURITY

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 cyberthreats 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 cyberthreat 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 (U.S.–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 11 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 cyberthreat 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 (E3A) gives DHS an active role in defending ".gov" network traffic. At this time, E3A provides Domain Name System and/or email protection services to 33 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 Cyberthreats

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 percent 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. U.S.–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 U.S.-based Internet Service Providers.

U.S.–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, U.S.–CERT provided this information to over 120 inter-

national partners, many of whom contributed to our mitigation efforts. U.S.–CERT, along with the FBI and other interagency partners, also deployed to affected entities on-site technical assistance, or "boots on the ground." U.S.–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 cyberthreat 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 and 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 publicly 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/U.S.–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 publicly available and can be found on U.S.–CERT's Web site, provides a nontechnical 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 cyberthreat indicators.

Also of significant note is our vision and direction moving forward to create broad situational awareness of cyberthreats 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 anal-

ysis 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 cyberthreat 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 Open SSL 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 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.

---

[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.

PREPARED STATEMENT OF VALERIE ABEND

SENIOR CRITICAL INFRASTRUCTURE OFFICER, OFFICE OF THE COMPTROLLER OF THE CURRENCY

DECEMBER 10, 2014

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 cyberthreats 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.

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.

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 pro-

---

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.

viders 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.

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 cyberthreats 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 cyberthreats 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 systemwide 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.

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 focuses 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.

Examiner Training and Communicating Expectations

All entry-level OCC examiners receive training on information technology risk management within their first 3 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 cyberthreats 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.

On-Site 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 on-site who perform ongoing supervision of the banks' IT policies, procedures, and practices. OCC examiners also perform on-site IT examinations at smaller banks every 12 to 18 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.

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 Web site.[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 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 cyberthreats 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*

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

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 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.

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 cyberthreats 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 cyberthreats, 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 sectorwide 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 cyberthreats 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 under-

[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.*

standing of cybersecurity activities through the sharing of best practices and exploring approaches to enhance cybersecurity protections.

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.

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.

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.

Other Legislative Proposals

The OCC has reviewed a number of legislative proposals that are pending in Congress to promote and facilitate information sharing concerning cyberthreats and attacks among Government agencies. The OCC generally supports such legislative initiatives. However, in the case of cyberthreat 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 cyberthreat 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 cyberthreat 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 cyberthreat 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.

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 cyberthreats 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.

PREPARED STATEMENT OF WILLIAM NOONAN

DEPUTY SPECIAL AGENT IN CHARGE, CYBER OPERATIONS BRANCH, CRIMINAL INVESTIGATIVE DIVISION, SECRET SERVICE

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 cybercrime 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 cybercriminals 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 U.S.C. §§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 cybercriminals involved in the largest known data breaches, including those of TJ Maxx, Dave and Buster's, Heartland Payment Systems, and others. Over the past 5 years Secret Service cybercrime 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 cybercriminals to justice.

The Transnational Cybercrime Threat

Advances in computer technology and greater access to personally identifiable information (PII) via the Internet have created online marketplaces for transnational cybercriminals 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 cybercrimes 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 cybercriminals who are intent on targeting our Nation's financial payment system for their illicit gain.

The growing collaboration amongst cybercriminals allows them to compartmentalize their operations, greatly increasing the sophistication of their criminal en-

---

[1] Beginning in 1970, and over the course of 3 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 cybercrime not only illustrates the long history of cybercrime, but the difficulty companies have in identifying and stopping cybercriminals 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) and 1030(d)(1).

[4] 18 U.S.C. §1030.

[5] 18 U.S.C. §1029.

[6] 18 U.S.C. §1029(e)(1).

deavors 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 cybercrime 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 cybercriminals 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 cybercrime using a variety of investigative means to infiltrate these transnational cybercriminal 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 cybercrime investigations, the Secret Service notified hundreds of U.S. entities of cybercriminal activity targeting their organizations. Additionally, as the Secret Service investigates cybercrime, 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/U.S.–CERT), and the Financial Services Information Sharing and Analysis Center (FS–ISAC) on the Back-Off malware to protect itself and its customers from cybercriminal 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 publicly 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 ac-

[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.*

cess 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 codefendants—Vladimir Kats, Azzeddine el Amine, Mark Marmilev, and Maxim Chukharev—have pleaded guilty and await sentencing. Charges against Liberty Reserve 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 cybercrime.[10]

Conclusion

The Secret Service is committed to continuing to safeguard the Nation's financial payment systems by defeating cybercriminal 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 cyberthreats. The Secret Service will continue to coordinate and collaborate with other Government agencies and the private sector as we develop new methods to combating cybercrime. Thank you for your continued commitment to protecting our Nation's financial system from cybercrime.

PREPARED STATEMENT OF JOSEPH M. DEMAREST, JR.

ASSISTANT DIRECTOR, CYBER DIVISION, FEDERAL BUREAU OF INVESTIGATION, DEPARTMENT OF JUSTICE

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 cyberthreats 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.

Cyberthreats Against the Financial Sector: Trends and Implications

Before describing the current cyberthreatscape, I'd like to give a brief overview of the FBI Cyber Division, our mission, and how we target the cyber adversaries

---

[9] See *http://www.justice.gov/usao/waw/press/2014/October/seleznev.html.*

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

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 cybercrime and cyber espionage, this is often the most difficult step, as cyberthreats 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 cybercriminals—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, JPMorgan 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 cybercriminals 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 cybercrimes 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 One prime example of the importance of collaboration and coordination is the recent take down 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 Web site known as Silk Road 2.0—one of the most extensive, sophisticated, and widely used criminal marketplaces ever created on the Internet. The Web site 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: cybercriminals 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 Web site 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 Web site.

On November 7, 2014, the U.S. Government seized the Silk Road 2.0 Web site in the largest law enforcement action to date against criminal Web sites 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 5 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 cyberthreat investigations among 19 Federal agencies. The FBI aims to strengthen and solidify the NCIJTF as the cybersecurity center for coordinating cyberthreat 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 cyberthreat 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 cyberthreat our Nation confronts. I will discuss in more detail some of our collaboration efforts with the private sector shortly.

Current FBI Efforts To Combat Cyberthreats

The FBI is engaged in a host of efforts to combat cyberthreats, 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 cyberthreat. 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 cyberthreats. 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 in-

trusions, 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 cyberthreat information shared with U.S. private-sector entities so that these entities may better defend themselves against cyberthreats. 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 cyberthreat activity, in addition to a platform for coordination and deconfliction of cyberthreat 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 cybercrime. 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 cybercrime. The NCFTA provides a unique environment for information sharing between law enforcement, private industry, and academia. The NCFTA is a nonprofit 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 cyberthreats and share information for mitigation and neutralization purposes. The NCFTA provides a one-of-a-kind opportunity for subject matter experts to address global cyberthreats such as botnets, spam, and malware. Because of its nonprofit status, the group can share information in a neutral environment, develop a strategic understanding of the threat, and work to address cyberthreats 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, cybercrime, and other major crime programs.

Charting the Cyber Future

The future cyberthreatscape 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 cyberthreats, 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.

  Cyberthreats 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 cyberthreat 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 cyberthreats we face, and sharing these insights is necessary to enhance our mutual understanding of the threat. Similarly, the operational collaboration required to identify cyberthreat 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 cyberthreats 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 area host of statutory and regulatory restrictions as well that provide nar-

rowly 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 cyberthreat 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 cyberthreats 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 cyberthreats and manage risks. The EO calls for the Government to collaborate more closely with industry by sharing information about cyberthreats 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 cyberthreats, 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 cyberthreats.

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 cybercrime, 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.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR CRAPO FROM BRIAN PERETTI

Q.1. Fast, efficient sharing of actionable cyberthreat information between law enforcement, the intelligence community, and industry is a vitally important component of protecting information systems. While we have seen significant progress over the past couple years in the timeliness and quality of information sharing, there is still room for improvement. Please describe, first, what steps are being taken at your agency or Department to improve the information-sharing process and more quickly disseminate actionable information to those who need it.

A.1. As the Sector Specific Agency for the Financial Sector, Treasury encourages private sector membership in the Financial Sector Information Sharing and Analysis Center (FS–ISAC). FS–ISAC membership has increased significantly over the past year and Treasury expects this trend to continue. As any ISAC is only as valuable as the information shared within it, Treasury also promotes and encourages individual private sector firms to actively share information through the organization. Increasing the number of private sector firms that actively share information within the FS–ISAC is a key goal for improving information sharing.

Treasury has created an information sharing and analysis unit, known as the Financial Sector Cyber Intelligence Group (CIG) to increase information sharing across the financial services industry. The CIG is a section within Treasury's Office of Critical Infrastructure Protection and Compliance Policy that focuses on cybersecurity information sharing with the financial sector. Its purpose is to increase the volume, timeliness and quality of cyberthreat information shared between the Government and the financial services sector as called for under Executive Order 13636 on Improving Critical Infrastructure Cybersecurity and Presidential Policy Directive 21 on Critical Infrastructure Security and Resilience, which designates Treasury as the Sector Specific Agency for the Financial Services Sector. The CIG was established in response to a need identified by the financial sector for the Government to have a focal point for sharing cyberthreat-related information with the sector.

The CIG identifies and analyzes all-source intelligence on cyberthreats to the financial sector; shares timely, actionable information that alerts the sector to threats and enables firms' prevention and mitigation efforts; and solicits feedback and information requirements from the sector. It produces threat and mitigation bulletins, called CIG Circulars; responds to Requests for Information from the financial sector about specific issues of concern to them; delivers classified briefings to appropriately cleared financial sector representatives; and encourages the sharing of information on specific threats to financial institutions. The CIG has a representative at the Department of Homeland Security's (DHS) National Cybersecurity and Communications Integration Center (NCCIC) and Treasury will support any new national initiative aimed at integrating cyberthreat intelligence efforts. The CIG is currently developing tools, systems, and processes to automate information sharing. Once these mechanisms are in place, the CIG will be able to share cyberthreat indicators with the financial sector in a machine readable format.

Q.2. Second, what obstacles or constraints delay the dissemination of such information?

A.2. Treasury engages frequently with individual financial institutions, industry groups, and interagency partners to understand, assess, and improve upon cybersecurity information sharing. Cybersecurity information sharing has improved in recent years, and we believe it is critically important that industry and Government continuously work together to improve the quality and timeliness of such information.

Generally, we see future work in improving information sharing processes focusing on:

- Sharing information from Government to industry, from industry to Government, and between individual companies within industry, including through working to address industry concerns over liability, regulatory use of information, and possible release of information through FOIA and other sunshine requirements; and
- Working with interagency and private sector partners to leverage DHS's STIX/TAXII protocol to automate information sharing processes. STIX/TAXII facilitates cyberthreat indicator sharing in a machine readable format.

Q.3. Financial institutions generally do a very good job sharing information with each other, but there is much less information sharing that occurs with other sectors. Because companies in different sectors can often be victims of the same attacks, robust cross-sector coordination is a key piece of the cybersecurity effort. What are some of the steps Treasury has taken or plans to take to promote better cross-sector coordination and information sharing?

A.3. Treasury recognizes that the financial sector is critically dependent on services provided by other sectors, including the energy, telecommunications, and information technology sectors. For this reason, we are working closely with the financial sector and our interagency partners to build processes for effectively sharing information across sectors. These efforts include working with the Department of Energy to promote the sharing of best practices across sectors, planning and participating in cross sector cybersecurity exercises, and sharing and receiving information from DHS's NCCIC, which serves as a focal point for cross-sector sharing among Government and private sector entities.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR MENENDEZ FROM BRIAN PERETTI

Q.1. As you know, Federal financial regulators have supervisory authority with respect to the cybersecurity efforts of regulated financial institutions. For example, the Gramm-Leach-Bliley Act requires financial institutions to safeguard consumers' personal information. But today's financial system extends far beyond regulated financial institutions—in the consumer payments area alone, for example, it extends to payment networks, merchants, and third-party payment processors, to name a few.

Aside from the Federal Trade Commission's Section 5 authority to guard consumers against unfair, deceptive, or abusive practices,

there seems to be a critical gap in the standards and attention that apply to parts of the system beyond financial institutions. In last year's data breach at Target, for example, a third-party vendor's credentials were used to infiltrate a retailer's system, resulting in the theft of consumer financial information.

How do you see the role of the Department of Homeland Security and other Federal Government actors in protecting against cybersecurity risks to the financial system more broadly, beyond just regulated institutions that are supervised by financial regulators?

A.1. Treasury communicates directly with financial institutions and other financial services sector organizations and works with other agencies and private sector groups to leverage communication channels in order to emphasize the importance of risk and vulnerability defenses within the whole system so that institutions can make appropriate risk management decisions. Paying attention to the whole risk picture requires attention to internal systems as well as vendor systems and services.

Treasury has been widely promoting the value of using the National Institute of Standards and Technology (NIST) Cybersecurity Framework to not only promote cybersecurity internally; but also for financial institutions to use this framework as a way to assess their entire supply chain, including third-party vendors. Treasury provides cyberthreat and best practices information to Federal and State financial regulators so that regulators can use this information to inform their supervisory oversight and incorporate this information into their examination procedures going forward. Treasury worked with regulators through the Financial Stability Oversight Council (FSOC) to identify cybersecurity as a key operational risk in its 2014 report, but remains concerned about regulators' limited ability to provide oversight of third party suppliers.

Q.2. What tools do DHS and other Federal Government actors have to address risks to parts of the financial system outside of regulated institutions, such as payment networks, other than through financial regulators' supervision of regulated institutions' relationships with third-party vendors?

A.2. Treasury partners with Financial and Banking Information Infrastructure Committee (FBIIC) member agencies to address risks to parts of the financial system outside of regulated institutions. Treasury continues to encourage financial services firms to utilize the NIST Cybersecurity Framework, which includes holding business partners, suppliers, and customers accountable to its risk management approach. In particular, efforts by the Securities Industry and Financial Markets Association (SIFMA) to develop auditable standards of the Framework may be beneficial in supporting broad adoption of best practices across the supply chain.

Treasury works closely with other agencies to identify and provide information that may be of use to private sector firms, and shares this information through FS–ISAC. Many of the financial sector technology service providers are members of FS–ISAC. Treasury encourages the sharing of information with other third-party service providers across sectors as appropriate.

Treasury also chairs the Committee on Foreign Investments in the United States (CFIUS). CFIUS reviews business transactions

that could result in control of a U.S. business by a foreign owned or controlled entity to determine the effect of such transactions on national security, including increased risk to parts of the financial sector outside of regulated institutions such as third party hardware or software vendors.

Q.3. Are there additional tools that would be helpful to have?

A.3. Treasury supports cyber legislation to increase information sharing that: facilitates cybersecurity information sharing between the Government and the private sector, as well as among private sector companies; incentivizes the adoption of best practices and standards for critical infrastructure protection by complementing the process set forth under the Executive Order; gives law enforcement the tools to fight crime in the digital age; updates Federal agency network security laws, and codifies DHS's cybersecurity responsibilities; creates a national data breach reporting requirement; incorporates appropriate privacy and civil liberties safeguards; reinforces the appropriate roles of civilian and intelligence agencies; and, includes targeted liability protections.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR WARNER FROM BRIAN PERETTI

Q.1. In responding to all questions below (in every category), please respond as if a "data security breach" is the "unauthorized access to, or acquisition from, a system operated or maintained by a financial institution or other entity within the financial services industry, or an agent, affiliated organization or service provider to that financial institution or other financial services entity, that compromises the protection, security, integrity, confidentiality, or privacy of any customer financial information that is itself personally identifiable or that may be associated with personally identifiable information of a customer."

How many data security breaches of systems operated or maintained by a financial institution or other entity within the financial services industry—whether such breach has been publicly reported or not—is your Government department or agency aware occurred during 2013 or 2014? In responding to this question, please note the following request for an explanation:

If your response to the forgoing question is that you do not have knowledge of any such data security breaches whatsoever, please indicate why your department or agency is not aware of any breaches given the public reports of multiple breaches within the industry in 2013 or 2014.

Additionally, if your department or agency has knowledge of such data security breaches that includes nonpublic information, and your answer will indicate that your are subject to a confidentiality obligation that prohibits your answering this question completely, please indicate which specific Federal law or other rule prohibits you from testifying to the Committee about this information on data security breaches of which your department or agency has knowledge.

A.1. Treasury does not investigate data security breaches, track data security breach investigation statistics, or have authority to

compel financial institutions to report information associated with data breaches. For this reason, we do not maintain a database of data security breach incidents. Instead, our efforts are focused on engaging with cybersecurity and law enforcement partners, independent regulators, and the sector itself to share information related to the technical details of a broad range of cyber incidents to reduce the risk of these incidents occurring elsewhere.

Q.2. Of those data security breaches at financial institutions and/or other entities within the financial services industry which your department or agency is aware occurred in 2013 or 2014, please indicate:

Approximately how many financial services customers—whether individuals or organizations—you estimate were affected by each of those data security breaches.

How many data security breaches resulted in individual customer notices mailed, emailed, or otherwise personally delivered to affected customers by the financial institution or other financial services entity?

How many data security breaches resulted in some form of public notice by the financial institution or other financial services entity? (In response to this subquestion, please indicate for each data security breach if notice was made to major media outlets in the geographic region served by the institution or entity, and/or if the notice resulted from media reports following a public regulatory filing.)

How many data security breaches have never resulted in any form of individual customer notices mailed, emailed, or otherwise personally delivered to affected customers by the financial institution or other financial services entity?

A.2. Treasury does not investigate data security breaches, track data security breach investigation statistics, or have authority to compel financial institutions to report information associated with data breaches. For this reason, we do not maintain a database of data security breach incidents. Instead, our efforts are focused on engaging with cybersecurity and law enforcement partners, independent regulators, and the sector itself to share information related to the technical details of a broad range of cyber incidents to reduce the risk of these incidents occurring elsewhere.

Q.3. Of those data security breaches which you are aware occurred in 2014, and for which no individual customer notice was given by the financial institution or other financial services entity, has your department or agency investigated the circumstances of the breach and considered taking any action to require or encourage individual customer notice of the same by such institution or entity?

A.3. Treasury does not investigate data security breaches, track data security breach investigation statistics, or have authority to compel financial institutions to report information associated with data breaches. For this reason, we do not maintain a database of data security breach incidents. Instead, our efforts are focused on engaging with cybersecurity and law enforcement partners, independent regulators, and the sector itself to share information related to the technical details of a broad range of cyber incidents to reduce the risk of these incidents occurring elsewhere.

Q.4. Has your department or agency ever engaged in any enforcement action against a financial institution or other entity within the financial services industry for failure to individually notify affected customers of a data security breach suffered by that entity?

A.4. No. Treasury does not have authority to take enforcement action in this regard.

Q.5. Has your department or agency ever assessed any civil penalty or fine against a financial institution or other entity within the financial services industry for failure to individually notify affected customers of a data security breach suffered by that entity?

A.5. No. Treasury does not have authority to take enforcement action in this regard.

Q.6. If the answer to either question 4 or 5 is yes, please specify the specific date of the department or agency action, the type of action taken, the entity which was subject to the action, and the amount of any penalty or fine that was assessed. If the answer to either question is no, please indicate the reason why your department or agency has not.

A.6. Treasury does not have authority to take enforcement action in this regard.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR CRAPO FROM PHYLLIS SCHNECK

Q.1. Fast, efficient sharing of actionable cyberthreat information between law enforcement, the intelligence community, and industry is a vitally important component of protecting information systems. While we have seen significant progress over the past couple years in the timeliness and quality of information sharing, there is still room for improvement. Please describe, first, what steps are being taken at your agency or Department to improve the information-sharing process and more quickly disseminate actionable information to those who need it.

A.1. The Department of Homeland Security (DHS) has made significant progress during the last 18 months to improve information sharing. Congress recognized this good work last year when it unanimously passed a law recognizing the National Cybersecurity and Communications Integration Center's (NCCIC) central role to coordinate and serve as an interface for cybersecurity information across the Government and private sector. In January 2015, the President announced a legislative proposal that builds on this significant action taken by Congress. The Administration's 2015 legislative proposal encourages the private sector to share appropriate cyberthreat indicators with the NCCIC by providing targeted liability protection for companies that share threat indicator information. The proposal aims to increase the speed, quality, and frequency of existing information sharing between the Government and private-sector entities, to better protect against the shared threat of cyber attacks.

We are actively working to maximize to the fullest extent possible the near-real-time dissemination of all relevant and actionable cyberthreat indicators among the private sector and Federal Departments for the purpose of network defense, while incor-

porating all appropriate privacy protections. We continue to make progress as Congress addresses key information-sharing constraints such as industries' concerns over liability protections.

DHS has a number of programs and initiatives dedicated to forging and maintaining the public and private-sector trust-relationships that enable meaningful information sharing including: partnerships with critical infrastructure owners and operators to ensure cohesive cybersecurity efforts; the Critical Infrastructure Cyber Community Voluntary Program (C3 Voluntary Program) offering cybersecurity resources to private and public-sector entities through DHS who voluntarily commit to the cybersecurity framework created as a result of Executive Order 13636; the sharing of sensitive indicators that support intrusion prevention measures through Enhanced Cybersecurity Services (ECS); as well as ongoing collaboration with the private sector through the NCCIC, DHS's 24/7 center for cybersecurity incident response, prevention and mitigation.

DHS is increasing the speed of indicator information sharing through the implementation of the Structured Threat Information eXpression (STIX) protocol and the Trusted Automated Exchange of Indicator Information (TAXII) a transport protocol. These protocols provide a structured framework for information sharing and dissemination that enables the analysis of full-spectrum cyberthreat information; a common language in which to share cyberthreat information across organizations and products; and a common set of services and messages that can be implemented to share information. TAXII and STIX are intended for use by Government and industry Computer Security Incident Response Teams to enable timely and secure threat information sharing. All threat sharing models, including hub-and-spoke, peer-to-peer, and source-subscriber, can take advantage of the standardization offered by TAXII and STIX. These protocols are in operational use today among several Information Sharing and Analysis Centers, within the Cyber Information Sharing and Collaboration Program (CISCP), and are being implemented across the NCCIC enterprise.

CISCP, which began in January 2012, established a systematic approach to cyberthreat information sharing and collaboration between critical infrastructure owners and operators across all critical infrastructure sectors. Partners who have signed the CISCP Cooperative Research and Development Agreement share unclassified, actionable, timely threat indicator data to enhance the protection of themselves and in many cases their customers and constituents. Important analytic collaboration meetings are held monthly at the unclassified level and quarterly at the classified secret level among CISCP partners.

With respect to cyberthreat intelligence, DHS's Office of Intelligence & Analysis (I&A) conducts cyberthreat intelligence outreach and engagements with key critical infrastructure sectors at the broadest level possible, with an emphasis on providing unclassified cyberthreat intelligence to increase owner and operator awareness and encourage them to make use of associated indicator data in their protection systems. I&A provides tailored analysis of cyberthreat activity to various private sector, State and local, and Federal partners to develop a common baseline understanding of

cyberthreats and enable decision makers to protect, prevent, and mitigate against cyberthreats.

DHS developed the C3 Voluntary Program to assist critical infrastructure in their adoption of the National Institute of Standards and Technology's Cybersecurity Framework, and to extend a range of cybersecurity resources to critical infrastructure including, among other things, information-sharing opportunities.

The ECS program is a voluntary information-sharing program that assists critical infrastructure owners and operators to improve protection of their systems from unauthorized access, exploitation, or data exfiltration. ECS consists of the operational processes and security oversight required to share sensitive and classified cyberthreat information with qualified Commercial Service Providers (CSP) that will enable them to better protect their customers who are critical infrastructure entities. The ECS program develops threat "indicators" with this information and provides CSPs with those indicators of active, malicious cybersecurity activity. CSPs may use these threat indicators to provide approved cybersecurity services to critical infrastructure entities.

Q.2. Second, what obstacles or constraints delay the dissemination of such information?

A.2. We believe that carefully updating laws to facilitate cybersecurity information sharing is one of several legislative changes essential to protect individuals' privacy and improve the Nation's cybersecurity. Such legislation should, among other things, provide for appropriate sharing with targeted liability protections.

The Administration's updated legislative proposal promotes better cybersecurity information sharing between the private sector and Government, and it enhances collaboration and information sharing amongst the private sector. Specifically, the proposal encourages the private sector to share appropriate cyberthreat information with the DHS NCCIC, and with private-sector developed and operated Information Sharing and Analysis Organizations (ISAOs), by providing targeted liability protection for companies that share information with these entities. Once information is received, the DHS NCCIC will then share it in as close to real-time as practicable with relevant Federal agencies and relevant ISAOs. It does not provide protection for individual private-sector entities sharing directly with one another.

The proposed legislation also encourages the formation of these ISAOs. The Administration's proposal would also safeguard Americans' personal privacy by requiring private entities to comply with certain privacy restrictions such as removing unnecessary personal information and taking measures to protect any personal information that must be shared in order to qualify for liability protection. The proposal further requires the Department of Homeland Security and the Attorney General, in consultation with the Privacy and Civil Liberties Oversight Board, the Director of the Office of Management and Budget, and others, to develop receipt, retention, use, and disclosure guidelines for the Federal Government. Finally, the Administration intends this proposal to complement and not to limit existing effective relationships between Government and the private sector. These existing relationships between law enforce-

ment and other Federal agencies are critical to the cybersecurity mission.

Q.3. On November 14, 2014, the DHS Office of Inspector General released a report that made some criticisms of DHS's cybersecurity efforts. The report found insufficient staffing at National Cybersecurity and Communications Integration Center (NCCIC) and the Office of Intelligence and Analysis, and insufficient technical training of staffers. The report also stated that DHS faces continuing challenges in sharing cyber incident information with Federal operations centers and coordinating effective responses. There have also been other reports of low staff morale and high staff turnover at key positions. Please discuss these problems in more detail and explain what the Department is doing to address them. Specifically, please explain what DHS is doing to ensure that information is being shared as quickly and efficiently as possible.

A.3. In regards to the specific recommendations mentioned in the November 2014 Office of Inspector General (OIG) report, NPPD has done the following: *OIG-14-02, DHS Efforts To Coordinate the Activities of Federal Cyber Operations Centers.*

- *Recommendation #2:* Collaborate with the Department of Defense (DOD) and National Institute of Standards and Technology (NIST) to develop a standard set of incident categories to ensure seamless information sharing between all Federal cyber operations centers. The United States Computer Emergency Readiness Team (U.S.–CERT) published the Revised Guidelines on October 1, 2014, and OIG closed this recommendation in October 7, 2014.
- *Recommendation #4:* Collaborate with I&A management to increase the number of its analysts available for continuous coverage at the NCCIC to provide more intelligence and analysis to all sectors. I&A did not receive the budget to increase the number of analysts for continuous coverage. It is uncertain when I&A will be able to increase the number of its analysts available for continuous coverage at the NCCIC. Due to uncertainty surrounding future budget years, the OIG closed this recommendation on January 7, 2015.

DHS's Office of Intelligence and Analysis is a key partner in NCCIC activities, providing tailored all-source cyberthreat intelligence and warning to NCCIC components and public and private critical infrastructure stakeholders to prioritize risk analysis and mitigation.

Within the NCCIC, the U.S. Computer Emergency Readiness Team (U.S.–CERT) provides response support and defense against cyber attacks for Federal civilian agency networks as well as private-sector partners upon request. U.S.–CERT collaborates and shares information with State and local government, industry, and international partners, consistent with rigorous privacy, confidentiality, and civil liberties guidelines, to address cyberthreats and develop effective security responses. In fiscal year (FY) 2014, U.S.–CERT processed approximately 55,523 cyber incidents involving Federal agencies, critical infrastructure, and our industry partners. In addition, U.S.–CERT issued 7,655 actionable cyber alerts in

FY2014 that were used by private sector and Government agencies to protect their systems.

The Department's Industrial Control Systems Cyber Emergency Response Team (ICS–CERT) responded to 240 incidents in FY2014 while completing 75 on-site assistance visits for response and recovery for significant private-sector cyber incidents. DHS also empowers owners and operators through a cyber self-evaluation tool, which was downloaded by more than 4,800 users in FY2014. ICS–CERT also trained more than 640 professionals in the Industrial Control Systems security industry.

Successful response to dynamic cyberthreats requires leveraging sector specific agencies (SSAs), homeland security, law enforcement, and military authorities and capabilities, which respectively promote sector resilience, domestic preparedness, criminal deterrence and investigation, and national defense. DHS, DOD, and the Department of Justice (DOJ), each play a key role in responding to cybersecurity incidents that pose a risk to the United States. In addition to the aforementioned responsibilities of our Department, SSAs like the Treasury Department develop and implement sector specific plans unique to respective sectors through a coordinated effort involving public and private-sector partners. DOJ is the lead Federal department responsible for the investigation, attribution, disruption, and prosecution of cybercrimes, while DOD is responsible for securing national security and military systems as well as gathering foreign cyberthreat information and defending the Nation from attacks in cyberspace. DHS supports our partners in many ways. For example, the United States Coast Guard as an Armed Force has partnered with U.S. Cyber Command and U.S. Strategic Command to conduct military cyberspace operations.

While each agency operates within the parameters of its authorities, the U.S. Government's response to cyber incidents of consequence is coordinated among these three agencies. Synchronization among SSAs, DHS, DOJ, and DOD not only ensures that whole of Government capabilities are brought to bear against cyberthreats, but also improves Government's ability to share timely and actionable cybersecurity information among a variety of partners, including the private sector.

Q.4. Please explain what DHS is doing to better train and retain key employees?

A.4. The recently passed Border Patrol Agent Pay Act of 2014 and Cybersecurity Workforce Assessment Act both contain provisions that require DHS to assess its current cybersecurity needs and workforce and to plan for the future. As part of the requirements of the two bills, DHS must inventory cybersecurity positions, attach workforce codes corresponding to the National Initiative for Cybersecurity Education (NICE) Framework, identify critical needs and develop a plan for achieving those. Using those workforce codes, DHS will be better-positioned to identify associated training needs and opportunities specific to employees' roles in the Department. The recent legislation also allows for hiring authorities for cybersecurity positions, and provides authority to set pay scale and incentives for certain cybersecurity positions.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR MENENDEZ FROM PHYLLIS SCHNECK

Q.1. As you know, Federal financial regulators have supervisory authority with respect to the cybersecurity efforts of regulated financial institutions. For example, the Gramm-Leach-Bliley Act requires financial institutions to safeguard consumers' personal information. But today's financial system extends far beyond regulated financial institutions—in the consumer payments area alone, for example, it extends to payment networks, merchants, and third-party payment processors, to name a few.

Aside from the Federal Trade Commission's Section 5 authority to guard consumers against unfair, deceptive, or abusive practices, there seems to be a critical gap in the standards and attention that apply to parts of the system beyond financial institutions. In last year's data breach at Target, for example, a third-party vendor's credentials were used to infiltrate a retailer's system, resulting in the theft of consumer financial information.

How do you see the role of the Department of Homeland Security and other Federal Government actors in protecting against cybersecurity risks to the financial system more broadly, beyond just regulated institutions that are supervised by financial regulators?

A.1. Addressing cybersecurity risks involves a range of policy tools and approaches, including voluntary assistance in implementing effective cybersecurity measures, and threat reduction through criminal investigations or other means. DHS plays a leading role through the National Protection and Programs Directorate which provides support through cybersecurity information-sharing programs and direct technical assistance when appropriate and requested, and the Secret Service and Immigration and Customs Enforcement conduct criminal investigations.

DHS strengthens the cybersecurity of the financial sector through voluntary measures by working in partnership with the Financial Services Information Sharing and Analysis Center, the Treasury Department, and private industry. USSS is a leader in investigating cybercrime across a variety of industries and partners closely with DOJ to apprehend and prosecute these criminals. The Federal Trade Commission, Consumer Financial Protection Bureau, Securities and Exchange Commission, and other entities with relevant regulatory authorities, enforce their regulations as they relate to cybersecurity consistent with their authorities. While coordinated action is important, this needs to be balanced with the need to foster private-sector cooperation by maintaining some distinction and separation between regulatory, criminal law enforcement, and cybersecurity protection assistance.

Q.2. What tools do DHS and other Federal Government actors have to address risks to parts of the financial system outside of regulated institutions, such as payment networks, other than through financial regulators' supervision of regulated institutions' relationships with third-party vendors?

A.2. DHS performs a leading role in both aiding industry in implementing effective cybersecurity protections and reducing the cybercrime risks they face through effective criminal investigations.

DHS works with a range of public and private partners to execute its role in addressing cybersecurity risks.

As it relates specifically to payment systems, most of the relevant cybersecurity requirements are developed by the Payment Card Industry (PCI) Security Council and enforced through contracts between financial institutions, payment processors, and retailers. The United States Secret Service works with the PCI Security Council and private industry to inform the development of these and other security standards based upon current trends in cybercrime activity. This private-sector driven cybersecurity standards system has proven to be highly adaptive to changes in technology, as well as to changes in cybercriminal techniques, and provide effective incentives for changes to security standards. On January 1, 2015, version 3.0 of the PCI Data Security Standards replaced version 2.0 to become the new standard.

Q.3. Are there additional tools that would be helpful to have?

A.3. DHS is focused on performing its role in providing voluntary cybersecurity assistance to private companies and conducting criminal investigations to identify and apprehend those responsible for computer intrusions. Further strengthening these capabilities will assist DHS in accomplishing its mission to safeguard and secure cyberspace.

As necessary, DHS will continue to work with its partners in the interagency and in Congress to develop and advance legislative proposals that foster rapid cybersecurity information sharing and that strengthen Federal law enforcement's authorities to investigate cybercrime, including the President's recent cybercrime authorities proposal which includes increased authorities to prosecute cybercrimes.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR WARNER FROM PHYLLIS SCHNECK

Q.1. In responding to all questions below (in every category), please respond as if a "data security breach" is the "unauthorized access to, or acquisition from, a system operated or maintained by a financial institution or other entity within the financial services industry, or an agent, affiliated organization or service provider to that financial institution or other financial services entity, that compromises the protection, security, integrity, confidentiality, or privacy of any customer financial information that is itself personally identifiable or that may be associated with personally identifiable information of a customer."

How many data security breaches of systems operated or maintained by a financial institution or other entity within the financial services industry—whether such breach has been publicly reported or not—is your Government department or agency aware occurred during 2013 or 2014? In responding to this question, please note the following request for an explanation:

If your response to the forgoing question is that you do not have knowledge of any such data security breaches whatsoever, please indicate why your department or agency is not aware of any breaches given the public reports of multiple breaches within the industry in 2013 or 2014.

Additionally, if your department or agency has knowledge of such data security breaches that includes nonpublic information, and your answer will indicate that your are subject to a confidentiality obligation that prohibits your answering this question completely, please indicate which specific Federal law or other rule prohibits you from testifying to the Committee about this information on data security breaches of which your department or agency has knowledge.

A.1. There were 14 incidents reported from the financial sector that are associated with data breaches in 2013–2014. Bear in mind that private entities are not required to report breaches to the NCCIC, though we make effort to encourage them to share information so that we can better inform our private and public partners. The NCCIC is the Federal coordination point for information sharing and analysis. We maintain trust-based relationships across the public and private sector to encourage entities to share information and to request assistance as needed, without fear of reprisal.

Through the Protected Critical Infrastructure Information (PCII) program, information voluntarily given by the private sector for homeland security purposes is exempt from disclosure except under specific procedures for Congressional disclosure. The PCII Program is an information-protection program that enhances voluntary information sharing between infrastructure owners and operators and the Government. PCII protections mean that homeland security partners can be confident that sharing their information with the Government will not expose sensitive or proprietary data. Designating information as PCII provides a level of protection that facilitates DHS's ability to work directly with the infrastructure owners and operators to identify vulnerabilities, mitigation strategies, and protective measures.

While protecting their information, DHS has the responsibility to provide assistance to those private-sector entities who request it and who voluntarily share information regarding an incident. Upon receipt of a Request for Technical Assistance (RTA), DHS provides on-site and/or remote operational support to Government and private-sector partners, focusing most specifically on supporting remediation, posture adjustment, and recovery efforts. DHS coordinates RTAs with DOJ and DOD, and participates in interagency response teams.

A DHS response team typically includes malware analysts, control systems experts, netflow analysts, and DHS law enforcement representation, when appropriate. Information learned during the operational support process is used not only to support the victim, but is also integrated (without attribution) into DHS's information-sharing products for the broader community.

Q.2. In responding to all questions below (in every category), please respond as if a "data security breach" is the "unauthorized access to, or acquisition from, a system operated or maintained by a financial institution or other entity within the financial services industry, or an agent, affiliated organization or service provider to that financial institution or other financial services entity, that compromises the protection, security, integrity, confidentiality, or privacy of any customer financial information that is itself personally

identifiable or that may be associated with personally identifiable information of a customer."

Of those data security breaches at financial institutions and/or other entities within the financial services industry which your department or agency is aware occurred in 2013 or 2014, please indicate:

Approximately how many financial services customers—whether individuals or organizations—you estimate were affected by each of those data security breaches.

How many data security breaches resulted in individual customer notices mailed, emailed, or otherwise personally delivered to affected customers by the financial institution or other financial services entity?

How many data security breaches resulted in some form of public notice by the financial institution or other financial services entity? (In response to this subquestion, please indicate for each data security breach if notice was made to major media outlets in the geographic region served by the institution or entity, and/or if the notice resulted from media reports following a public regulatory filing.)

How many data security breaches have never resulted in any form of individual customer notices mailed, emailed, or otherwise personally delivered to affected customers by the financial institution or other financial services entity?

A.2. Private-sector entities are not required to report breaches to DHS; our interactions with them are voluntary. DHS notifies victims of cyber incidents primarily through the NCCIC (U.S.–CERT, ICS–CERT, and National Coordinating Center) and the USSS, and this notification is executed in coordination with Federal cyber centers and with the FBI. Importantly, DHS is responsible for notifying not only the known targets of an attack, but also other organizations and sectors that could be targeted in the future. These cross sector alerts and warnings are a key piece of DHS's efforts to develop shared situational awareness and feed various protection efforts. *DHS, however, does not have the authority to instruct or require financial institutions to provide us with information regarding their affected customers and their policies regarding customer notification of a breach.*

The NCCIC is proud of the partnerships it has established with the financial sector. In fact, there are several financial partners with presence in NCCIC operations center. The below list of NCCIC financial sector partners constitute entities that maintain physical and/or virtual representation on the NCCIC operations floor:

- Department of the Treasury
- Financial Sector-Information Sharing and Analysis Center (FS–ISAC)
- Federal Deposit Insurance Corporation
- United States Secret Service (USSS)
- Federal Bureau of Investigation (FBI)
- private-sector entities

Individuals from the private sector, through FS–ISAC representatives, cleared at the Top Secret/Sensitive Compartmented Information (TS/SCI) level, can and do access daily briefs and other NCCIC meetings to share information on threats, vulnerabilities, incidents and potential or known impacts to the sector. The FS–ISAC, formed to share specific threat and vulnerability assessments and effective incident response practices, reaches more than 11,000 financial institutions throughout the country. FS–ISAC members include: banking firms and credit unions, securities firms, insurance companies, credit card companies, mortgage banking companies, financial services sector utilities, financial services service bureaus, sector-appropriate industry associations.

Building the trust necessary to have these relationships with private sector and Federal partners is one of our most important goals. However, we have run into numerous examples whereby partners have chosen not to share information with us despite the possible protection that information could offer other partners. We have found that companies' are often concerned that if knowledge of a cyber incident becomes public it will cause serious damage to their reputation.

To alleviate these fears, the Department offers protection from disclosure of sensitive information under the Protected Critical Infrastructure Information (PCII) Act. The PCII program helps to ensure the confidentiality of private-sector company information, allowing us to strengthen our trust and thereby our information sharing and response activities.

Q.3. In responding to all questions below (in every category), please respond as if a "data security breach" is the "unauthorized access to, or acquisition from, a system operated or maintained by a financial institution or other entity within the financial services industry, or an agent, affiliated organization or service provider to that financial institution or other financial services entity, that compromises the protection, security, integrity, confidentiality, or privacy of any customer financial information that is itself personally identifiable or that may be associated with personally identifiable information of a customer."

Of those data security breaches which you are aware occurred in 2014, and for which no individual customer notice was given by the financial institution or other financial services entity, has your department or agency investigated the circumstances of the breach and considered taking any action to require or encourage individual customer notice of the same by such institution or entity?

A.3. The responsibility to regulate actions by financial sector entities before, during or after a cyber breach is not within the purview of DHS responsibilities—as DHS is not a regulator of the financial sector. However, we are a coordination point for information sharing during and after a cyber breach; and the NCCIC works to mitigate damages and provide technical assistance upon request. For instance, following attacks on the financial services sector in 2013 and 2014, U.S.–CERT went on-site with major financial institutions and other critical infrastructure to provide technical assistance. U.S.–CERT's technical data and assistance included identifying 600,000 Distributed Denial of Service-related IP addresses

and contextual information about the source of the attacks, the identity of the attacker, or associated details. We have had long-term, consistent threat engagements with the Department of Treasury, the FBI, and private-sector partners in the Financial Services Sector.

DHS notifies victims of cyber incidents primarily through the NCCIC (U.S.–CERT, ICS–CERT, and NCC) and the USSS. This notification is executed in coordination with Federal cyber centers and with the FBI. Importantly, DHS is responsible for notifying not only the known targets of an attack, but also other organizations and sectors that could be targeted in the future. These cross-sector alerts and warnings are a key piece of DHS's efforts to develop shared situational awareness and feed various protection efforts. DHS, however, does not have the authority to instruct or require financial institutions to provide us with information regarding their affected customers and their policies regarding customer notification of a breach.

Q.4. In responding to all questions below (in every category), please respond as if a "data security breach" is the "unauthorized access to, or acquisition from, a system operated or maintained by a financial institution or other entity within the financial services industry, or an agent, affiliated organization or service provider to that financial institution or other financial services entity, that compromises the protection, security, integrity, confidentiality, or privacy of any customer financial information that is itself personally identifiable or that may be associated with personally identifiable information of a customer."

Has your department or agency ever engaged in any enforcement action against a financial institution or other entity within the financial services industry for failure to individually notify affected customers of a data security breach suffered by that entity?

Has your department or agency ever assessed any civil penalty or fine against a financial institution or other entity within the financial services industry for failure to individually notify affected customers of a data security breach suffered by that entity?

If the answer to either question is yes, please specify the specific date of the department or agency action, the type of action taken, the entity which was subject to the action, and the amount of any penalty or fine that was assessed. If the answer to either question is no, please indicate the reason why your department or agency has not.

A.4. The responsibility to regulate actions by financial sector entities before, during or after a cyber breach is not within the purview of DHS responsibilities—as DHS is not a regulator of the financial sector. However, we are a coordination point for information sharing during and after a cyber breach; and the NCCIC works to mitigate damages and provide technical assistance upon request. For instance, following attacks on the financial services sector in 2013 and 2014, U.S.–CERT went on-site with major financial institutions and other critical infrastructure to provide technical assistance. U.S.–CERT's technical data and assistance included identifying 600,000 Distributed Denial of Service-related IP addresses and contextual information about the source of the attacks, the

identity of the attacker, or associated details. We have had long-term, consistent threat engagements with the Department of Treasury, the FBI, and private-sector partners in the Financial Services Sector.

DHS notifies victims of cyber incidents primarily through the NCCIC (U.S.–CERT, ICS–CERT, and NCC) and the USSS. This notification is executed in coordination with Federal cyber centers and with the FBI. Importantly, DHS is responsible for notifying not only the known targets of an attack, but also other organizations and sectors that could be targeted in the future. These cross-sector alerts and warnings are a key piece of DHS's efforts to develop shared situational awareness and feed various protection efforts. DHS, however, does not have the authority to instruct or require financial institutions to provide us with information regarding their affected customers and their policies regarding customer notification of a breach.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR CRAPO FROM VALERIE ABEND

Q.1. Fast, efficient sharing of actionable cyberthreat information between law enforcement, the intelligence community, and industry is a vitally important component of protecting information systems. While we have seen significant progress over the past couple years in the timeliness and quality of information sharing, there is still room for improvement. Please describe, first, what steps are being taken at your agency or Department to improve the information-sharing process and more quickly disseminate actionable information to those who need it.

First, What steps are being taken at your agency or Department to improve the information-sharing process and more quickly disseminate actionable information to those who need it?

Second, what obstacles or constraints delay the dissemination of such information?

A.1. Cyberthreats evolve rapidly, and banks and their critical service providers need to have in place appropriate methods for monitoring, sharing, and responding to threat and vulnerability information to safeguard customer and other sensitive information and technology systems. For this reason, the OCC, along with the other Federal Financial Institutions Examination Council (FFIEC) members, issued the *Cybersecurity Threat and Vulnerability Monitoring and Sharing Statement* on November 3, 2014. The statement reiterated that banks are expected to monitor and maintain sufficient awareness of cybersecurity threat and vulnerability information so they can evaluate risk and respond accordingly. This statement also recommended that banks participate in the Financial Services—Information Sharing and Analysis Center (FS–ISAC) and leverage other resources to obtain threat information on a timely basis.

We recognize that obtaining timely, relevant, and actionable information is critically important for financial institutions and the ability of the financial sector to prepare for, respond to, and mitigate evolving threats. Constraints on the timely dissemination of threat information can vary depending upon the speed at which in-

stitutions share, process, and act upon the information. To address these obstacles, the private sector is working to develop more automated processes for distribution of threat information. Further, a statutory safe harbor from liability for the sharing of information about cyberthreats among institutions and the Federal Government would encourage information sharing.

Q.2. During some recent data breaches, hackers have been able to break into companies' systems by exploiting vulnerabilities of vendors. Please discuss:

First, what the financial regulators are doing to address cybersecurity capabilities at third party service providers for financial institutions, using their authorities under the Bank Service Company Act of 1962;

Second, what regulators expect from financial institutions in their management of third party relationships; and

Finally, whether, based on the FFIEC assessment conducted this past summer, small institutions are capable of meeting these expectations.

A.2. The OCC supervises third-party service providers under our Bank Service Company Act (BSCA) authority. The OCC, together with the other Federal bank regulatory agencies, developed a program to supervise, on an interagency basis, those third-party technology service providers (TSPs) that are most critical to the banking industry. Supervision of the largest TSPs is coordinated through the Information Technology (IT) Subcommittee of the FFIEC Task Force on Supervision. Other TSPs that are smaller in size or complexity are supervised on an interagency basis through the regional offices of the agencies.

As provided in the BSCA, the services performed by a TSP for a depository institution are subject to regulation and examination to the same extent as if such services were performed by the depository institution itself on its own premises. Accordingly, the Federal bank regulatory agencies examine the adequacy of TSPs' cybersecurity programs, including their IT risk management, controls, and information security. Examinations are conducted using the same FFIEC information technology work programs that are applicable to depository institutions. A report of examination is then issued to the TSP, along with an URSIT[1] rating. The examination report is made available to depository institutions that use the examined services at the time of the examination. The supervision program standards used by the Federal bank regulatory agencies can be found in the FFIEC IT Examination Handbook *Supervision of Technology Service Providers* booklet. Each Federal bank regulatory agency has issued guidance for financial institutions regarding the oversight of third-party service providers. For the OCC, this guidance is contained in OCC Bulletin 2013–29 *Third-Party Relationships: Risk Management Guidance.* This guidance outlines risk management expectations for financial institutions' selection, oversight and ongoing monitoring of their third-party service providers. This guidance has been incorporated into the OCC' s supervisory strategies used to examine national banks and Federal savings associations. In addition to agency specific guidance, the FFIEC

[1] Uniform Rating System for Information Technology.

members have jointly issued guidance on exam procedures to examiners that can be found in the FFIEC IT Examination Handbook *Outsourcing Technology Services* booklet.

Based on the results from this past summer's pilot of new exam procedures, we found that OCC-supervised community institutions involved in the assessment generally have processes to manage third-party relationships. We will continue to communicate the risks posed by third-party relationships and our expectations that financial institutions manage these risks. Where examiners determine that an institution does not meet our expectations, they will require the institution to ensure any gaps are addressed.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR MENENDEZ FROM VALERIE ABEND

Q.1. As you know, Federal financial regulators have supervisory authority with respect to the cybersecurity efforts of regulated financial institutions. For example, the Gramm-Leach-Bliley Act requires financial institutions to safeguard consumers' personal information. But today's financial system extends far beyond regulated financial institutions—in the consumer payments area alone, for example, it extends to payment networks, merchants, and third-party payment processors, to name a few.

Aside from the Federal Trade Commission's Section 5 authority to guard consumers against unfair, deceptive, or abusive practices, there seems to be a critical gap in the standards and attention that apply to parts of the system beyond financial institutions. In last year's data breach at Target, for example, a third-party vendor's credentials were used to infiltrate a retailer's system, resulting in the theft of consumer financial information.

How do you see the role of the FFIEC and its members in protecting against cybersecurity risks to the financial system more broadly, beyond just regulated institutions?

A.1. Weak cybersecurity has become an increasing risk to the safety and soundness of financial institutions and the whole financial system. In recognition of this risk, the FFIEC created a Cybersecurity and Critical Infrastructure Working Group (CCIWG). The CCIWG serves as a dedicated forum to address policy relating to cybersecurity and critical infrastructure security and resilience of financial institutions and their technology service providers. In support of this role and its objectives, the CCIWG communicates with the intelligence community, law enforcement, and homeland security agencies regarding cybersecurity and critical infrastructure issues on an ongoing basis. The CCIWG also serves as a forum for members to communicate, collaborate, and build on existing efforts to support and strengthen the activities of other interagency and private sector groups that promote financial services sector cybersecurity and critical infrastructure security and resilience.

Q.2. What tools do Federal financial regulators have to address risks to parts of the system outside of regulated institutions, such as payment networks, other than through supervision of regulated institutions' relationships with third-party vendors?

A.2. The OCC regulates national banks, Federal savings associations, and their third-party service providers. The OCC's legal authority to supervise third party service providers is set forth in the BSCA. Under this authority, the OCC in conjunction with other FFIEC member agencies, supervises TSPs, including several payment system processors. Supervision of the largest and most systemically important TSPs is centrally coordinated through the IT Subcommittee of the FFIEC Task Force on Supervision.

Other third-party TSPs, smaller in size or complexity, are supervised on an interagency basis through the regional offices of the agencies.

As provided in the BSCA, the services performed by a TSP for a depository institution are subject to regulation and examination to the same extent as if such services were performed by the depository institution itself. Accordingly, the Federal bank regulatory agencies examine the adequacy of TSPs' cybersecurity programs as part of their examinations of IT risk management, controls, and information security. Examinations are conducted using the same FFIEC information technology work programs that are applicable to depository institutions. A report of examination is then issued to the TSP, along with an URSIT rating. The TSP's examination report also is made available to insured financial institutions using the examined services at the time of the examination. The supervision program standards used by agencies can be found in the FFIEC IT Examination Handbook *Supervision of Technology Service Providers* booklet.

In addition, under the Dodd-Frank Act, the Financial Stability Oversight Council (Council), of which the OCC is a member, has the ability to designate critical payment, clearing, settlement and other financial market utilities as systemically important. Designated financial market utilities performing payment, clearing, or settlement activities are subject to heightened prudential standards and supervision by the Board of Governors of the Federal Reserve System.

Also, the OCC is a member of the Financial and Banking Industry Infrastructure Council (FBIIC) and directly interacts with other financial sector regulatory agencies. The FBIIC coordinates efforts to improve the reliability and security of financial information infrastructure. Through this interaction, the OCC can elevate any concerns it has with financial sector service providers that are supervised by other regulatory agencies.

Q.3. Are there additional tools that would be helpful to have?

A.3. It would be helpful if sectors such as telecommunications and public utilities, upon which banks depend, were subject to similar standards and oversight.

Q.4. Like Federal regulators, State financial regulators are also incorporating cybersecurity considerations into their examination and supervision of regulated institutions. On December 10, for example, the New York Department of Financial Services (NYDFS) announced new examination procedures relating to information technology (IT), including a focus on cybersecurity as part of an institution's risk-management strategy.

While there appears to be some overlap with Federal financial regulators' requirements, there also seem to be some notable differences, such as in the information requested and whether the level of scrutiny varies based on factors like the size of the institution. One press report in the *American Banker* describes NYDFS's requirements as "tougher than the FFIEC's."

How would you compare the FFIEC's cybersecurity approach and examination procedures to State efforts such as NYDFS's?

A.4. The OCC by itself, and in conjunction with other members of the FFIEC, has developed a comprehensive IT supervision program that includes supervisory guidance and examination procedures relating to cybersecurity. This approach has been in place for several years and the NYDFS' recently announced examination procedures appear similar.

The FFIEC IT Examination Handbook includes 11 individual booklets covering examination areas such as IT Management, IT Audit, Information Security, Development and Acquisition, Operations and other key technology control functions. Each of these booklets, and the Information Security booklet in particular, addresses cybersecurity controls.

The FFIEC also has issued a number of guidance statements covering cybersecurity-related risks including:

- *Authentication in an Internet Banking Environment Guidance* and the related supplement.
- *Cyber Attacks on Financial Institutions' ATM and Card Authorization Systems Joint Statement.*
- *Distributed Denial of Service Attacks, Risk Mitigation, and Additional Resources Joint Statement.*
- *Threat and Vulnerability Monitoring and Information Sharing Statement.*

In addition to guidance issued jointly through the FFIEC, examples of guidance issued specifically by the OCC include:

- OCC Bulletin 2008-16 *Information Security: Application Security.*
- OCC Bulletin 2013-29 *Third-Party Relationships: Risk Management Guidance.*

Since cybersecurity threats and attacks evolve, the OCC and FFIEC have mechanisms in place to continually reevaluate and strengthen overall information technology supervision processes. We compare and leverage information from recognized governmental, regulatory, and industry frameworks and standards when developing our examination programs to ensure the scope of our examinations adequately cover evolving risks.

Recognizing the need to continue to strengthen supervision of cybersecurity processes at financial institutions, FFIEC members piloted a cybersecurity examination work program (Cybersecurity Assessment) at over 500 community financial institutions to evaluate their preparedness to mitigate cyber risks. The FFIEC members are using the results of this Cybersecurity Assessment to identify and prioritize actions to enhance the effectiveness of cybersecurity-

related supervisory programs, guidance, notification expectations, and examiner training.

Q.5. What operational areas does the FFIEC consider most important for cybersecurity? How does this compare to State approaches, such as NYDFS's?

A.5. The OCC assesses the key operational areas needing examination coverage based on the inherent risk of each institution supervised. A financial institution's inherent risk is based on the products and services it offers, its processing volumes, customer base, technologies used, third-party connectivity, and a number of other factors.

While the risks and corresponding control expectations will differ based on the inherent risks of the institution, key areas of our focus include:

- Risk Management and Oversight;
- Threat Intelligence and Collaboration;
- Cybersecurity Controls;
- External Dependency Management; and
- Cyber Incident Management and Resiliency.

These areas of focus are similar to those of the NYDFS.

Q.6. Because of the fast-evolving nature of the cybersecurity field, to what extent does the FFIEC look to State efforts for possible models or elements to incorporate into Federal approaches?

A.6. The OCC and other FFIEC members, which include State bank regulators, have been considering many statutory, regulatory and industry-recognized frameworks, such as the Federal Information Security Modernization Act requirements, National Institute of Standards and Technology publications and framework, Control Objectives for Information and Related Technology framework, International Organization for Standardization standards, Capability Maturity Models, and others when developing supervisory policies and examination programs.

The OCC also monitors State laws for possible elements to incorporate in its guidance and examination approaches, if appropriate. For example, when promulgating its customer information guidance in 2005, the OCC reviewed and was guided by the California breach notification law.

Q.7. Are there elements of NYDFS's model that FFIEC is considering incorporating? For example, is the FFIEC considering expanding the information it requests to include any items covered by NYDFS's new policy?

A.7. Information outlined in the NYDFS letter, dated December 10, 2014, on its New Cyber Security Examination Process generally is already requested as part of ongoing examinations at the financial institutions we supervise. The OCC has requested such information from institutions for quite some time and tailors its requests for information based on the risk and complexity of products and operations of the individual institution being examined. Examples of the type of information requested can be found in the FFIEC IT Examination Handbook.

Q.8. To what extent are Federal financial regulators engaging with State regulators more generally relating to cybersecurity examinations and supervision, to help inform State regulators as well as to be informed by their experiences?

A.8. State banking regulators are represented on the FFIEC. The Chair of the State Liaison Committee (SLC) is a voting member of the FFIEC and the SLC is comprised of representatives from the Conference of State Banking Supervisors, the American Council of State Savings Supervisors, and the National Association of State Credit Union Supervisors.

The State Liaison Committee is also represented on the FFIEC Task Force on Supervision's IT Subcommittee and the CCIWG. These groups are responsible for developing and implementing the FFIEC IT guidance statements, work programs, and the cybersecurity pilot outlined throughout this response. These groups also provide a forum for Federal and State regulators to share experiences regarding cybersecurity examinations and supervision.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR WARNER FROM VALERIE ABEND

Q.1. In responding to all questions below (in every category), please respond as if a "data security breach" is the "unauthorized access to, or acquisition from, a system operated or maintained by a financial institution or other entity within the financial services industry, or an agent, affiliated organization or service provider to that financial institution or other financial services entity, that compromises the protection, security, integrity, confidentiality, or privacy of any customer financial information that is itself personally identifiable or that may be associated with personally identifiable information of a customer."

How many data security breaches of systems operated or maintained by a financial institution or other entity within the financial services industry—whether such breach has been publicly reported or not—is your Government department or agency aware occurred during 2013 or 2014? In responding to this question, please note the following request for an explanation:

If your response to the forgoing question is that you do not have knowledge of any such data security breaches whatsoever, please indicate why your department or agency is not aware of any breaches given the public reports of multiple breaches within the industry in 2013 or 2014.

Additionally, if your department or agency has knowledge of such data security breaches that includes nonpublic information, and your answer will indicate that your are subject to a confidentiality obligation that prohibits your answering this question completely, please indicate which specific Federal law or other rule prohibits you from testifying to the Committee about this information on data security breaches of which your department or agency has knowledge.

A.1. All national banks and Federal savings associations are expected to report to the OCC "as soon as possible when the institution becomes aware of an incident involving unauthorized access to or use of 'sensitive customer information,'" as defined in 12 CFR

Part 30 Appendix B, Supplement A (national banks), and Part 170, Appendix B, Supplement A (Federal savings associations) (referred to in the answers that follow as "The Response Program Guidance" or the "Guidance"). The OCC issued the Guidance together with the Board of Governors of the Federal Reserve System (State member banks), the Federal Deposit Insurance Corporation (State nonmember banks) and the National Credit Union Administration (credit unions).

During 2013 and 2014, there were approximately 20 reported security breaches of systems at financial institutions supervised by the OCC that fell within the scope of the Response Program Guidance.

Q.2. Of those data security breaches at financial institutions and/or other entities within the financial services industry which your department or agency is aware occurred in 2013 or 2014, please indicate:

Approximately how many financial services customers—whether individuals or organizations—you estimate were affected by each of those data security breaches.

A.2. The number of customers impacted by any one of the events about which the OCC was notified range from less than 10 customers to over 83 million customers.

While a single event can potentially affect millions of customers, most events have had an impact on fewer than one thousand customers, with many of the individual events affecting a small number of customers.

Q.3. How many data security breaches resulted in individual customer notices mailed, emailed or otherwise personally delivered to affected customers by the financial institution or other financial services entity?

A.3. The Response Program Guidance states that a financial institution should notify a customer of unauthorized access to sensitive customer information if it determines that the misuse of such information has occurred or is reasonably possible. OCC examiners, as a part of their ongoing supervisory activities, determine whether a financial institution that experiences a breach of sensitive customer information has notified customers in accordance with the Guidance. OCC examiners also determine whether the institution has policies and procedures to ensure that it is complying with any relevant State laws.

Of the incidents listed in response to Question 1 above, all but three resulted in direct notification to the affected customers. In two instances, it was determined that while malware affected the bank's system, no sensitive customer information was viewed or removed from the bank's system and thus misuse of sensitive customer information did not occur and was not reasonably possible, within the meaning of the Response Program Guidance. In the third instance, the type of information accessed did not meet the definition of sensitive customer information contained in the Response Program Guidance. Therefore, in these cases, notification was not required. In the third instance, the institution did, however, issue a public press release and posted notice on its public Web site.

Q.4. How many data security breaches resulted in some form of public notice by the financial institution or other financial services entity? (In response to this subquestion, please indicate for each data security breach if notice was made to major media outlets in the geographic region served by the institution or entity, and/or if the notice resulted from media reports following a public regulatory filing.)

A.4. The Response Program Guidance does not require public notification to media outlets. The OCC has observed that financial institutions typically issue a press release or public statement for large-scale breach events.

Q.5. How many data security breaches have never resulted in any form of individual customer notices mailed, emailed, or otherwise personally delivered to affected customers by the financial institution or other financial services entity?

A.5. Of the incidents noted above, there is only one data security breach where an institution did not notify affected customers. As described above, it was determined that the customer information accessed or removed from the institution's system did not meet the definition of sensitive customer information described in the Response Program Guidance. The institution did, however, issue a public press release and posted notice on its public Web site about the breach event.

Q.6. Of those data security breaches which you are aware occurred in 2014, and for which no individual customer notice was given by the financial institution or other financial services entity, has your department or agency investigated the circumstances of the breach and considered taking any action to require or encourage individual customer notice of the same by such institution or entity?

A.6. When the OCC is notified that a breach of sensitive customer information has occurred, as defined by the Response Program Guidance, and the institution determines that the information has been or reasonably likely to be misused, a financial institution is expected to provide notice to affected customers. The OCC reviews the facts upon which the institution's determination is based to ensure that customers are notified when warranted.

Q.7. Has your department or agency ever engaged in any enforcement action against a financial institution or other entity within the financial services industry for failure to individually notify affected customers of a data security breach suffered by that entity?

Has your department or agency ever assessed any civil penalty or fine against a financial institution or other entity within the financial services industry for failure to individually notify affected customers of a data security breach suffered by that entity?

If the answer to either question is yes, please specify the specific date of the department or agency action, the type of action taken, the entity which was subject to the action, and the amount of any penalty or fine that was assessed. If the answer to either question is no, please indicate the reason why your department or agency has not.

A.7. The OCC has not brought an enforcement action against a financial institution or other entity within the financial services in-

dustry for failure to individually notify affected customers of a "data security breach" suffered by that entity, as defined in Question 1. However, between 2009 and 2013, the OCC took formal enforcement actions against 60 national banks for failing to have adequate information security programs and required them to enhance their information technology systems and/or third-party management processes.

National banks and Federal savings associations are expected to provide notice to customers in accordance with the Response Program Guidance and any applicable State law. The OCC has not observed failures to provide this notice and therefore has not taken any enforcement action requiring a financial institution to do so.

Q.8. Based in part to the OCC's responses to the questions above, in addition to other information it deems relevant, please give the Committee your complete and thorough assessment of the following questions regarding the interpretive guidance issued by the OCC, Federal Reserve Board, FDIC, and OTS on March 29, 2005, to every financial institution regarding their implementation of a response program designed to address incidents of unauthorized access to sensitive customer information maintained by the financial institution or its service provider:

Has the OCC conducted an annual or other periodic review of the interpretive guidance since its issuance in 2005 and, if so, what are the OCC's conclusions from those reviews with respect to the current applicability and sufficiency of the interpretive guidance to today's data security breaches?

A.8. The OCC conducts periodic reviews of our Response Program Guidance, and has done so most recently as part of a Cybersecurity Risk Assessment of over 500 financial institutions that was conducted under the auspices of the FFIEC in which the OCC participated. We currently are reviewing the results of the Assessment together with other sources of information, to determine whether the Guidance should be changed and, if so, how best to make these changes.

Q.9. In light of the 47 State laws regarding breach notification that have been enacted to date, has the OCC reviewed the circumstances under which financial institutions may be subject to such laws, and has it considered updating the 2005 interpretive guidance to bring it in line with current requirements for all businesses subject to such State laws to individually notify affected customers when that business suffers a breach (as defined under each law)?

A.9. Financial institutions are subject to State breach notification laws that provide greater protections than the Response Program Guidance. See Section 507 of the Gramm-Leach-Bliley Act (GLBA), 12 U.S.C. §6807. While drafting the Response Program Guidance in 2005, the OCC reviewed and was guided by existing State laws, in particular California's breach notification law. The OCC also reviews State breach notification laws from time-to-time for new developments. Many of the current State laws are similar to the Response Program Guidance.

Q.10. In the opinion of the OCC, does the 2005 interpretive guidance legally "require" financial institutions, or other entities within

the financial services industry, to provide individualized notices via mail, email, or other personal deliver service to all potentially affected customers when a system operated or maintained by a financial institution or other financial services entity, or an agent, affiliated organization or service provider to that financial institution or other financial services entity, suffers a data security breach? If your response to this question is "yes," please explain the legal reasoning that supports your conclusion that the interpretive guidance "requires" financial institutions to notify customers in light of the text of the guidance indicating financial institutions "should" contain procedures to notify customers when warranted, and does not explicitly State that financial institutions "shall" notify affected customers (similar to the express obligation in Sate data breach notification laws).

A.10. As noted above, national banks and Federal savings associations are subject to State law breach notice requirements. The Response Program Guidance interprets section 501(b) of the GLBA and the lnteragency Guidelines Establishing Information Security Standards. See 12 CFR Part 30, Appendix B (national banks) and Part 170, Appendix B (Federal savings associations). The Guidelines, which are enforceable by their terms, require banks to have a response program that specifies actions to be taken when the bank suspects or detects that unauthorized individuals have gained access to customer information systems, including appropriate reports to regulatory and law enforcement agencies. The Guidance elaborates on this requirement to state that the OCC expects a financial institution's response program to include procedures for notifying customers when there has been unauthorized access to their sensitive information and misuse of the information has occurred or is reasonably possible.

Q.11. If your response to the subquestion above indicates that individual customer notice is legally "required" for a data security breach, please indicate whether the OCC has ever enforced such a "requirement" against any financial institution or other financial services entity, or any agent, affiliated organization, or service provider to that financial institution or other financial services entity. If the OCC has not enforced such a legal "requirement" to notify in all cases of which it is aware of a data security breach that has not resulted in such notice, please explain why it has not enforced this requirement in each case.

A.11. Please see the response to Questions 7 and 8.

Q.12. If your response to the subquestion above indicates that individual customer notice is legally "required" for a data security breach, please indicate if the OCC has ever assessed any civil penalty or fine against any financial institution or other financial services entity, or any agent, affiliated organization, or service provider to that financial institution or other financial services entity, for failure to individually notify affected customers of a data security breach suffered by that entity.

A.12. Please see the response to Questions 7 and 8.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR CRAPO FROM WILLIAM NOONAN

Q.1. Fast, efficient sharing of actionable cyberthreat information between law enforcement, the intelligence community, and industry is a vitally important component of protecting information systems. While we have seen significant progress over the past couple years in the timeliness and quality of information sharing, there is still room for improvement. Please describe:

First, What steps are being taken at your agency or Department to improve the information-sharing process and more quickly disseminate actionable information to those who need it?

A.1. The U.S. Secret Service (Secret Service) continues to be committed to quickly disseminating actionable information to those who need it, and continues to take steps to further improve our ability to notify victims of computer intrusions and widely share information to aid organizations in protecting their computer networks from the latest cybercriminal methods. In FY2014, the Secret Service notified or responded to network intrusion incidents at nearly 400 organizations.

As the Secret Service investigates cybercriminal activity, we frequently discover new criminal techniques or methods that can inform computer network defense activities. As the Secret Service discovers such information, we partner with the National Cybersecurity and Communications Integration Center (NCCIC), and other public and private entities, to rapidly and widely disseminate actionable cybersecurity information, while protecting victim privacy and ongoing investigations.

For example, this past summer, UPS Stores, Inc. announced it had been able to use information published in a joint report on the Back-Off malware to protect itself and its customers from cybercriminal activity. The information in this report was derived from a Secret Service investigation of a network intrusion at a small retailer in upstate New York. As a result, UPS Stores, Inc. was able to identify 51 stores in 24 States that had been impacted, approximately 1 percent of their total stores, and then contain and mitigate this cyber incident before it developed into a major data breach.

The Secret Service continues to expand its network of Electronic Crimes Task Forces (ECTFs) and build relationships with public and private-sector partners in order to further improve our ability to share actionable cybersecurity information in a timely manner.

Q.2. Second, what obstacles or constraints delay the dissemination of such information?

A.2. The primary constraint in disseminating cybersecurity information is sufficient personnel to analyze the cyberthreat information collected through Secret Service investigations, in order to extract the relevant actionable cybersecurity information to enable computer network defense activities, while protecting victim privacy and ongoing investigations.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR WARNER FROM WILLIAM NOONAN

Q.1. In responding to all questions below (in every category), please respond as if a "data security breach" is the "unauthorized access to, or acquisition from, a system operated or maintained by a financial institution or other entity within the financial services industry, or an agent, affiliated organization or service provider to that financial institution or other financial services entity, that compromises the protection, security, integrity, confidentiality, or privacy of any customer financial information that is itself personally identifiable or that may be associated with personally identifiable information of a customer."

How many data security breaches of systems operated or maintained by a financial institution or other entity within the financial services industry—whether such breach has been publicly reported or not—is your Government department or agency aware occurred during 2013 or 2014? In responding to this question, please note the following request for an explanation:

If your response to the forgoing question is that you do not have knowledge of any such data security breaches whatsoever, please indicate why your department or agency is not aware of any breaches given the public reports of multiple breaches within the industry in 2013 or 2014.

Additionally, if your department or agency has knowledge of such data security breaches that includes nonpublic information, and your answer will indicate that your are subject to a confidentiality obligation that prohibits your answering this question completely, please indicate which specific Federal law or other rule prohibits you from testifying to the Committee about this information on data security breaches of which your department or agency has knowledge.

A.1. The Secret Service has identified 52 case files involving confirmed data breaches of financial services entities in 2013 or 2014.

Q.2. Of those data security breaches at financial institutions and/or other entities within the financial services industry which your department or agency is aware occurred in 2013 or 2014, please indicate:

Approximately how many financial services customers—whether individuals or organizations—you estimate were affected by each of those data security breaches.

A.2. The Secret Service does not generally keep records of the number of customers affected, and instead focuses on the total fraud losses or other measures of economic impact. A review of the 52 case files indicates that the cases vary from potentially a single customer impacted to millions of customers impacted. Recorded fraud losses range from $2,000 to in excess of $8 million.

Q.3. How many data security breaches resulted in individual customer notices mailed, emailed, or otherwise personally delivered to affected customers by the financial institution or other financial services entity?

A.3. The Secret Service generally keeps no records on whether customer notifications are performed as a result of a data security

breach. The Secret Service is focused on investigating and apprehending the criminals responsible for data breaches.

Q.4. How many data security breaches resulted in some form of public notice by the financial institution or other financial services entity? (In response to this subquestion, please indicate for each data security breach if notice was made to major media outlets in the geographic region served by the institution or entity, and/or if the notice resulted from media reports following a public regulatory filing.)

A.4. The Secret Service does not generally keep records on whether the victim organization made any form of public notice.

Q.5. How many data security breaches have never resulted in any form of individual customer notices mailed, emailed, or otherwise personally delivered to affected customers by the financial institution or other financial services entity?

A.5. The Secret Service does not generally keep records on whether the victim organization made any form of notice to their customers.

Q.6. Of those data security breaches which you are aware occurred in 2014, and for which no individual customer notice was given by the financial institution or other financial services entity, has your department or agency investigated the circumstances of the breach and considered taking any action to require or encourage individual customer notice of the same by such institution or entity?

A.6. The Secret Service is focused on working collaboratively with victim companies to investigate the criminals responsible for data breaches and minimize fraud losses. The Secret Service does not have authority to require victim companies to make customer notice, and generally only encourages companies to take actions as they further our investigative aims of countering the cybercriminal activity.

Q.7. Has your department or agency ever engaged in any enforcement action against a financial institution or other entity within the financial services industry for failure to individually notify affected customers of a data security breach suffered by that entity? If yes, please specify the specific date of the department or agency action, the type of action taken, the entity which was subject to the action, and the amount of any penalty or fine that was assessed. If no, please indicate the reason why your department or agency has not.

A.7. The Secret Service has not engaged in any enforcement action against a financial institution or other entity within the financial services industry for failure to individually notify affected customers of a data security breach suffered by that entity. The Secret Service does not have any authority to engage in any such enforcement action.

Q.8. Has your department or agency ever assessed any civil penalty or fine against a financial institution or other entity within the financial services industry for failure to individually notify affected customers of a data security breach suffered by that entity? If yes, please specify the specific date of the department or agency action, the type of action taken, the entity which was subject to the action,

and the amount of any penalty or fine that was assessed. If no, please indicate the reason why your department or agency has not.

A.8. The Secret Service has never assessed any civil penalty or fine against a financial institution or other entity within the financial services industry for failure to individually notify affected customers of a data security breach suffered by that entity. The Secret Service does not have any authority to assess civil penalties or fines for such matters.

ADDITIONAL MATERIAL SUPPLIED FOR THE RECORD

LETTER TO AGENCIES SUBMITTED BY CHAIRMAN JOHNSON AND SENATOR CRAPO

United States Senate
COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS
WASHINGTON, DC 20510-6075

October 21, 2014

The Honorable Jacob Lew
Secretary
U.S. Department of the Treasury
1500 Pennsylvania Avenue, NW
Washington, DC 20220

The Honorable Janet Yellen
Chair
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue, NW
Washington, DC 20551

The Honorable Martin Gruenberg
Chairman
Federal Deposit Insurance Corporation
550 17th Street, NW
Washington, DC 20429

The Honorable Thomas Curry
Comptroller
Office of the Comptroller of the Currency
400 7th Street, SW
Washington, DC 20219

The Honorable Debbie Matz
Chair
National Credit Union Administration
1775 Duke Street
Alexandria, VA 22314

Dear Secretary Lew, Chair Yellen, Comptroller Curry, Chairman Gruenberg, and Chair Matz:

Over the past decade, cybersecurity has become a foremost national priority for both the government and the private sector. Our networks and information systems are under attack from a wide range of actors, including sophisticated criminal organizations, nation-states, and "hacktivists," who commit cyberattacks for a variety of reasons. Cyberattacks come in many different forms, including distributed denial service attacks against websites, point-of-sale attacks against merchants, malware attacks to infiltrate secure systems, phishing scams, and many more.

As Chairman and Ranking Member of the U.S. Senate Committee on Banking, Housing, and Urban Affairs, we are particularly concerned with the safety and integrity of the U.S. financial system, especially as it pertains to Americans' personal financial information. The economic impact of cyberattacks is staggering. A recent Center for Strategic and International Studies report projected global economic losses of up to $575 million annually in the U.S. alone. An earlier report cited by President Obama estimated losses of $1 trillion just from intellectual property theft by cyberattacks over the previous year. Financial institutions are a particularly lucrative target. Many find themselves under constant attack, with some spending up to $250 million per year on cybersecurity.

According to Larry Zelvin, Director of the National Cybersecurity and Communications Integration Center at the Department of Homeland Security (DHS), of the sixteen critical infrastructure sectors, "finance probably wins the cybersecurity threat award. . . . [The industry is] a massive target . . . because [it is] where the money is." The Office of the Comptroller of the Currency recently noted in its Semi-Annual Risk Perspective for U.S banks that [cyberattacks and breaches] are a leading operational risk and that "recurring security breaches at retail merchants highlight the interdependencies in today's payment systems…there is concern that criminals will transition from disruptive attacks to attacks that are intended to cause destruction and corruption."

Over the past year, we have seen a notable increase in the frequency and scope of data breaches at U.S. companies, which often involve the theft of customers' financial and other personal information. According to a recent study conducted by the Ponemon Institute, 43 percent of companies experienced a breach in the last year, up from 33 percent the prior year, and 60 percent reported a breach in the last two years. These numbers likely underestimate the magnitude of the current threat, as many breaches occur undetected. In the words of former FBI Director Robert Mueller, "There are only two types of companies: those that have been hacked, and those that will be. Even that is merging into one category: those that have been hacked and will be again." Earlier this month, JPMorgan Chase, the nation's largest bank by assets, announced that personal information from 76 million households and 7 million small businesses had been compromised, one of the largest corporate breaches in history. Additional reports indicate that at least a dozen financial companies were targeted by the same hacker group. Ensuring that customer information is secure is essential to the integrity of the financial system. Furthermore, as new forms of payment become increasingly popular, strong data security will take on even greater importance.

While we recognize that federal agencies have heightened their attention to cybersecurity issues, we are writing to seek more information on the role your agency or Department is playing to protect our financial system from cyberattacks. Please also respond to the following questions to the extent they are applicable to your agency or Department.

First, what is your agency's or Department's process for acquiring information on potential or occurring cyberattacks and passing information to the financial services sector in a timely manner? What obstacles and/or legal restrictions hinder information sharing? Specifically, as the financial services sector's Sector-Specific Agency, Treasury has a number of responsibilities described in Presidential Policy Directive 21 and Executive Order 13636. What actions is Treasury taking to fulfill those responsibilities?

Second, please describe what coordination and interaction each of your agencies and Department have with each other, as well as law enforcement, DHS, and the intelligence community. How would legislative proposals improve or impede your coordination and relationships with other government agencies?

Third, last year, the Financial Stability Oversight Council (FSOC) recommended that regulators devote additional supervisory attention toward cybersecurity. What is the FSOC's role in monitoring cybersecurity risks?

Finally, earlier this year the Federal Financial Institutions Examination Council announced that it is planning cybersecurity and risk-mitigation assessments to help smaller institutions address cybersecurity gaps. Please describe this effort and what particular considerations or risks may exist at institutions of varying sizes.

It is vital that government agencies and private institutions remain vigilant and coordinated in ensuring the safety and security of our networks, especially as it applies to the valuable personal and financial information of American consumers.

Thank you for your attention to this matter.

Sincerely,

Tim Johnson

Mike Crapo

LETTER OF RESPONSE SUBMITTED BY JOINT AGENCIES

December 9, 2014

The Honorable Timothy P. Johnson
Chairman
Committee on Banking, Housing, and Urban Affairs
United States Senate
Washington, DC 20510

Dear Chairman Johnson:

Thank you for your letter dated October 21, 2014, regarding the role of our agencies in protecting the United States financial system from cyber threats.

We agree with you that cybersecurity is a foremost national priority. Responding to the cyber threat demands a commensurate level of attention and one that can be best achieved by recognizing the distinct roles, responsibilities, and authorities of organizations. This includes collaboration between cabinet agencies such as Treasury, independent state and federal regulatory agencies, law enforcement, the intelligence community, and, importantly, the private sector companies, which own and operate the vast majority of our nation's financial sector infrastructure.

The financial sector, federal and state regulators, and the Treasury coordinate through the Financial and Banking Information Infrastructure Committee (FBIIC) to address critical infrastructure concerns including cyber threats and vulnerabilities. Earlier this year, we instituted regular meetings of the top officials from each FBIIC member to focus on strategic, policy-level issues around cybersecurity and related coordination. This collaboration is contributing to shared threat briefings, the development of more dynamic information sharing processes, and exercises to test incident response protocols.

Additionally, the federal banking and credit union agencies coordinate and share information through the Federal Financial Institutions Examination Council (FFIEC). Over the past year, through the creation of the Cybersecurity and Critical Infrastructure Working Group (CCIWG), the FFIEC members have undertaken a number of steps to assess the level of preparedness among financial institutions and raise awareness to help institutions to improve their cybersecurity preparedness.

We look forward to continuing to engage with you on this issue in the future. The nature of the cyber threat will continue to require our vigilance and dedication. We are providing you with this joint response to reinforce our belief in the importance of both this issue and the close coordination required to address it. You should expect to receive individual letters from each of our agencies that reflect our unique roles and authorities.

Sincerely,

Jacob J. Lew
Secretary
Department of the Treasury

Janet L. Yellen
Chair
Board of Governors of the
Federal Reserve System

Martin J. Gruenberg
Chairman
Federal Deposit Insurance Corporation

Thomas J. Curry
Comptroller of the Currency
Office of the Comptroller of the Currency

Debbie Matz
Chair
National Credit Union Administration

Identical letter sent to:
The Honorable Michael D. Crapo

LETTER OF RESPONSE SUBMITTED BY THE DEPARTMENT OF THE TREASURY

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

December 9, 2014

The Honorable Timothy P. Johnson
Chairman
Committee on Banking, Housing, and Urban Affairs
United States Senate
Washington, DC 20510

Dear Chairman Johnson:

Thank you for your letter regarding federal government efforts to protect the U.S. financial system from cybersecurity threats. In addition to our joint letter with the federal banking and credit union regulators reaffirming our commitment to and extensive collaboration on cybersecurity matters, the Secretary asked that I write to you separately to provide you more detail on Treasury's role and efforts.

Treasury serves as the day-to-day federal interface and coordinating agency for the financial services sector under Presidential Policy Directive 21 (PPD-21). PPD-21 establishes a unified approach to strengthen and maintain secure, functioning, and resilient critical infrastructure against cyber and physical threats in 16 critical sectors. In order to fulfill its responsibilities under PPD-21 and the related executive order (EO 13636), Treasury:

- Coordinates with the White House, the Department of Homeland Security (DHS), law enforcement and the intelligence community, as well as independent financial regulators—activities designed to strengthen the resilience of the financial sector;
- Interfaces between financial institutions and government agencies to, among other things, facilitate Requests for Technical Assistance and prioritize government resources to help respond to incidents;
- Facilitates the sharing of timely, actionable information regarding cyber threats and incidents with a view toward limiting damage from intrusions and stopping contagion across systems, networks, and institutions;
- Assists in effective, prompt response and recovery from cyber incidents to reassure the public and protect public and private assets;
- Promotes best practices, including the NIST Cybersecurity Framework, that help operators of financial systems prevent attacks from succeeding and minimize the damage from any successful attacks; and
- Contributes to governmental reports, including the development of an Incentives Report and Financial Services Sector Specific Plan.

Treasury coordinates with federal and state regulators through the Financial and Banking Information Infrastructure Committee (FBIIC) to address critical infrastructure concerns, including cyber threats and vulnerabilities. The eighteen members of FBIIC engage on issues such as streamlining and improving information sharing; identifying best practices across the sector (including for small and medium size financial institutions); and enhancing the coordination of incident responses. Recently, Treasury Secretary Lew and Deputy Secretary Bloom Raskin began to regularly convene top officials from the FBIIC member agencies and organizations. These meetings focus on strategic, policy-level issues around cybersecurity and other operational risks within the financial sector.

In order to monitor matters related to financial stability, the Financial Stability Oversight Council (FSOC) also receives specific input on the state of cybersecurity risks through FBIIC representatives of its member agencies, as well as from Treasury directly. This has included holding public and private sessions on cybersecurity, including threat briefings related to ongoing incidents. However, FSOC is not the forum for day-to-day coordination on cybersecurity and defers that responsibility to the FBIIC.

As you identify in your letter, information sharing is a crucial component of government and private sector cybersecurity efforts. Establishing shared awareness of cyber threats requires that diverse stakeholders — including government agencies and private sector companies — with insights into malicious activity combine their knowledge to identify actionable information to better secure systems. To help facilitate timely sharing and analysis of information about cyber threats to the financial sector, Treasury established the Financial Sector Cyber Intelligence Group (CIG). The CIG develops and shares actionable information and collaborates with interagency partners to provide classified and unclassified cybersecurity briefings to private sector officials. The CIG works especially closely with DHS and the FBI in these efforts to provide financial sector expertise through established liaison officers. The CIG also works closely with private sector organizations, including the Financial Service Information Sharing and Analysis Center (FS-ISAC). To that end, we commend the FFIEC for their cybersecurity examination pilot and particularly their recommendation that "firms of all sizes participate in the FS-ISAC as part of their process to identify, respond to, and mitigate cybersecurity threats and vulnerabilities".

We look forward to continuing discussions with you on this critically important and highly complex subject so that we may work together to advance the objective of improving financial sector resiliency for the twenty-first century.

Sincerely,

Randall DeValk

Randall DeValk
Counselor to the Secretary

Identical letter sent to:
The Honorable Michael D. Crapo

LETTER OF RESPONSE SUBMITTED BY FEDERAL DEPOSIT INSURANCE CORPORATION

FEDERAL DEPOSIT INSURANCE CORPORATION, Washington, DC 20429

MARTIN J. GRUENBERG
CHAIRMAN

November 24, 2014

Honorable Tim Johnson
Chairman
Committee on Banking, Housing, and Urban Affairs
United States Senate
Washington, D.C. 20510

Dear Chairman Johnson:

Thank you for your letter seeking information on the role the Federal Deposit Insurance Corporation is playing to protect our financial system from cybersecurity threats. We share your concern that cybersecurity threats pose a risk to the safety and integrity of the U.S. financial system.

The FDIC recognizes that there are several essential components to our response to the cybersecurity threats facing the financial services industry. These include the process of acquiring and sharing actionable information. In this regard, the FDIC actively participates in a wide range of interagency and public/private information-sharing initiatives. In addition, the FDIC coordinates closely with our fellow regulators, law enforcement, and the intelligence community in addressing threats to the financial industry.

The FDIC also is engaged in strengthening our cybersecurity supervisory programs. The FDIC regularly and routinely evaluates all of its regulated financial institutions' information security programs through our information technology (IT) examinations. The federal banking agencies also conduct IT examinations of major technology service providers that provide services to financial institutions. These examinations are designed, in part, to ensure that financial institutions protect both bank and customer information. Depending on the findings from our examinations, informal or formal enforcement action may be pursued to achieve corrective actions.

The FDIC's Division of Risk Management Supervision prepared the enclosed responses to your questions. Thank you for your interest in this important matter. If you have additional questions, please call me at (202) 898-3888 or Eric Spitler, Director of the Office of Legislative Affairs, at (202) 898-7140.

Sincerely,

Martin J. Gruenberg

Martin J. Gruenberg

Enclosure

Response to an Inquiry from
The Honorable Tim Johnson and The Honorable Mike Crapo
Committee on Banking, Housing, and Urban Affairs
United States Senate

Q1: What is your agency's or department's process for acquiring information on potential or occurring cyberattacks and passing information to the financial services sector in a timely manner? What obstacles and/or legal restrictions hinder information sharing?

A1. Cybersecurity has become an issue of the highest importance for the Federal Financial Institution Examination Council (FFIEC) members[1] and throughout the federal government. The rapidly evolving nature of cybersecurity risks reinforces the need for regulators, financial institutions, and critical technology service providers to have appropriate procedures in place for collecting, monitoring, sharing, and responding to the latest cyber-related threat information. As such, the FDIC actively participates in interagency and public/private information-sharing initiatives including: the Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center's Cyber Unified Coordination Group; the Financial and Banking Information Infrastructure Committee (FBIIC), a group chartered as part of the President's Working Group on Financial Markets to facilitate interagency communication among federal agencies; and, the Financial Services Information Sharing and Analysis Center (FS-ISAC), a public/private information forum for sharing cybersecurity and information technology related risk information. The FDIC also has served a unique role since 2007 by providing a staff member to serve as the FBIIC liaison to DHS. This position initially was embedded with DHS' Infrastructure Protection area, supporting the DHS Banking and Finance Sector specialist. Given the increasing cybersecurity risk faced by the financial services sector, this liaison role expanded to DHS's National Cybersecurity and Communications Integration Center (NCCIC) after its activation in 2009. This individual also represents the FBIIC on the NCCIC's Cyber Unified Coordination Group.

Real-time threat and vulnerability information also is obtained by each of the individual FFIEC members from a variety of sources, including directly from supervised financial institutions, examiners, the Department of the Treasury, and technology service providers.

Whenever possible, and as appropriate, the FDIC and the FFIEC share information with the financial services industry to provide details of cybersecurity threats, risk mitigation steps, and reference materials to consider. Some of these issuances are posted on FFIEC member public websites, while others are distributed through non-public sites available only to examiners and financial institutions. When requested by the Treasury, the FDIC has shared sensitive information regarding potential or occurring cyber-attacks directly with financial institutions through a secure non-public web portal. Financial institutions also may receive cybersecurity threat and vulnerability information from law enforcement and intelligence agencies that maintain relationships with the private sector, and through information sharing forums such as

[1] The FFIEC members are the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, the Consumer Financial Protection Bureau, the National Credit Union Administration, and the State Liaison Committee.

the FS-ISAC and DHS's United States Computer Emergency Readiness Team (US-CERT). On April 10, 2014, the FDIC issued a press release providing the institutions it supervises with a list of the available sources for cyber-related threat and mitigation information.

The FDIC also relies on information-sharing relationships to ensure our operations are safe and secure. The FDIC has a designated Federal Senior Intelligence Coordinator, who promotes intelligence sharing within the FDIC and between the FDIC and other agencies. In addition, forums, such as the federal Chief Information Officer Council, provide critical insights on sensitive cybersecurity matters and include law enforcement, the intelligence community, and DHS. To ensure sensitive information is protected and shared appropriately, the FDIC recently created a Sensitive Compartmented Information Facility for exchanging classified intelligence internally and with other agencies.

While the scope of information sharing among the FFIEC members and the industry is generally strong, the rapidly evolving nature of cybersecurity incidents has highlighted gaps in the legal framework. For example, the Gramm-Leach-Bliley Act (GLBA), Section 501(b) requires the bank regulatory agencies to develop Interagency Guidelines Establishing Information Security Standards (12 C.F.R. 364, Appendix B) requiring every financial institution to have an information security program approved by the institution's board of directors to protect customer information. Similarly, the Federal Trade Commission (FTC) can enforce standards for protection of customer information (16 C.F.R. 314) by all other financial institutions that are not insured depository institutions. However, others, such as retailers, are not subject to national regulatory requirements to protect customer data. Further, the Bank Service Company Act (BSCA), 12 U.S.C. 1867, was enacted in 1962. Given the significant changes that have occurred in the fields of information technology (IT) and cybersecurity since 1962, the FDIC would recommend a review of the Bank Service Company Act to determine whether additional enforcement authority is necessary for the federal banking agencies with respect to non-bank financial institutions that provide direct services to banks.

Q2: Please describe what coordination and interaction each of your agencies and Department have with each other, as well as law enforcement, DHS, and the intelligence community. How would legislative proposals improve or impede your coordination and relationships with other government agencies?

A2. Coordination among the FFIEC members, law enforcement, and the intelligence community is critically important to maximize intelligence awareness within the FDIC and the financial services industry at large. In order to facilitate this coordination, the FDIC has designated representatives that coordinate these relationships and ensure information is disseminated appropriately. While we recognize the support of our law enforcement and intelligence partners, information sharing obstacles associated with ongoing law enforcement investigations can present a challenge. For example, the findings from forensic analysis and the methodologies used by attackers identified during law enforcement investigations may be useful in drafting supervisory guidance or responses if shared earlier in the process with regulators that possess appropriate security clearances. Moreover, the interagency sharing of financial institution cyber incident information beyond just the primary federal regulator may be valuable to support our role as insurer and backup regulator. As such, the FDIC and the other FFIEC members are

working through the FBIIC to strengthen information sharing protocols among law enforcement and the FFIEC.

Q3: The Financial Stability Oversight Council (FSOC) recommended that regulators devote additional supervisory attention toward cybersecurity. What is the FSOC's role in monitoring cybersecurity risks?

A3. As established by the *Dodd-Frank Wall Street Reform and Consumer Protection Act* (Pub. L. 111-203), the Financial Stability Oversight Council (FSOC) is tasked with identifying risks to the financial stability of the United States, promoting market discipline, and responding to emerging risks to the stability of the United States financial system. The Chairman of the FDIC serves as one of the ten voting members of the FSOC that provides a forum for regulatory coordination and information-sharing regarding policy development, rulemaking, supervisory information, and reporting requirements. The FSOC has identified cyber-attacks as a potential threat to the financial system and recommended that financial regulators continue their efforts to assess cyber-related vulnerabilities facing their regulated entities and identify gaps in oversight that need to be addressed. The establishment of the FFIEC Cybersecurity and Critical Infrastructure Working Group (CCIWG) is consistent with the recommendations of the FSOC.

The FFIEC serves as the formal interagency body empowered to prescribe uniform principles, standards, report forms, and information sharing to support the federal examination of financial institutions. While the FFIEC has in place established task forces that facilitate collaboration and information sharing, the FFIEC recognized that a more focused approach was needed to address the emerging cybersecurity challenges. In response, the FFIEC formed the CCIWG in June 2013 to serve as a liaison with the intelligence community, law enforcement, and the DHS on issues related to cybersecurity and the protection of critical infrastructure. The CCIWG is empowered to help the banking agencies collaborate in establishing cyber-related examination policy, developing training programs, coordinating responses to cybersecurity incidents, and managing information-sharing efforts.

Q4: Earlier this year the Federal Financial Institutions Examination Council announced that it is planning cybersecurity and risk-mitigation assessments to help smaller institutions address cybersecurity gaps. Please describe this effort and what particular considerations or risks may exist at institutions of varying sizes.

A4. The FFIEC members are undertaking a number of initiatives to raise awareness of financial institutions and their critical third-party service providers with respect to cybersecurity risks and the need to identify, assess, and mitigate these risks in light of the increasing volume and sophistication of cyber threats. These include:

- April 2014: Issued joint press releases informing institutions about three vulnerabilities: the OpenSSL "Heartbleed vulnerability," cyber-attacks on automated teller machines and card authorization systems, and distributed denial of service attacks.

- May 2014: Conducted a webinar for approximately 5,000 chief executive officers and senior managers from community financial institutions to highlight efforts to enhance cybersecurity measures. The FFIEC offered this webinar to raise awareness about the pervasiveness of cyber threats, discuss the role of executive leadership in managing these risks, and share actions being taken by the FFIEC.

- June 2014: Launched a cybersecurity webpage to help promote the awareness of cybersecurity and to serve as a central repository for current and future FFIEC-related materials on cybersecurity.

- June 2014: Initiated a pilot cybersecurity focused work program at more than 500 community institutions and technology service providers. The work program was completed by state and federal regulators during regularly scheduled examinations. Regulators focused particularly on risk management and oversight of threat intelligence information, cybersecurity controls, cyber incident management, technology service provider risk management, and resilience. Another aim of the pilot was to help regulators make risk-informed decisions to enhance the effectiveness of supervisory programs, guidance, and examiner training.

- November 2014: Released general observations from the Cybersecurity Assessment describing the range of inherent risks and the varied risk management practices observed among financial institutions. The document provides suggested questions for chief executive officers and boards of directors to consider when assessing their financial institutions' cybersecurity and preparedness without setting forth regulatory guidance.

- November 2014: Issued joint statement highlighting the value for institutions of all sizes of participating in cyber-related information sharing forums such as the FS-ISAC to ensure awareness of cybersecurity threats and vulnerabilities.

In addition, the FDIC recognizes that addressing cyber risks can be especially challenging for community banks and we have taken a number of independent actions to further improve awareness of cyber risks and encourage practices to protect against threats:

- July 2013: Issued a technical assistance video on information technology, highlighting for bank directors how the basic information technology governance framework applies to cyber events, such as account takeovers and distributed denial of service attacks.

- April 2014: Issued a press release urging financial institutions to utilize available cyber resources to identify and help mitigate potential threats.

- April 2014: Re-issued documents that contain practical ideas for community banks to consider when they engage in technology outsourcing. The documents are: *Effective Practices for Selecting a Service Provider*; *Tools to Manage Technology Providers' Performance Risk: Service Level Agreements*; and *Techniques for Managing Multiple Service Providers*.

- July 2014: Distributed an information package to chief executive officers of all FDIC-supervised institutions that included a copy of *Cyber Challenge: A Community Bank Cyber Exercise*. FDIC created *Cyber Challenge* to encourage community financial institutions to discuss operational risk issues and the potential impact of information technology disruptions on common banking functions. The *Cyber Challenge* exercise is designed to facilitate discussion between financial institution management and staff about operational risk issues. The exercise can provide valuable information about an institution's current state of preparedness and identify opportunities to strengthen resilience to operational risk. *Cyber Challenge* consists of four short video vignettes and related challenge questions. Each video vignette depicts a unique scenario, including an item processing failure, a customer account takeover, a phishing and malware case, and a problem with a technology service provider. The challenge questions for each vignette are designed to facilitate discussion about how the bank would respond to the scenario. Also included were lists of reference materials where participants could obtain additional information.

LETTER OF RESPONSE SUBMITTED BY THE NATIONAL CREDIT UNION ADMINISTRATION

National Credit Union Administration

Office of the Chairman

December 4, 2014

The Honorable Tim Johnson
Chairman
Senate Committee on Banking,
Housing and Urban Affairs
534 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Mike Crapo
Ranking Member
Senate Committee on Banking,
Housing and Urban Affairs
534 Dirksen Senate Office Building
Washington, DC 20510

Dear Chairman Johnson and Ranking Member Crapo:

Thank you for your October 21, 2014, letter about what NCUA is doing independently as an agency and cooperatively with our fellow financial institutions regulators and the U.S. Department of the Treasury to combat cyber-attacks. I very much agree with you about the need for regulators to take steps to protect the financial services sector from cybersecurity threats.

NCUA collaborates closely with our counterparts within the federal government to develop and issue cybersecurity guidance for federally supervised or insured credit unions. For example, our technical experts participate on the Federal Financial Institutions Examination Council (FFIEC) information security and cybersecurity working groups. We actively promote the use of the FFIEC IT Handbooks, which constitute the majority of information and cybersecurity examination guidance and policies for financial institutions.

Furthermore, we regularly receive and share information on cybersecurity and other national security threats through our participation on the Financial and Banking Information Infrastructure Committee (FBIIC). Additionally, we are developing protocols to receive and share intelligence reports on cybersecurity threats. We also receive updates on cyber-attacks directly from the Department of the Treasury, the Federal Bureau of Investigation, the Department of Homeland Security, and the U.S. Secret Service.

Moreover, NCUA has worked to align the agency's efforts with the FFIEC's initiatives through the Cybersecurity and Critical Infrastructure Working Group. We also continue to work collaboratively with our FFIEC and FBIIC counterparts to encourage credit unions to join the Financial Services Information Sharing and Analysis Center and similar organizations to increase preparedness and improve information sharing throughout the financial services sector.

In addition, NCUA has deployed a comprehensive cybersecurity resources page on our website.[1] The webpage features a wealth of information on cybersecurity threats, tactics and preventive measures for credit unions to review and use. NCUA is also in the process of developing a critical communications portal for our supervised institutions and state regulatory partners.

[1] See http://www.ncua.gov/Resources/Pages/cyber-security-resources.aspx.

1775 Duke Street - Alexandria, VA 22314-3428 - 703-518-6300

NCUA further employs a risk-based approach toward cybersecurity by focusing our specialized resources on the institutions that pose the greatest potential risk. Although our supervisory focus is on decreasing risk across the system through targeted examination of our larger institutions, we remain concerned that small institutions are equally at risk.

As part of the 2014 budget, the NCUA Board additionally established the Office of Continuity and Security Management. NCUA created this office to aggregate all security-related functions, including continuity of operations planning, physical security, and personnel security. The office also addresses national security issues affecting the financial services industry, including compliance with various statutes and orders related to the safeguarding of critical infrastructure and other national assets and protecting against cybersecurity threats.

To bolster the agency's cybersecurity expertise, NCUA's 2015 budget also included two new positions. First, the budget added a new intelligence specialist within the Office of Continuity and Security Management with knowledge of both financial sector threats and cybersecurity threats. This new position will provide support to NCUA network security and business operations by sharing information on critical infrastructure protection for the credit union sector and coordinating with the interagency initiatives jointly managed with FBIIC. Second, the budget provided for a new cybersecurity manager within the Office of Examination and Insurance. This position will help to establish the policy, risk management and communication objectives to support the cybersecurity priorities of NCUA and the interagency initiatives jointly managed with the FFIEC to protect the financial services industry.

Finally, as I have previously testified, NCUA is the only federal financial institutions regulator without the authority to examine third-party vendors, which provide technology solutions and payment systems services for small institutions. This lack of authority represents a growing regulatory blind spot that poses an increasing risk across the credit union sector, in particular as it relates to cybersecurity. NCUA again requests that Congress act on this legislative priority for the agency. A more detailed discussion of this legislative request is found below.

The remainder of this letter addresses the specific questions raised in your incoming letter.

First, your letter asks how NCUA acquires information about potential or occurring attacks and then shares that information with the financial services sector in a timely way. You also ask about legal impediments or restrictions that hinder information sharing.

As mentioned above, NCUA receives critical cybersecurity information directly from the Department of the Treasury, the Department of Homeland Security, and jointly from our FFIEC and FBIIC counterparts. The Treasury Department also is coordinating a principals' level working group through the FBIIC to address information-sharing protocols. NCUA is further establishing protocols to coordinate with the intelligence community and our partner FBIIC agencies on prioritizing collection and analysis on cybersecurity and other national security threats to the financial services sector. NCUA also receives regular unclassified cybersecurity

updates and threat reporting from the Department of Homeland Security, the Federal Bureau of Investigation, and public sources.

NCUA is not aware of specific legal restrictions or impediments concerning the sharing of information among the federal regulatory agencies with supervisory oversight for financial institutions. Provisions of federal law specifically contemplate that the agencies will share examination and supervisory information. For example, federal law provides that covered agencies, including the NCUA and the federal banking agencies, may share information among themselves without waiving any applicable privileges associated with that information and recognized under applicable federal or state law.[2]

FFIEC Rules of Operation also contain guidelines that govern the way in which information may be shared among the Council's members. FFIEC members may, in cases involving specific subsets of information, such as with the Home Mortgage Disclosure Act, enter uniquely drafted Memorandums of Understanding to govern the sharing and use of that information. The Right to Financial Privacy Act also contains an exception that specifically authorizes the exchange of financial records, examination reports, or other information involving regulated financial institutions among and between the member agencies comprising the FFIEC, as well as the Securities and Exchange Commission, Federal Trade Commission, and Commodity Futures Trading Commission.[3]

Additionally, NCUA and the other financial services regulatory agencies are parties to a Memorandum of Understanding through which the agencies may share information pertaining to violations of the Bank Secrecy Act with the with the Financial Crimes Enforcement Network. In response to properly authorized and documented requests, NCUA and the other financial services regulators also share relevant information with other law enforcement agencies.

In terms of practical constraints affecting information sharing, current regulatory reporting requirements are limited in scope to breaches of sensitive consumer information. Financial institutions are not required to report incidents unrelated to those types of breaches. Incidents unrelated to a breach may be captured on a suspicious activity report. However, the number and volume of such incidents can be material should a report be required for each incident.

As noted above, NCUA works with other financial services agencies and the Department of the Treasury to share information internally. In sharing information with agencies outside the financial services regulatory framework or with the public sector, NCUA must balance the need-to-know and the timeliness of critical cybersecurity information with the requirements to provide necessary protections for proprietary financial information.

External sharing remains a challenge due to the sensitive nature of some of the information. This information may be part of a criminal investigation or it could be supervisory in nature, including

[2] See 12 U.S.C. 1821(t) and 12 C.F.R. 792.31.
[3] See 12 U.S.C. 3412(e).

protected proprietary business information or information we cannot easily disconnect from the institution that could reap additional harm to the institution if disclosed. Improvements to current reporting regulations with the ability to develop a discretionary reporting regimen, such as summary versus by incident, may feed additional metrics that could help strengthen overall cybersecurity.

Second, you ask about the coordination between NCUA and the federal banking agencies, the Department of the Treasury, the Department of Homeland Security, and the intelligence community. You also inquire about how legislative proposals would improve or impede interagency coordination and relationships.

We currently participate on working groups aimed at strengthening the flow of intelligence and threat information between agencies. For example, as previously mentioned, NCUA participates in FBIIC as well as additional Department of the Treasury critical infrastructure and cybersecurity venues. We also coordinate and collaborate with law enforcement regarding cyber-attacks on a specific firm or financial institution.

NCUA regularly receives important information and updates from the Department of the Treasury and other agencies, and we make use of that information through either direct communication with our supervised institutions or our subject matter experts and specialized information technology examiners, based on the criticality and sensitivity of the information. NCUA has an ongoing internal assessment process to identify where we can improve our use of intelligence and information to stem the exposure of the credit union system to cyber-attacks, as well as enhance our sharing protocols.

A major focus of the FFIEC's Cybersecurity and Critical Infrastructure Working Group includes promoting greater communication and information sharing among agencies to improve operational awareness across the financial services sector.

Additionally, most of NCUA's supervised credit unions are very small by financial institutions standards. In fact, approximately two-thirds of credit unions hold less than $50 million in assets. These institutions have limited resources and more frequently rely to a greater extent on outsourced relationships for data processing, information security, and network and payment systems management. As a result, third parties play a critical role in credit union cybersecurity preparedness.

However, as noted above, NCUA is the only federal financial institutions regulator without the authority to examine third-party service companies. As highlighted in testimony before the Senate Banking Committee in September, NCUA's top legislative initiative is to gain parity with the other federal regulators.[4] We therefore request that Congress grant similar authority to NCUA that the Federal Deposit Insurance Corporation and the Office of the Comptroller of the Currency possess under the Bank Service Company Act. Such authority is even more important

[4] See pages 15 and 16 at http://www.ncua.gov/News/Press/CL20140916bl/azio.pdf

for NCUA because of the large and growing number of credit unions relying on third parties and a significant number of credit union-specific service companies that are not covered by the Bank Service Company Act.

The enactment of this legislation by Congress would ensure NCUA is able to participate in joint-agency examinations of third-party vendors. By directly examining third-party vendors we can address risk at the source and that will, in turn, reduce the amount of time we spend receiving third-party vendor information indirectly during credit union exams. This will result in a reduced burden on credit unions.

Third, you ask us to share our view of the Financial Stability Oversight Council's role in monitoring cybersecurity risk.

NCUA has a positive view of the Financial Stability Oversight Council's work on cybersecurity. The Council highlighted cybersecurity as a key emerging threat and included recommendations related to cybersecurity in its 2014 annual report. The Financial Stability Oversight Council has also held briefings on cybersecurity issues for the Council's members, as well as discussions within the Council's Systemic Risk Committee and in other venues. The importance placed on this issue by the Council has helped NCUA to raise awareness about cybersecurity threats within the credit union system.

Fourth, you ask us to describe the FFIEC's cybersecurity risk assessment aimed at helping smaller financial institutions to address cybersecurity gaps.

The Cybersecurity and Critical Infrastructure Working Group was chartered to focus on cybersecurity-specific risks in the financial services sector for entities supervised by the FFIEC agencies. The Working Group continues to focus on the central issues of awareness, information sharing and communications, and risk mitigation within the financial services sector.

The Cybersecurity and Critical Infrastructure Working Group conducted a pilot assessment at more than 500 institutions during June and July. The agencies jointly employed a comprehensive cybersecurity framework for the review. The agencies are currently working to assess the results for further consideration and specifically to identify opportunities for:

- Additional awareness training,
- Information sharing and communications,
- Industry guidance,
- Examination procedures, and
- Staff alignment and training.

Information on the pilot assessment can be found on the FFIEC website.[5] The FFIEC agencies also recently issued General Observations from the recently completed pilot cybersecurity assessment. The General Observations can be found on the FFIEC website, as well.[6]

The FFIEC agencies have additionally issued a statement recommending all financial institutions enhance information sharing and knowledge on cybersecurity threats by tapping into the vast resources of the Financial Services Information Sharing and Analysis Center, as well as other federal cybersecurity information sources. This Information Sharing Statement is available on the FFIEC's website.[7]

The assessment is providing valuable insight on how FFIEC agencies can better align expectations with a comprehensive cybersecurity framework. The assessment is under review, and we will focus on opportunities for enhancing cybersecurity in our supervised institutions.

In closing, thank you again for inquiring about our efforts related to and views on the critical issue of cybersecurity. NCUA is committed to addressing cybersecurity threats within the credit union system and to working with Congress and other agencies to further protect the financial services sector from cyber-attacks.

Please do not hesitate to contact me about this or any other issue of interest or concern to you.

Sincerely,

Debbie Matz
Chairman

[5] http://www.ffiec.gov/pdf/cybersecurity/2014_June_FFIEC-Cybersecurity-Assessment-Overview.pdf
[6] http://www.ffiec.gov/press/PDF/FFIEC_Cybersecurity_Assessment_Observations.pdf
[7] http://www.ffiec.gov/press/PDF/FFIEC_Cybersecurity_Statement.pdf

LETTER OF RESPONSE SUBMITTED BY THE BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM
WASHINGTON, D. C. 20551

December 05, 2014

JANET L. YELLEN
CHAIR

The Honorable Tim Johnson
Chairman
Committee on Banking, Housing,
and Urban Affairs
United States Senate
Washington, D.C. 20510

The Honorable Mike Crapo
Ranking Member
Committee on Banking, Housing,
and Urban Affairs
United States Senate
Washington, D.C. 20510

Dear Mr. Chairman and Ranking Member:

Thank you for your letter dated October 21, 2014, inquiring about our role in protecting the financial services sector from cyberattacks. We agree that these events represent a significant risk to the safety of the U.S. financial system and protection of personal financial information.

The Board of Governors of the Federal Reserve System (Board) has long held a strong interest in information security at the financial institutions and financial market utilities (FMU) we supervise, as well as at the technology service providers supporting their activities. Working in conjunction with state and other federal banking regulators, we evaluate the numerous cyberthreats to the banking industry and firms' efforts to address these risks through various routine examination and ongoing monitoring activities. In addition, in 2014, we engaged in several targeted cybersecurity related supervisory initiatives, such as the Federal Financial Institutions Examination Council (FFIEC)[1] cybersecurity assessment of community financial institutions. Our efforts also involve communication and coordination with the law enforcement and intelligence communities, as well as financial industry groups.

[1] The FFIEC members are the Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency, Consumer Financial Protection Bureau, National Credit Union Administration, and the State Liaison Committee.

The Honorable Tim Johnson
The Honorable Mike Crapo
Page Two

Below are responses to your questions that are applicable to the Board.

1. *What is your agency's or Department's process for acquiring information on potential or occurring cyberattacks and passing information to the financial services sector in a timely manner?*

The timely acquisition and sharing of cyberthreat-related information is conducted through a variety of means. The Board engages on an on-going basis with the U.S. Treasury, Department of Homeland Security (DHS), and the Financial Services-Information Sharing and Analysis Center (FS-ISAC), as well as with the law enforcement and intelligence communities to maintain awareness of current threats and vulnerabilities that could have an impact on the financial services sector. The Board also has staff assigned to the Federal Bureau of Investigation's (FBI) Joint Terrorism Task Force (JTTF) to ensure the immediate notification to the Board of threats and vulnerabilities.

The Board encourages institutions to maintain an awareness of cyber developments and obtain threat information directly from the FS-ISAC, DHS, U.S. Computer Emergency Readiness Team, the FBI's InfraGard program and other information sharing forums rather than rely primarily on the Board as the source of this information. The FFIEC member agencies recently issued a joint statement recommending that financial institutions of all sizes participate in the FS-ISAC as part of their process to identify, respond to, and mitigate cybersecurity threats and vulnerabilities. The FFIEC statement advised financial institutions and their critical technology service providers that cyberthreat information provided by the FS-ISAC could improve their ability to identify attack tactics and successfully mitigate cyberattacks on their systems. Additional government resources to assist financial institutions with identifying and responding to cyberattacks were also cited in this statement.

In cases where the Board determines that the nature of a particular cyberthreat warrants heightened awareness, we promptly take steps to convey this information directly to organizations under our supervision. These notifications generally take the form of joint FFIEC statements and alerts issued to the financial services sector. Examiner discussions with management during the course of ongoing supervisory activities is another method used for rapidly sharing cyberthreat intelligence.

As a member of the FFIEC, the Board communicates cybersecurity concepts and supervisory expectations through the FFIEC Information Technology Handbook (IT Handbook), which provides guidance to examiners and management of all financial institutions and technology service providers. The Board also participates in efforts to raise industry awareness on cybersecurity-related issues, for example through webinar presentations delivered to large audiences of financial institutions.

2. *What obstacles and/or legal restrictions hinder information sharing?*

There are no material obstacles or legal restrictions that currently impede the Board's ability to communicate appropriate cybersecurity-related information with financial institutions; however, the financial services sector would benefit from increased information sharing about cyberattacks among its members. Current statute limits the exchange of information solely for the purposes of identifying and reporting activities that may involve terrorist acts or money laundering activities without the risk of incurring civil liability. Creating a safe harbor to facilitate the timely sharing of information concerning other criminal activities, including information about cyberattacks and data breaches, would promote the safety of the U.S. financial system.

3. *Please describe what coordination and interaction each of your agencies and Department have with each other, as well as law enforcement, DHS, and the intelligence community.*

The Board also actively engages with interagency groups such as the Financial and Banking Information Infrastructure Committee (FBIIC), Financial Services Sector Coordinating Council (FSSCC), and the FFIEC's Cybersecurity and Critical Infrastructure Working Group (CCIWG) to share information and collaborate on cyber and critical infrastructure-related issues impacting the financial services sector. The Board participates in classified briefings provided to the FBIIC, which are typically coordinated by the U.S. Treasury Department and conducted by the DHS, FBI and the U.S. Secret Service. The Board works within these groups to develop coordinated messages to the financial services sector on cyber developments, threat intelligence, and ways to improve the sector's ability to mitigate these risks and respond to actual attacks.

4. *How would legislative proposals improve or impede your coordination and relationships with other government agencies?*

The Board would welcome efforts that improve coordination of government agencies on cybersecurity-related matters. While the various sources and processes described above have generally provided an effective means for acquiring cybersecurity information, delays in connection with on-going law enforcement investigations pose an obstacle to obtaining and acting on cyberthreats in a timely manner. These investigations usually require several months or longer to complete, and information related to forensic analysis and attack methodologies is typically not shared in the interim. Given the systemic and rapidly evolving nature of cyberthreats, more immediate disclosure from law enforcement and intelligence communities to appropriate federal banking agencies would enhance our ability to ensure the safety and soundness of the financial services sector and protection of consumers.

5. *Last year, the Financial Stability Oversight Council (FSOC) recommended that regulators devote additional supervisory attention toward cybersecurity. What is the FSOC's role in monitoring cybersecurity risks?*

The FSOC provides an essential forum for communication and coordination of regulatory efforts to address cyberthreats across the financial services sector. Cybersecurity recommendations contained within FSOC's 2014 annual report have contributed to a series of regulatory actions on this topic. The FFIEC and Board cybersecurity assessments described below are in direct response to those recommendations and intended to assess cybersecurity-related vulnerabilities facing regulated entities and identify any gaps in oversight that need to be addressed. Previously cited joint FFIEC statements and alerts issued to the financial services sector are examples of recommended awareness initiatives.

6. *Earlier this year the Federal Financial Institutions Examination Council announced that it is planning cybersecurity and risk-mitigation assessments to help smaller institutions address cybersecurity gaps. Please describe this effort and what particular considerations or risks may exist at institutions of varying sizes.*

During the summer of 2014, FFIEC members conducted cybersecurity assessments at over 500 community financial institutions to evaluate their cybersecurity risk exposure and preparedness. The assessments build upon key aspects of existing supervisory expectations addressed in the FFIEC IT Handbook and other regulatory guidance. Each institution's current practices and overall cybersecurity preparedness were evaluated, with a focus on the following key areas:

- Risk Management and Oversight
- Threat Intelligence and Collaboration
- Cybersecurity Controls
- External Dependency Management
- Cyber Incident Management and Resilience

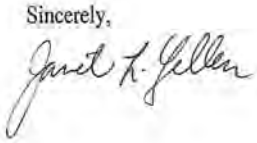
The assessment found that the level of cybersecurity inherent risk varies significantly across the community financial institutions reviewed. Cybersecurity risk management also varies by organization. Analysis of the assessment results are still in process; however, preliminary findings indicate that most community financial institutions have established fundamental cybersecurity controls. Management and board oversight, employee training, prevention and detection systems, and processes to manage third-party relationships are in varying stages of maturation. Based on the assessment results, further enhancements to strengthen cybersecurity at these organizations are warranted and currently under way. FFIEC member agencies are evaluating the effectiveness of cybersecurity-related supervisory programs, guidance and examiner training guidance to

align with current industry conditions and changing cybersecurity risks based on the results of this assessment.

During 2014, the Board also conducted a targeted cybersecurity assessment on a select group of FMU and large financial institutions. The assessment found that these firms, while facing a greater inherent level of cybersecurity risk than community financial institutions, are generally well prepared to address existing cyberthreats. The Board and the other federal banking agencies are actively engaged with the management of these organizations to ensure they maintain an effective state of preparedness against future cyberattacks. Since these organizations operate a significant percentage of the nation's critical financial infrastructure, coordination of the U.S. Government's various efforts aimed at combating cyberthreats should be prioritized to assist these firms in the protection of the financial services sector.

We appreciate your interest in this matter and would welcome the opportunity to be of further assistance.

Sincerely,



LETTER OF RESPONSE SUBMITTED BY THE OFFICE OF THE COMPTROLLER OF THE CURRENCY

Office of the Comptroller of the Currency

Washington, DC 20219

November 21, 2014

The Honorable Tim Johnson
Chairman
Committee on Banking, Housing, and Urban Affairs
United States Senate
Washington, DC 20510-6075

Dear Chairman Johnson:

Thank you for your letter dated October 21, 2014, regarding the role of the Office of the Comptroller of the Currency (OCC) in protecting our financial system from cyber attacks. The OCC has been actively raising the awareness of national banks and federal savings associations (collectively, banks) regarding cyber threats and the need to have appropriate methods for monitoring, sharing, and responding to information about cyber threats and vulnerabilities.

Assessing the resiliency of banks is a key focus of our ongoing supervision programs. In addition, I want to underscore the OCC's strong commitment to working collaboratively with both the government and private sector on cybersecurity. I have stressed repeatedly that effective collaboration is essential due to the interconnectedness and interdependencies both within the financial sector and between the financial sector and other critical infrastructure providers, such as our nation's telecommunications network providers. Indeed, when I became chairman of the Federal Financial Institutions Examination Council (FFIEC) last year, one of my first actions was to call for the creation of the Cybersecurity and Critical Infrastructure Working Group (CCIWG) to help foster and promote such coordination. The CCIWG has been operational since June 2013.

Below are responses to your questions that are applicable to the OCC.

1. *What is your agency's or Department's process for acquiring information on potential or occurring cyber attacks and passing information to the financial services sector in a timely manner?*

The OCC uses information sharing forums, intelligence community relationships, and the supervision process to acquire information on potential or actual cyber threats and attacks. The primary processes by which we obtain information are through:

- Membership in the Financial Services Information Sharing and Analysis Center (FS-ISAC), an industry forum for collaboration on critical security threats facing the global financial services sector.
- Relationships with the law enforcement and intelligence communities, and participation in classified briefings. Additionally, the OCC receives significant alerts through the U.S. Treasury Department that provide information related to cyber threats.
- Ongoing communication by OCC examiners with the banks that they supervise. This includes information related to incidents that may cause significant disruption to systems, facilities, or business processes and attacks and breaches involving sensitive customer information that occur at a bank, its operating subsidiary or affiliate, or at a third-party service provider. Examiners monitor the bank's response to such incidents and assess the level of impact and risk to customers, business operations, and whether there are any systemic or downstream impacts.

The OCC uses formal and informal processes, based on the nature of the threat and the immediacy of potential impact, to communicate information to the banks we supervise. These processes include:

- 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.
- Using our secure BankNet system and coordinating with other regulators for wide-scale distribution of alert or threat information.
- Issuing supervisory alerts or guidance, typically in collaboration with other FFIEC members, that identifies a threat or vulnerability and communicates regulatory expectations or information for addressing the risk. One recent example was the interagency alert on the "Shellshock" vulnerability (http://www.ffiec.gov/press/pr092614.htm).

Cyber threats evolve rapidly, and banks and their critical service providers need to have in place appropriate methods for monitoring, sharing, and responding to threat and vulnerability information to safeguard customer and other sensitive information and technology systems. For this reason, the OCC, along with other FFIEC member agencies, issued the *Cybersecurity Threat and Vulnerability Monitoring and Sharing Statement* on November 3, 2014. The statement reiterated that banks are expected to monitor and maintain sufficient awareness of cybersecurity threat and vulnerability information so they can evaluate risk and respond accordingly. This statement also recommended that banks participate in the FS-ISAC and leverage other resources to obtain threat information on a timely basis. We recognize the critical importance that timely, relevant and actionable information plays in an institution's and the sector's ability to prepare for, respond to, and mitigate the evolving threats.

2. *What obstacles and/or legal restrictions hinder information sharing?*

The OCC believes that the existing statutory framework could be improved to encourage information sharing about cyber attacks among institutions. We believe the enclosed amendment to the USA Patriot Act, which the OCC supports, would do so by creating a safe harbor to

facilitate and promote the timely sharing of information among financial institutions concerning criminal activities, including information about cybersecurity threats, cyber attacks, and data breaches.

3. *Please describe what coordination and interaction each of your agencies and Department have with each other, as well as law enforcement, DHS, and the intelligence community.*

In June 2013, the FFIEC established the CCIWG to enhance communication among its members and build on existing efforts to strengthen the activities of other interagency and private sector groups, such as the FFIEC's Information Technology Subcommittee of the Task Force on Supervision, the Financial and Banking Information Infrastructure Committee (FBIIC), the Financial Services Sector Coordinating Council, and the FS-ISAC. The CCIWG members have been coordinating among themselves and with intelligence, law enforcement, Homeland Security, and industry officials to share accurate and timely threat information, and to assist institutions in protecting themselves and their customers from the growing risk posed by cyber threats. These activities are part of a broader FFIEC cybersecurity awareness initiative that covers institutions of all sizes and complexity. The OCC is also a member of the FBIIC and attends classified briefings organized by Treasury.

4. *How would legislative proposals improve or impede your coordination and relationships with other government agencies?*

We have reviewed a number of legislative proposals 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 Department of Homeland Security, 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 appropriate 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.

5. *Last year, the Financial Stability Oversight Council (FSOC) recommended that regulators devote additional supervisory attention toward cybersecurity. What is the FSOC's role in monitoring cybersecurity risks?*

FSOC provides a mechanism to promote collaborative efforts on cybersecurity issues, and has set forth specific recommendations to advance cybersecurity efforts. For example, in its 2014 annual report, FSOC recommended that Treasury 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 Council 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 to inform and raise awareness of cyber threats and attacks. To help promote private and public sector coordination, last December FSOC members discussed cyber issues and collaborative efforts with the Assistant Secretary for Financial Institutions at Treasury, who chairs the FBIIC, and the Chair of the Financial Services Roundtable BITS Committee Board of Directors.

The FFIEC's CCIWG work is directly responsive to the FSOC's recommendations. A key activity of the working group is to monitor and issue alerts to the industry about emerging threats. Within its first year, this working group released joint statements on the risks associated with "distributed denial of service" attacks, automated teller machine "cash-outs," and the wide-scale "Heartbleed" vulnerability. In September of this year, the group issued an alert to institutions about the "Shellshock" vulnerability, and in November issued a statement encouraging financial institutions to join FS-ISAC to enhance their ability to monitor and respond to emerging threats. These statements and alerts outline the risks associated with the threats and vulnerabilities, the risk mitigation steps that financial institutions are expected to take, and additional resources to help institutions mitigate the risks.

6. *Earlier this year the Federal Financial Institutions Examination Council announced that it is planning cybersecurity and risk-mitigation assessments to help smaller institutions address cybersecurity gaps. Please describe this effort and what particular considerations or risks may exist at institutions of varying sizes.*

The FFIEC is taking a number of steps to provide resources to support banks of all sizes, particularly community institutions that may not have access to the resources available to larger institutions. In May 2014, the FFIEC offered a webinar focused on community banks, entitled "*Executive Leadership of Cybersecurity: What Today's CEOs Need to Know About the Threats They Don't See.*" In June 2014, the FFIEC launched a cybersecurity web page (http://www.ffiec.gov/cybersecurity.htm) that provides links to interagency statements, webinars, and other cybersecurity information that is helpful to financial institutions.

In addition, the FFIEC members recently piloted a cybersecurity assessment examination work program (Cybersecurity Assessment) designed for use by federal and state banking regulators to assess the vulnerability of community institutions to cyber threats and their preparedness to mitigate cyber risks. The Cybersecurity Assessment builds upon key aspects of existing supervisory expectations addressed in the FFIEC IT Handbook (http://ithandbook.ffiec.gov/it-booklets.aspx) and other regulatory guidance. The objectives of the work program are to:

- Assess the complexity of an institution's operating environment, including the types of communication connections and payments initiated, as well as how the institution manages its information technology products and services.

- Assess an institution's current practices and overall cybersecurity preparedness, with a focus on the following key areas:
    - Risk Management and Oversight
    - Threat Intelligence and Collaboration
    - Cybersecurity Controls
    - External Dependency Management
    - Cyber Incident Management and Resilience

On November 3, the FFIEC released general observations from the pilot assessment program (http://www.ffiec.gov/press/PDF/FFIEC_Cybersecurity_Assessment_Observations.pdf). The summary provides an overview of the range of cybersecurity risks that are common to community banks and the risk management practices that banks are using to mitigate those risks. It also offers practical steps that community banks can take to strengthen their cybersecurity preparedness, and questions that bank management and boards of directors can consider to assess their banks' cybersecurity risk management.

The Cybersecurity Assessment will help FFIEC members make risk-informed decisions to identify and prioritize actions to enhance the effectiveness of cybersecurity-related supervisory programs, guidance and examiner training. It will also be beneficial in identifying actions that can strengthen the overall level of preparedness of members and their ability to address evolving and increasing cyber threats.

7. *What particular considerations or risks may exist at institutions of varying sizes?*

The risk of cyber threats and attacks affects institutions of all sizes. Large banks have a worldwide presence, have high public profiles, and therefore are subject to a greater number of attacks. As a result, they need to bring considerable resources to respond to the volume and sophistication of these attacks. Smaller financial institutions generally do not have the same level of resources, which is one reason why the OCC and FFIEC have focused on providing resources and tools that community bankers can use to assess and help mitigate potential vulnerabilities.

A key theme from the Cybersecurity Assessment and recent breaches is the increasing interconnectedness and interdependencies between banks and other parties, including third-party service providers. In a highly interconnected environment, each connection can introduce a potential vulnerability to a cyber attack. This is why the OCC is emphasizing that banks should maintain strong controls over their own systems and how others connect to them. In addition, the OCC is stressing that banks carefully monitor the ways in which they connect to third parties, and how these third parties manage their systems and connect to other third parties. OCC Bulletin 2013-29 *Third-party Relationships: Risk Management Guidance* emphasizes that banks should have strong oversight and processes in place to govern these relationships. The majority of smaller banks tend to rely more heavily on service providers to support their business operations, and the OCC, in coordination with the Federal Deposit Insurance Corporation and the Federal Reserve Board, supervises the largest technology service providers to these institutions.

In summary, the OCC shares your concerns about cybersecurity and we are committed to working closely with the other financial regulators and government agencies, law enforcement, the private sector, and Members of Congress to strengthen the resiliency of our nation's financial sector against such attacks. If you have any further questions about our efforts, please feel free to contact me or Carrie Moore, Director, Congressional Liaison, at (202) 649-6737.

Sincerely,

Thomas J. Curry
Comptroller of the Currency

Enclosure

Suggested Amendment to Section 314 of the USA PATRIOT Act

(31 U.S.C 5311 note)

Section 314 of the USA PATRIOT Act (31 U.S.C 5311 note) is amended—

(1) in subsection (b)—

(A) by striking "terrorist or money laundering activities" and inserting "terrorist or money laundering activities or a specified unlawful activity (as defined in section 1956(c)(7) of Title 18, United States Code) "; and

(B) by striking "terrorist acts or money laundering activities" and inserting "these acts or activities";

(2) in subsection (c) by striking "terrorist acts or money laundering activities" and inserting "terrorist acts or money laundering activities or a specified unlawful activity (as defined in section 1956(c)(7) of Title 18, United States Code) ".

EXPLANATION:

This amendment would facilitate and promote the timely sharing of information concerning criminal activities, among financial institutions, including information concerning cybersecurity threats, cyber attacks, and data breaches. It modifies Section 314(b) and (c) of the USA PATRIOT Act, which provides safe harbors to encourage financial institutions to share information with one another regarding individuals, entities, organizations, and countries suspected of specified unlawful activity, without incurring civil liability. More specifically, the amendment expands these safe harbors, which currently apply to the sharing of information solely for the purposes of identifying and reporting activities that may involve terrorist acts or money laundering activities, to also apply to information sharing for the purposes of identifying and reporting activities that involve the Federal crimes listed in 18 U.S.C. 1956(c)(7). These include crimes relating to computer fraud and abuse, and many other serious offenses. Financial institutions are often unwilling to share information concerning suspected unlawful activity because of the risk of incurring liability. Expanding the safe harbors in this fashion will protect financial institutions that share information with one another, for example, regarding identity theft, cybercrime, and bank fraud, without requiring a determination that the crime also involves money laundering or terrorist activities.

LETTER TO THE CONFERENCE OF STATE BANK SUPERVISORS SUBMITTED BY CHAIRMAN JOHNSON AND SENATOR CRAPO

United States Senate
COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS
WASHINGTON, DC 20510-6075

November 13, 2014

John W. Ryan
President and CEO
Conference of State Bank Supervisors
1129 20th Street, NW, 9th Floor
Washington, DC 20036

Dear Mr. Ryan:

Over the past decade, cybersecurity has become a foremost national priority. Our networks and information systems are under attack from a wide range of actors, including sophisticated criminal organizations, nation-states, and "hacktivists," who commit cyberattacks for a variety of reasons. Cyberattacks come in many different forms, including distributed denial service attacks against websites, point-of-sale attacks against merchants, malware attacks to infiltrate secure systems, phishing scams, and many more.

As Chairman and Ranking Member of the U.S. Senate Committee on Banking, Housing, and Urban Affairs, we are particularly concerned with the safety and integrity of the U.S. financial system, especially as it pertains to Americans' personal financial information. The economic impact of cyberattacks is staggering. A recent Center for Strategic and International Studies report projected global economic losses of up to $575 million annually in the U.S. alone. An earlier report cited by President Obama estimated losses of $1 trillion just from intellectual property theft by cyberattacks over the previous year. Financial institutions are a particularly lucrative target. Many find themselves under constant attack, with some spending up to $250 million per year on cybersecurity.

According to Larry Zelvin, Director of the National Cybersecurity and Communications Integration Center at the Department of Homeland Security (DHS), of the sixteen critical infrastructure sectors, "finance probably wins the cybersecurity threat award. . . . [The industry is] a massive target . . . because [it is] where the money is." The Office of the Comptroller of the Currency recently noted in its Semi-Annual Risk Perspective for U.S banks that cyberattacks and breaches are a leading operational risk and that "recurring security breaches at retail merchants highlight the interdependencies in today's payment systems…there is concern that criminals will transition from disruptive attacks to attacks that are intended to cause destruction and corruption."

Over the past year, we have seen a notable increase in the frequency and scope of data breaches at U.S. companies, which often involve the theft of customers' financial and other personal information. According to a recent study conducted by the Ponemon Institute, 43 percent of companies experienced a breach in the last year, up from 33 percent the prior year, and 60 percent reported a breach in the last two years. These numbers likely underestimate the magnitude of the current threat, as many breaches occur undetected. In the words of former FBI Director Robert Mueller, "There are only two types of companies: those that have been hacked, and those that will be. Even that is merging into one category: those that have been hacked and will be again." Earlier this month, JPMorgan Chase, the nation's largest bank by assets, announced that personal information from 76 million households and 7 million small businesses had been compromised, one of the largest corporate breaches in history. Additional reports indicate that at least a dozen financial companies were targeted by the same hacker group. Ensuring that customer information is secure is essential to the integrity of the financial system.

Furthermore, as new forms of payment become increasingly popular, strong data security will take on even greater importance.

While we recognize that federal and state agencies have heightened their attention to cybersecurity issues, we are writing to seek more information on the role members of the Conference of State Bank Supervisors (CSBS) are playing to protect our financial system from cyberattacks. Please also respond to the following questions:

First, what are CSBS and its members doing to address cybersecurity concerns at the institutions they regulate? What are CSBS and its members' processes for acquiring information on potential or occurring cyberattacks and passing information to the financial services sector in a timely manner? What obstacles and/or legal restrictions hinder information sharing?

Second, please describe what coordination and interaction CSBS and its members have with federal financial agencies, as well as law enforcement, DHS, and the intelligence community. How would legislative proposals improve or impede your coordination and relationships with other government agencies?

Finally, earlier this year the Federal Financial Institutions Examination Council announced that it is planning cybersecurity and risk-mitigation assessments to help smaller institutions address cybersecurity gaps. As members of the FFIEC, please describe this effort and what particular considerations or risks may exist at institutions of varying sizes.

It is vital that government agencies and private institutions remain vigilant and coordinated in ensuring the safety and security of our networks, especially as it applies to the valuable personal and financial information of American consumers.

Thank you for your attention to this matter.

Sincerely,

Tim Johnson

Mike Crapo

LETTER OF RESPONSE SUBMITTED BY THE CONFERENCE OF STATE BANK SUPERVISORS

December 8, 2014

The Honorable Senator Tim Johnson
Chairman
Senate Banking Committee
136 Hart Senate Office Building
Washington, D.C. 20510

The Honorable Mike Crapo
Ranking Member
Senate Banking Committee
239 Dirksen Senate Office Building
Washington, D.C. 20510

Dear Senators Johnson and Crapo:

Thank you for your November 13, 2014 letter regarding the efforts of the Conference of State Bank Supervisors (CSBS)[1] and State Banking Departments in protecting the financial system from cyber attacks. Information technology (IT) has always been a component of bank supervision, and incorporating cybersecurity into supervisory processes has been a natural evolution. As cyber threats have grown in number, scope, and intensity, state regulators have responded with a variety of initiatives.

CSBS applauds the Committee's efforts to focus attention on the role of regulators in promoting cybersecurity. We appreciate the opportunity to provide an overview of state efforts to address cyber risks at our members' regulated institutions and to note measures that would improve state efforts to access and share timely threat information.

Question 1: First, what are CSBS and its members doing to address cybersecurity concerns at the institutions they regulate? What are CSBS and its members' processes for acquiring information on potential or occurring cyberattacks and passing information to the financial services sector in a timely manner? What obstacles and/or legal restrictions hinder information sharing?

State Efforts to Address Cybersecurity at Regulated Institutions

Ensuring that financial institutions are knowledgeable about and properly addressing cybersecurity risks is a high priority for state regulators. Collectively through CSBS and individually, our members are engaged in a variety of cybersecurity efforts. These efforts

[1] CSBS is the nationwide organization of banking regulators from all 50 U.S. states, the District of Columbia, Guam, Puerto Rico, and the U.S. Virgin Islands. For more than a century, CSBS has given state supervisors a national forum to coordinate bank supervision and develop regulatory policy. State banking departments also regulate a variety of non-bank financial services providers. This broad supervisory portfolio provides state regulators with a unique perspective on the range of cyber threats facing the financial system.

1129 20th Street, N.W. • Ninth Floor • Washington, DC • 20036
www.csbs.org • 202-296-2840 • FAX 202-296-1928

encompass both depository and non-depository financial institutions and have focused on raising industry awareness and understanding and on equipping our members and their agencies with the knowledge and tools to supervise for cybersecurity risks.

Raising Industry Awareness

One of CSBS's highest priorities has been to focus bank executive leadership on cybersecurity. To this end, in July 2014 CSBS launched the Executive Leadership on Cybersecurity (ELOC) Initiative. ELOC's goal is to raise awareness among community bank executives and emphasize that cybersecurity is not just a "back office" issue but also an executive and board level issue. To achieve this goal, ELOC provides comprehensive content highlighting today's cybersecurity environment, the impact on the financial system, the importance of CEO and executive level engagement in cybersecurity management, and best practices and efforts to better protect against these threats.

The ELOC Initiative includes tailored content to help bank leadership better engage in cybersecurity management at their bank. The initiative uses diversified methods and platforms to ensure content is meaningfully distributed, including a nine week website campaign, talking points for state bank supervisors, upcoming webinars for commissioners and deputies, and industry outreach events. The ELOC webpage has received thousands of hits,[2] and hundreds of bank CEOs and senior executives have signed up to receive the ELOC Resource Guide[3], illustrating the level of interest in cybersecurity. On December 3, 2014, the Texas Department of Banking, in partnership with several industry groups, kicked off the outreach component of the ELOC initiative with a one day Executive Leadership on Cybersecurity event in Dallas that drew a crowd of over 300 bankers. Deputy Treasury Secretary Sarah Bloom Raskin provided the keynote address and set out a 10-question checklist for bankers focused on cybersecurity awareness and preparedness.[4] We expect similar events to follow in 2015.

While the ELOC initiative is nationwide in scope, several state banking agencies have launched individual initiatives focused on state-specific needs and priorities. In some cases, those initiatives have then been replicated in other states. For example, in 2010, following an increase in cyber theft throughout the state, the Texas Department of Banking partnered with the United States Secret Service Dallas Field Office to form the Texas Bankers Electronic Crimes Task Force. Recognizing the potential financial losses from fraudulent wire and Automated Clearing House (ACH) transactions, the Task Force developed a list of best practices for reducing the risks of Corporate Account Take Over (CATO)[5] attacks and issued minimum standards to Texas

[2] The ELOC Webpage can be found at: http://www.csbs.org/CyberSecurity/Pages/default.aspx.

[3] The Resource Guide is designed for CEOs and executive level leadership so they better understand the cyber security risks facing their institutions and are better prepared to address the risks. The Resource Guide will be available soon.

[4] Deputy Secretary Raskin's remarks can be found at: http://www.treasury.gov/press-center/press-releases/Pages/jl9711.aspx.

[5] A CATO attack occurs when cyber thieves gain access to a computer system, steal confidential banking information, and impersonate the business to send unauthorized wire and ACH transactions to accounts controlled by the thieves. http://www.ectf.dob.texas.gov/aboutcato.htm.

state-chartered banks. Leveraging the benefits of the program, CSBS, the U.S. Secret Service, and the Financial Services – Information Sharing and Analysis Center (FS-ISAC)[6] partnered in 2012[7] to issue these standards and best practices to financial institutions nationwide through industry training, webinars, and CSBS's website[8]. State regulators across the country have disseminated the CATO standards to their institutions.

Similarly, the Kentucky Department of Financial Institutions recently formed a Financial Cybercrime Task Force[9] to identify and address emerging threats facing Kentucky's financial system. The task force focuses on disseminating best practices, guidance, and warnings to the financial services industry. The underlying themes of the task force are educating the industry and monitoring cybersecurity events.

Finally, to better understand cyber risks and challenges, in 2013 the New York Department of Financial Services (DFS) conducted a survey of regulated institutions seeking information about information security frameworks, corporate governance around cybersecurity, and the nature of and cost associated with responding to cyber breaches. Following completion of the survey,[10] New York DFS announced plans to conduct regular cybersecurity preparedness assessments at financial institutions as part of the examination process.

Addressing Cybersecurity through Examiner Training and Supervision

In addition to ensuring bank executives are sensitive to growing cyber threats and engaged in their institutions' cybersecurity efforts, CSBS has taken steps to help state regulators enhance cybersecurity supervision. This effort includes increased information sharing and dialogue among regulators and a focus on identifying and seeking to meet the training needs of state regulators. Since cybersecurity is an operational risk that cuts across several aspects of supervision, CSBS is working to provide state regulators with various levels of training.

CSBS's State Supervisory Processes Committee (SSPC) formed an IT Advisory Group to ensure state banking regulators collaborate, communicate and stay abreast of emerging IT examination issues and threats. This group is comprised of IT examiners from banking departments across the country to discuss field-level information on emerging IT risks, help ensure state supervisory processes are equipped to respond to cyber threats, and discuss training needs. The IT Advisory Group has proven to be a useful forum for ensuring that states share the latest threat and vulnerability data and for helping state regulators keep current on best practices.

---

[6] FS-ISAC is an industry forum for collaboration on critical security threats facing the financial services sector. Their webpage can be found at: https://www.fsisac.com/.

[7] Press Release announcing the partnership is available at: http://www.csbs.org/news/press-releases/pr2012/Pages/pr-120712.aspx.

[8] http://www.csbs.org/ec/cato/Pages/cato.aspx.

[9] http://www.kfi.ky.gov/industry/Pages/cybercrime.aspx.

[10] The New York State Department of Financial Services Report on Cybersecurity in the Banking Sector is available at: http://www.dfs.ny.gov/about/press2014/pr140505_cyber_security.pdf.

In an effort to get a more holistic view of a rapidly changing industry, in 2010, CSBS partnered with the Money Transmitter Regulators Association[11] (MTRA) to bring the combined resources of the two associations to bear both in terms of services offered and technologies used. As "movers" of money facilitated through increasingly complex technologies, money services businesses (MSBs) are especially vulnerable to a broad range of cybersecurity risks. One product of this effort was the 2012 formation of the Multi-State Money Services Businesses Examination Taskforce (MMET) to coordinate and communicate supervisory processes among state regulators. Recognizing the significant cybersecurity threats facing their regulated entities, the MMET is working towards identifying IT and cybersecurity gaps within state supervisory approaches to MSB regulation. MTRA held its annual training event for non-bank examiners in November of this year, which included examiner awareness of cyber threats and data breaches.

The work of MTRA, the MMET, the CSBS IT Advisory Group and general feedback from our members all pointed to a clear need for state supervisors of bank and non-bank entities to have an overview of IT fundamentals. To address this continuing need, CSBS rolled out a pilot IT examiner school in October 2014 focused on examiners with limited to no IT experience. The course is structured to include case studies and practical exercises, and the curriculum covers a broad range of information technology topics including emerging technologies, operations security and risk management, disaster recovery, business continuity, wire transfers, identify theft, bank fraud, corporate account takeovers, third party service providers, and cybersecurity management. Based on the success of this pilot, CSBS expects to conduct multiple sessions in 2015.

Benefits and Risks of Emerging Payments

State regulators have undertaken a number of initiatives to ensure that institutions are aware of the risks associated with technological advancements in financial services. In particular, the rapid pace of payments innovation led CSBS to create an Emerging Payments Task Force (EPTF) earlier this year to assess the implications of changes in the payment system. The CSBS Emerging Payments Task Force (EPTF) is examining various innovations in payments, from proposals for modernizing the traditional payment rails to virtual currencies. As the EPTF looks at the changes across the payments landscape, the importance of institutional cybersecurity and protecting consumer information and assets are key considerations.

The EPTF held a public hearing in May 2014. During that hearing, members of the EPTF discussed cybersecurity with representatives of mobile payments providers. This discussion covered electronic payment systems vulnerabilities fraud as well as industry efforts to develop and implement new security mechanisms such as dynamic Card Verification Values (CVV).[12]

---

[11] MTRA is the professional membership association of state regulators involved in regulating money transmitters and sellers of traveler's checks, money orders, drafts and other money instruments. http://www.mtraweb.org/.

[12] A conventional CVV is a 3-4 digit number of the back of a credit card. Dynamic CVVs change with every transaction, making them significantly more difficult to counterfeit. A transcript for this hearing is available at: http://www.csbs.org/regulatory/ep/Documents/EPTF%20Hearing%20Panel%202.pdf.

The hearing also touched on cybersecurity concerns related to virtual currency activities in light of the recent high profile bitcoin theft from the now infamous Mt. Gox exchange.[13]

Information Sharing

Given the rapidly changing cyber threat environment, CSBS has made obtaining and sharing actionable threat intelligence a priority. CSBS uses information sharing forums, intelligence community relationships and the state supervisory process to acquire information on potential or actual cyber threats and attacks. Then, CSBS distributes information as appropriate to state bank regulators. State bank regulators have both formal and informal processes to communicate information with their supervised institutions.

CSBS receives threat information from a variety sources:

- A principal source for threat information is the Financial Services Information Sharing and Analysis Center[14] (FS-ISAC), which is an industry forum for collaboration on critical security threats facing the financial services sector. FS-ISAC constantly gathers reliable and timely information from financial services providers, commercial security firms, federal, state and local government agencies, law enforcement and other trusted resources. Specifically, the Department of the Treasury (Treasury) and Department of Homeland Security (DHS) rely on the FS-ISAC to disseminate critical information to financial institutions during crises. To support FS-ISAC's mission and role and to improve industry access to timely information, several state banking commissioners, including New York, Massachusetts, and Kentucky, have encouraged their regulated institutions to join FS-ISAC.

- The Financial and Banking Information Infrastructure Committee[15] (FBIIC), under Treasury, is another prime source of cyber threat information. FBIIC, charged with improving communication and coordination among state and federal financial regulators, plays a crucial role identifying critical infrastructure assets, potential vulnerabilities, and prioritizing their importance to the financial system. CSBS participates in classified briefings and maintains secure communications with FBIIC to ensure we receive the latest and most sensitive threat alerts.

- The Federal Financial Institutions Examination Council (FFIEC) Cybersecurity Critical Infrastructure Working Group (CCIWG) has proven to be an invaluable information sharing forum for CSBS and our members. Within its first year, CCWIG has issued several alerts and statements directed towards the industry to outline the risks associated

[13] A transcript of this hearing is available at: http://www.csbs.org/regulatory/ep/Documents/EPTF%20Hearing%20Panel%203.pdf.

[14] FS-ISAC is comprised of financial institutions, insurance companies, publicly held securities/brokerage firms, utilities and privately held stand alone securities firms. The organization gathers information from financial services providers, commercial security firms, federal/national, state and local government agencies, law enforcement and other trusted resources. https://www.fsisac.com.

[15] http://www.fbiic.gov/.

with specific threats and vulnerabilities, the risk mitigation steps that institutions are expected to take, and additional resources to help mitigate the risks. FFIEC alerts to date cover distributed denial of service (DDos)[16] and ATM cash-out attacks[17], and the "Heartbleed"[18] and "Shellshock"[19] vulnerabilities. Additionally, the FFIEC recently issued a statement encouraging financial institutions to join FS-ISAC and outlining expectations for bank management regarding monitoring and maintaining sufficient awareness of cybersecurity threats.[20]

- Finally, through its IT Advisory Group, CSBS has tapped the resources of our members to obtain information related to incidents, attacks and breaches and ongoing supervisory impacts. This collaborative forum has proven to be an excellent venue for states to share information and learn from each other.

Once CSBS learns of potential cyber threats and vulnerabilities, the threats are distilled, analyzed, and prioritized based on the nature of the threat or vulnerability. CSBS has an internal process to ensure that state bank supervisors with a need to know are informed of the latest intelligence through secure channels. The final link in the chain is the process state bank regulators use to share information with their institutions. It is a high priority for state regulators to pass on timely and appropriate threat information to their regulated institutions.

Obstacles/Legal Restrictions to Information Sharing

Access to Classified Information

The classified nature of certain cyber threats can impede the rapid transmission of critical information. To facilitate timely information sharing, it is important that state regulators have a means of obtaining the appropriate security clearances to receive the latest and most critical threat alerts. Currently, state banking commissioners do not have access to the same level of threat information as their federal counterparts. As a result, our members are hampered in their ability to evaluate the seriousness of an emerging cyber threat and whether the threat requires rapid action to inform and protect their regulated entities.

DHS has a formal process for issuing federal government employees and contractors security clearances. However, DHS evaluates state government personnel on a case-by-case basis, which

[16] The FFIEC Joint Statement on DDos attacks is available at: http://www.ffiec.gov/press/PDF/FFIEC%20DDoS%20Joint%20Statement.pdf.

[17] The FFIEC Joint Statement on ATM cash-out attacks is available at: http://www.ffiec.gov/press/PDF/FFIEC%20ATM%20Cash-Out%20Statement.pdf.

[18] The OpenSSL "Heartbleed" Vulnerability Alert is available at: http://www.ffiec.gov/press/PDF/OpenSSLAlert041014.pdf.

[19] The Bourne-Again Shell (Bash) 'Shellshock' Vulnerability Alert is available at: http://www.ffiec.gov/press/PDF/FFIEC_JointStatement_BASH_Shellshock_Vulnerability.pdf.

[20] Cybersecurity Threat and Vulnerability Monitoring and Sharing Statement is available at: http://www.ffiec.gov/press/PDF/FFIEC_Cybersecurity_Statement.pdf.

has proven to be a barrier to state regulators' ability to obtain timely information about cyber threats. Congressional support – through oversight and, potentially, legislation -- for state regulators' efforts to seek a more formalized, streamlined process for state government personnel to receive security clearances could help us address this gap.

Barriers to Incident Reporting

Separately, financial institutions may be wary to report details of breaches and intrusions to avoid incurring legal liability for disclosing consumer personal information. Policy makers should evaluate the allocation of risks in such circumstances to ensure that federal and state laws incentivize, rather than discourage, the appropriate dissemination of credible cyber threats.

Question 2: "Second, please describe what coordination and interaction CSBS and its members have with federal financial agencies, as well as law enforcement, DHS, and the intelligence community. How would legislative proposals improve or impede your coordination and relationships with other government agencies?"

Coordination Efforts

Active coordination between state and federal regulators and law enforcement is essential to mitigating evolving cyber threats. State regulators coordinate through the following fora and with the following law enforcement agencies: the Financial Stability Oversight Council (FSOC), the FFIEC, and U.S. Secret Service and the Federal Bureau of Investigation (FBI).

In response to the financial crisis, Congress created the FSOC to comprehensively monitor and mitigate threats to the financial system as well as ensure greater coordination among financial regulators. Congress affirmed the importance of state regulators in the financial regulatory structure by including a state banking regulator as a non-voting member of the FSOC.[21] Recognizing the threat cyber attacks pose to the stability of our financial system, FSOC held a public meeting in December 2013 where representatives from the public and private sector gave presentations on cyber security.[22] The meeting touched upon the overall importance of a private-public partnership with respect to cybersecurity.

As a voting member of the FFIEC, the State Liaison Committee (SLC) coordinates with other FFIEC member agencies on cybersecurity related supervisory matters. The FFIEC's CCIWG enhances communication among FFIEC members and builds on existing efforts to strengthen the activities of other interagency and private sector groups, such as the FFIEC's Information Technology Subcommittee of the Taskforce on Supervision, FBIIC, Financial Services Sector Coordinating Council (FSSCC)[23] and FS-ISAC. The CCIWG members have been coordinating

[21] 12 U.S.C. § 5321(b)(2)(D). In addition to a state banking regulator, the FSOC includes a state insurance and a state securities regulator as non-voting members.

[22] The minutes from the meeting are available at: http://www.treasury.gov/initiatives/fsoc/council-meetings/Documents/Dececmber%209%202013.pdf.

[23] The Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC), established in 2002, is the sector coordinator for Financial Services for the protection of critical

among themselves and with intelligence, law enforcement, DHS and industry officials to share accurate and timely threat information, and to assist institutions in protecting themselves and their customers from the growing risk posed by cyber threats. These activities are a part of a broader FFIEC cybersecurity awareness initiative.

Furthermore, CSBS's coordination efforts extend beyond regulatory bodies to include law enforcement agencies. As detailed above, CSBS has partnered with the U.S. Secret Service to bring the CATO Initiative to a nationwide platform. CSBS hopes to build off this proven model, and partner with law enforcement agencies in the future to both develop frameworks that are responsive to emerging threats and disseminate the information throughout the industry.

Legislative Proposals

As Congress considers legislative proposals related to cybersecurity, CSBS and its members believe it is important to integrate state regulators into any proposed information sharing or regulatory coordination proposals. State banking commissioners, who charter 75% of all FDIC-insured institutions and have supervisory authority for a diverse array of non-bank financial providers, bring a unique perspective informed by this broader regulatory portfolio and by our members' more locally-focused approach. Building on fora and models such as FFIEC, FSOC, and FBIIC, which institutionalize state participation in regulatory and supervisory bodies, is critical to ensuring states meaningfully participate in decisions that affect the financial sector.

Additionally, CSBS supports legislative initiatives that reduce barriers to the transmission of critical threat information and promote information sharing. As discussed above, Congress should consider legislative solutions to establish a process by which state government personnel can obtain clearances from DHS.

Moreover, financial institutions, both bank and non-bank, should be able to report details of cyber breaches without fear of legal liability. While there is a relatively mature regime regarding breach reporting for banks, liability concerns persist. Moreover, there is not a commensurate legal regime for breaches against non-bank entities. Federal and state laws should incentivize, rather than discourage, the wide dissemination of credible cyber threats experienced by both banks and non-banks.

Question 3: "Earlier this year the FFIEC announced that it is planning cybersecurity and risk-mitigation assessments to help smaller institutions address cybersecurity gaps. As members of the FFIEC please describe this effort and what particular considerations or risks may exist at institutions of varying sizes"

Cybersecurity and Risk-Mitigation Assessments

The FFIEC members recently piloted a cybersecurity assessment examination work program (Cybersecurity Assessment) designed for federal and state regulators to assess the vulnerability

---

infrastructure, focused on operational risks. Their homepage can be found at: http://www.fsscc.org/fsscc/default.jsp.

of community institutions to cyber threats and their preparedness to mitigate cyber risks. The Cybersecurity Assessment builds upon key aspects of existing supervisory expectations addressed in the FFIEC IT Handbook.[24] The objectives of the work program include:

- Assess the complexity of an institution's operating environment, including the types of communication connections and payments initiated, as well as how the institution manages its information technology products and services.
- Assess an institution's current practices and overall cybersecurity preparedness, with a focus on the following key areas:
    - Risk management and oversight
    - Threat intelligence and collaboration
    - Cybersecurity controls
    - External dependency management
    - Cyber incident management and resilience

The FFIEC released general observations from the pilot assessment program on November 3.[25] The summary provides an overview of the range of cybersecurity risks that are common to community banks and the risk management practices that banks are using to mitigate those risks. It also offers practical steps that community banks can take to strengthen their cybersecurity preparedness, and questions that bank management and boards of directors can consider to assess their banks' cybersecurity risk management.

The Cybersecurity Assessment will help FFIEC members enhance the effectiveness of cybersecurity-related supervisory programs, guidance and examiner training. It will also be beneficial in identifying actions that can strengthen the overall level of preparedness of members and their ability to address evolving and increasing cyber threats.

Particular Considerations and Risks at Institutions of Varying Sizes

Cyber attacks are a risk for institutions of all sizes. Large banks have a worldwide presence and high public profiles, and are therefore subject to a greater number of attacks. As a result, they need to expend considerable resources to respond to the volume and sophistication of these attacks. Smaller financial institutions generally do not have the same level of resources, which is one reason why the FFIEC has focused on providing resources and tools for community bankers to assess and mitigate potential vulnerabilities.

A key theme from the Cybersecurity Assessment and recent breaches is the increasing interconnectedness and interdependencies between banks and other parties, including third-party service providers (TSPs). In a highly interconnected environment, each connection can introduce a potential vulnerability to a cyber attack. The Cybersecurity Assessment revealed that smaller institutions tend to rely more heavily on service providers to support their business operations. Thus, FFIEC members have emphasized that banks should carefully monitor the

[24] The FFIEC IT Handbook is available at: http://ithandbook.ffiec.gov/it-booklets.aspx.

[25] The general observations are available at: http://www.ffiec.gov/press/PDF/FFIEC_Cybersecurity_Assessment_Observations.pdf.

connection points between their systems and third parties. Robust supervisory process of TSPs would benefit institutions – particularly community banks – and help improve the resiliency of the financial system.

* * *

CSBS and its members share your concerns on cybersecurity and are committed to working closely with the federal banking and government agencies, law enforcement and the industry to strengthen the resiliency of our financial service sector against cyber attacks. Ensuring state regulators have the appropriate level of security clearance provides an important tool in improving state regulators' ability to coordinate with our federal counterparts and share timely and actionable "need to know" information with our regulated institutions. We welcome Congress's continued focus on cybersecurity and financial system and look forward to working with you and your staff on these issues.

Sincerely,

John W. Ryan
President & CEO

STATEMENT SUBMITTED BY THE NATIONAL ASSOCIATION OF FEDERAL CREDIT UNIONS

NAFCU
3138 10th Street North
Arlington, VA 22201-2149
P: 703.842.2234
F: 703.522.0594
chunt@nafcu.org

Carrie R. Hunt
Senior Vice President of Government Affairs
and General Counsel

National Association of Federal Credit Unions | www.nafcu.org

December 9, 2014

The Honorable Tim Johnson
Chairman
Committee on Banking, Housing
And Urban Affairs
United States Senate
Washington, D.C. 20510

The Honorable Mike Crapo
Ranking Member
Committee on Banking, Housing
and Urban Affairs
United States Senate
Washington, D.C. 20510

Re: Cybersecurity and Data Security

Dear Chairman Johnson and Ranking Member Crapo:

On behalf of the National Association of Federal Credit Unions (NAFCU), the only trade association exclusively representing our nation's federally chartered credit unions, I write in conjunction with tomorrow's hearing, "*Cybersecurity: Enhancing Coordination to Protect the Financial Sector.*" Credit unions serve over 98 million members across the country and we appreciate your interest in fighting against cyber threats in the financial services sector.

In commenting on the importance of cybersecurity just yesterday, National Credit Union Administration Chairman Debbie Matz noted that credit unions will find an active partner with NCUA when it comes to cybersecurity and protecting financial data. While credit unions and other financial institutions have been subject to standards on data security since the passage of the *Gramm-Leach-Bliley Act*, including having federal regulators to oversee and work with them on these standards, retailers and merchants are not held to the same high standards of data security. As Chairman Matz also noted in her comments, "Retailers should be held to the same high data protection standards. It is time to end the double standard." NAFCU agrees and is hopeful that Congress will also take legislative action to address ongoing data security breaches at our nation's retailers.

NAFCU continues to recommend that Congress make the following priorities in any legislation dealing with cybersecurity and data security:

- **Payment of Breach Costs by Breached Entities:** NAFCU asks that credit union expenditures for breaches resulting from card use be reduced. A reasonable and equitable way of addressing this concern would be to require entities to be accountable for costs of data breaches that result on their end, especially when their own negligence is to blame.

- **National Standards for Safekeeping Information:** It is critical that sensitive personal information be safeguarded at all stages of transmission. Under Gramm-Leach-Bliley, credit unions and other financial institutions are required to meet certain criteria for safekeeping consumers' personal information. Unfortunately, there is no comprehensive regulatory structure akin to Gramm-Leach-Bliley that covers retailers, merchants and others who collect and hold sensitive information. NAFCU strongly supports the passage of legislation requiring any entity responsible for the storage of consumer data to meet standards similar to those imposed on financial institutions under the *Gramm-Leach-Bliley Act*.

- **Data Security Policy Disclosure:** Many consumers are unaware of the risks they are exposed to when they provide their personal information. NAFCU believes this problem can be alleviated by simply requiring merchants to post their data security policies at the point of sale if they take sensitive financial data. Such a disclosure requirement would come at little or no cost to the merchant but would provide an important benefit to the public at large.

- **Notification of the Account Servicer:** The account servicer or owner is in the unique position of being able to monitor for suspicious activity and prevent fraudulent transactions before they occur. NAFCU believes that it would make sense to include entities such as financial institutions on the list of those to be informed of any compromised personally identifiable information when associated accounts are involved.

- **Disclosure of Breached Entity:** NAFCU believes that consumers should have the right to know which business entities have been breached. We urge Congress to mandate the disclosure of identities of companies and merchants whose data systems have been violated so consumers are aware of the ones that place their personal information at risk.

- **Enforcement of Prohibition on Data Retention:** NAFCU believes it is imperative to address the violation of existing agreements and law by merchants and retailers who retain payment card information electronically. Many entities do not respect this prohibition and store sensitive personal data in their systems, which can be breached easily in many cases.

- **Burden of Proof in Data Breach Cases:** In line with the responsibility for making consumers whole after they are harmed by a data breach, NAFCU believes that the evidentiary burden of proving a lack of fault should rest with the merchant or retailer who incurred the breach. These parties should have the duty to demonstrate that they took all necessary precautions to guard consumers' personal information but sustained a violation nonetheless. The law is currently vague on this issue, and NAFCU asks that this burden of proof be clarified in statute.

Again, thank you for you interest in enhancing the security of the financial sector and holding this important hearing. NAFCU urges Congress to come together in a bipartisan way and put forward legislative recommendations to hold retailers to the same strict standards of cybersecurity and data security that financial institutions must already adhere to.

On behalf of our nation's credit unions and their 98 million members we thank you for your attention to this important matter. If my staff or I can be of assistance to you, or if you have any questions regarding this issue, please feel free to contact myself, or NAFCU's Vice President of Legislative Affairs, Brad Thaler, at (703) 842-2204.

Sincerely,

Carrie R. Hunt

cc: Members of the Senate Banking Committee

STATEMENT SUBMITTED BY THE SECURITIES INDUSTRY AND FINANCIAL MARKETS ASSOCIATION

December 10, 2014

Statement of the Securities Industry and Financial Markets Association

Senate Committee on Banking, Housing, and Urban Development

Hearing Entitled "Cybersecurity: Enhancing Coordination to Protect the Financial Sector

In today's digital world, both the public and private sectors must improve their ability to defend against a diverse set of cyber threats and be proactive in protecting their partners and clients in addition to their data and networks from theft, disruption or destruction. From criminals seeking financial gain to nation states committing corporate espionage or seeking to dislocate markets and destroy confidence, cyber threat actors are becoming more sophisticated, making cybersecurity an area of risk that must be actively managed by firms similar to other areas of risk. The destruction of financial data or the disruption of our capital markets caused by a successful cyber attack would have a ripple effect across the economy and across the globe. In that light, President Obama has stated that the "cyber threat is one of the most serious economic and national security challenges we face as a nation" and that "America's economic prosperity in the 21st century will depend on cybersecurity." SIFMA[1] and its member firms are leaders in developing and participating in the critical partnership between the government and the financial

[1] The Securities Industry and Financial Markets Association (SIFMA) brings together the shared interests of hundreds of securities firms, banks and asset managers. SIFMA's mission is to support a strong financial industry, investor opportunity, capital formation, job creation and economic growth, while building trust and confidence in the financial markets. SIFMA, with offices in New York and Washington, D.C., is the U.S. regional member of the Global Financial Markets Association (GFMA). For more information, visit http://www.sifma.org.

services industry and appreciate the interest shown by this Committee and others in evaluating our collective efforts.

SIFMA has recently undertaken a five part effort to address cybersecurity threats and related risks to its membership and the financial services industry at large. The ultimate goal of this effort is to better identify the vulnerabilities for a cyber attack, improve the industry's cybersecurity protections and prepare individual firms and the broader sector to respond to a cyber attack, thereby enhancing protections for the capital markets and the millions of Americans who use financial services every day. More than 30 firms from across the industry are engaged in this work to ensure the unique interests and needs of institutions of all shapes and sizes are addressed.

Standards

Effective cybersecurity regulatory guidance is critical both for the financial services sector and the other critical infrastructure sectors we rely on. SIFMA commends the various agencies for conducting a review of their cybersecurity policies, regulations, and guidance and conducting surveys and sweeps of the firms that they cover with the goal of strengthening the defense and response of firms to cyber attacks and better understanding the investments that firms have already made to mitigate this risk. In addition to the reviews being conducted, we suggest via our recently published Principles for Effective Cybersecurity Regulatory Guidance[2] that regulations should be harmonized for greater effectiveness. Industry looks to the government to help identify uniform standards, promote accountability across the entire critical infrastructure, and provide access to essential information. Likewise, government depends upon industry to

[2] Principles for Effective Cybersecurity Regulatory Guidance: http://www.sifma.org/issues/item.aspx?id=8589951691

implement regulation or guidance and collaborate on identifying risks and providing effective solutions. The guiding principles are designed to encourage regulation that facilitates a collaborative relationship and protects the financial industry for the overall security of investors and the nation's economy and SIFMA urges policymakers to consider how best to incorporate the principles into their respective regulatory initiatives.

Improving Resiliency in the Markets

We recently assembled a working group to develop a diagnostic on the U.S. equity and Treasury markets. The working group brought together a broad collection of market participants to identify risks and areas of concern around processes and technology. After mapping process flows within the markets, a workshop was held during which a set of 10 diverse cyber-risk scenarios were applied to the markets and a number of potential risks were identified as a result. These results will be shared with the government and other industry stakeholders in order to jointly identify potential mitigating actions to address the identified risks and further improve equity and treasury market structure.

Incident Response

SIFMA's members refined the industry's crisis incident response plans to ensure that it is well tested and recognizes the appropriate role of our government partners. Building off the after-action reports and lessons learned from the cyber exercise "Quantum Dawn 2" and Superstorm Sandy, SIFMA developed and documented the protocols and process to efficiently create an industry consensus recommendation in response to a systemic incident within the Equity and Fixed Income markets. To enable this process, SIFMA created two new market response committees covering the markets above, which will facilitate the process in the event of a crisis.

On October 24, 2014, SIFMA conducted a test of the process with both committees. Participation from firms, exchanges, financial utilities and regulators was extensive and an after action from the exercise will likely be available at the end of December. This year, SIFMA also launched a multi-faceted approach to engaging the government in order to facilitate a common understanding of how the capital markets will be supported in the event of an attack and what mechanisms and capabilities are available for defending the markets, and in turn investors, while re-establishing public confidence in the recovery.

Insider Threat

Building upon a proactive approach to cybersecurity, SIFMA has developed a set of best practices to assist firms in the development of their own insider threat mitigation programs. This best practices guide provides context, considerations, and a method for implementation of an insider threat program that aligns with the NIST Cybersecurity Framework to facilitate integration into firms' cybersecurity programs and allow synergies to be leveraged as many risks overlap. As we have learned from recent events, the threat of breach and unauthorized disclosure can appear from both external and internal sources and both need to be actively addressed and monitored.

Information Sharing

SIFMA has worked to deepen our members' engagement with the Financial Services Information Sharing and Analysis Center (FS-ISAC) by promoting general membership and participation in its programs. The FS-ISAC is the global financial industry's go-to resource for cyber and physical threat intelligence and a key operational component of the sector's defense. Its role is so central that on November 3, 2014, the Federal Financial Institutions Examination

Council (FFIEC) recommended that financial institutions should join sector-wide information sharing organizations like the FS-ISAC. The FFIEC noted that "participating in information-sharing forums is an important element of an institution's risk management processes and its ability to identify, respond to, and mitigate cybersecurity threats and incidents." In line with this recommendation, SIFMA has funded a one year membership for 181 SIFMA members in the small firm category in order to achieve a near 100% membership overlap with FS-ISAC. In addition to promoting information sharing, we have also sought ways to increase the level of cyber defense and readiness for small firms, by publishing a cybersecurity guidebook informed by best practices at larger institutions and government partners centered on the NIST Cybersecurity Framework. Looking into the future, SIFMA and its members are supportive in both the development and implementation of Soltra Edge, a software solution from DTCC and FS-ISAC that is designed to facilitate the collection of cyber threat intelligence from various sources, convert it into an industry standard language and provide timely information on which users can decide to take action to better protect their company.

Furthermore, there is a need for Congress to engage more productively in this effort to improve our cybersecurity and the best place to start is by the Senate taking up and passing S. 2588, the Cybersecurity Information Sharing Act (CISA) of 2014, which received large bipartisan support in the Senate Intelligence Committee this past July. The threat our economy faces from cyber attacks is real and Congressional action will significantly improve information sharing crucial to improving our cyber defenses. SIFMA believes the Committee has taken a balanced approach which will help the financial services industry to better protect our systems and data and the privacy of our customers. Congress should move swiftly. We cannot wait for the next attack to

legislate, but must remain vigilant and proactive and provide the private sector with laws that will enable us to better protect ourselves and collaborate with our government partners.

Conclusion

Neither the industry nor the government can prevent or prepare for cyber threats on their own. SIFMA believes that a dynamic and collaborative partnership between the industry and government is the most effective path forward to accomplishing this goal. Among other areas for collaboration, government participation in industry exercises is critical to gain a better understanding of our collective capabilities in the event of a crisis. For Quantum Dawn 3 (QD3), we are currently planning for a major industry-wide exercise in September 2015. QD3 will build upon the breadth and success of QD2 and continue to focus on an attack on the US equity market that has a systemic impact. The exercise will include participants from the public and private sector and focus on how we collaborate during a crisis to maintain operations in the face of a destructive data attack.

Another area where collaboration is critically important surrounds efforts to enhance regulatory harmonization beyond existing requirements to improve the protection of the financial sector. The benefits of this partnership approach led to the development of the NIST Cybersecurity Framework, which SIFMA is actively promoting within its membership and encourages regulators to use as a universal structure that can be leveraged as a starting point for creating a unified approach to cybersecurity.

As an industry, we have made cybersecurity a top priority. SIFMA has brought together experts from across the public and private sectors to better understand the risks involved in a cyber attack and develop best practices to be better prepared to thwart an attack, but to be effective, we

must work closely with the federal government to strengthen our partnership, protect our economy and the millions of Americans who place their confidence in the financial markets each and every day.

###

STATEMENT SUBMITTED BY THE INDEPENDENT COMMUNITY BANKERS OF AMERICA

December 10, 2014

Cybersecurity: The Community Bank Perspective

On behalf of the more than 6,500 community banks represented by the Independent Community Bankers of America (ICBA), thank you for convening today's hearing "Cybersecurity: Enhancing Coordination to Protect the Financial Sector." We welcome the opportunity to share the community bank perspective on this critical, dynamic issue.

The financial services industry and community banks are on the front lines of defending against cybersecurity threats and take their role in securing data and personal information very seriously. Community banks are strong guardians of the security and confidentiality of customer information as a matter of good business practice as well as legal and regulatory requirements. Safeguarding customer information is central to maintaining public trust and the key to long-term customer retention. As Congress, law enforcement and the regulatory agencies continue to address the real and present danger cybercriminals pose to the financial system, we ask that they keep in mind the following policy principles and objectives of the community banking industry:

Policymakers Must Recognize Existing Data Security Mandates and Close Remaining Gaps. Any new legislation, frameworks, or standards policymakers develop should first recognize the existing standards and practices community banks observe to protect the confidentiality and integrity of customer personal data as well as to mitigate cyber threats and then focus on closing remaining gaps. The National Institute for Standards and Technology (NIST) framework, for example, and the 2013 Executive Order implementing it, were developed to create a baseline to reduce cyber risk to all critical infrastructure sectors, and the Gramm-Leach-Bliley Act, sets forth rigorous and effective data security protocols for the financial sector. It is important to extend comparable standards to ALL critical infrastructure sectors, including the commercial facilities sector which incorporates the retail industry and other potentially vulnerable entities.

Threat Information Sharing is Critical. ICBA supports the sharing of advanced threat and attack data between federal agencies and the appropriate financial sector participants, including community banks. Community banks rely on this critical information to help them manage their cyber threats and protect their systems. ICBA supports community banks' involvement with services such as the Financial Services Information Sharing and Analysis Center (FS-ISAC). The FS-ISAC is a non-profit, information-sharing forum established by financial services industry participants to facilitate the public and private sectors' sharing of physical and cybersecurity threat and vulnerability information. ICBA also supports FS-ISAC efforts to take complex threat information across communities, people and devices and analyze, prioritize, and route it to users in real-time as long as those efforts incorporate community banks and such advancements are cost effective for them.

Additionally, ICBA supports the recent creation of the Retail Cyber Intelligence Sharing Center (R-CISC) and supports the establishment of robust information sharing protocols between the two sector ISACs.

Regulators Should Do More to Control Third Party Risk. Community banks significantly rely on third parties, such as data processing companies and software vendors, to support their systems and business activities. While community banks are diligent in their management of third parties, mitigating sophisticated cyber threats to these third parties, especially when they have connections to other institutions and servicers, can be challenging. Regulators should enhance their oversight of these third parties in order to mitigate the risks associated with interconnectivity and share threat and other applicable information with community banks on a timely basis.

ICBA Position on Recent Data Breaches

Community bankers and their customers are deeply alarmed by the wide-scale data breaches at national retail chains and other entities. These far-reaching and costly breaches have the potential to jeopardize consumers' financial integrity and confidence in the payments system.

To mitigate this risk, ICBA calls on policymakers to consider the following:

The Party that Incurs a Breach Should be Liable for Associated Costs. It is critical that the party that incurs a data breach, whether it be a retailer, financial institution, data processor or other entity, bear responsibility for the related fraud losses and costs of mitigation. Allocating financial responsibility with the party that is best positioned to secure consumer data will provide a strong incentive for it to do so effectively. Additionally, aligning incentives to maximize data security by all parties that process and/or store consumer data will make the payments system stronger over time. Payments rules should mandate merchant security provisions to further protect customer data, particularly debit and credit card information.

Extend Gramm-Leach-Bliley Act-Like Standards. Under current law, retailers and other parties that process or store consumer financial data are not subject to the same federal data security standards and oversight as financial institutions. Securing financial data at financial institutions is of limited value if it remains exposed at the point-of-sale and other processing points. ICBA supports subjecting these entities to Gramm-Leach-Bliley Act-like standards with similar enforcement. It is equally important that these entities provide uniform and timely notification to banks concerning the nature and scope of any breach when bank customer information may have been compromised.

A National Data Security Breach and Notification Standard is Vital. Most states have enacted laws with differing requirements for protecting customer information and giving notice in the event of a data breach. This patchwork of state laws only increases burdens and costs, fosters confusion, and ultimately is detrimental to customers. ICBA believes customer notification is appropriate to let customers take steps to protect themselves from identity theft or fraud resulting from data breaches. However, it is important that notification requirements allow financial institutions and others flexibility to determine when notice is appropriate. Overly broad notification requirements defeat the purpose of calling attention to the risks associated with a particular breach. Federal banking agencies should set the standard for financial institutions, as they currently do.

Thank you again for the opportunity to submit this statement for the record. ICBA is committed to working with this committee to address cyber threats and data breaches brought by criminal enterprises.

"PROTECTING MERCHANT POINT OF SALE SYSTEMS DURING THE HOLIDAY SEASON"

FINANCIAL SERVICES ISAC

R-CISC

Protecting Merchant Point of Sale Systems during the Holiday Season

November 7, 2014

Executive Summary

This advisory was prepared in collaboration with the Financial Services Information Sharing and Analysis Center (FS-ISAC), the United States Secret Service (USSS), and the Retail Cyber Intelligence Sharing Center (R-CISC), and is directed towards retailers or companies which are processing financial transactions and managing customer personally identifiable information (PII) during the upcoming holiday season and beyond. This advisory serves to provide information on and recommends possible mitigations for common cyber exploitation tactics, techniques and procedures (TTPs) consistently and successfully leveraged by attackers in the past year. Many of these TTPs have been observed by the FS-ISAC, through its members, and identified in Secret Service investigations.

The TTPs discussed in this report include:

- Exploiting commercial application vulnerabilities
- Unauthorized access via remote access
- Email phishing
- Unsafe web browsing from computer systems used to collect, process, store or transmit customer information

This document provides recommended security controls in these four commonly observed areas to protect customer data and also provides recommendations to smaller merchants who should work with their vendors to implement these recommendations (see Appendix A).

This advisory is not intended to be a robust, all-inclusive list of procedures as attackers will modify TTPs depending upon the target's network and vulnerabilities. This report does not contain detailed information about memory scraping Point of Sale (PoS) malware that has been used in recent high-profile data breaches. Secret Service investigations of many of the recent PoS data breaches have identified customized malware only being used once per target. A list of observed PoS malware families is provided in Appendix B.

These recommendations should be analyzed by cyber threat analysis and fraud investigation teams based on their operational requirements. The information contained in this advisory does not augment, replace or supersede requirements in the Payment Card Industry Data Security Standard (PCI DSS); however, the PCI DSS version 3.0 recommendations are cited when appropriate.[1]

[1] For the full PCI DSS v. 3.0 guide please see https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf

Table of Contents

Executive Summary 1
Application Security 3
Recommendations 3
Remote Access Controls 3
Recommendations 4
Third Party Vendors 4
Recommendations 5
PoS Management 5
Recommendations 6
Points of Contact 7
Appendix A. Simple Network Controls for Small Merchants to Protect Customer Data 9
Appendix B. List of Common PoS Malware Family Names 12
Appendix C. Multi-Factor Authentication 14
Enable Two-Factor Authentication 14
Configuring Two-Factor Authentication 14
Two-Factor Authentication Tokens authentication methods for XenApp Web Sites 17

Application Security

During the past year attackers have continued to use brute force password attacks against network assets such as webservers or externally facing databases. According to a 2013 survey conducted by the security firm Alert Logic, brute force attacks increased from 30 to 44 percent among its customers.[2]

Once inside a network, hackers usually map the network to determine the most valuable data to steal. One method of connecting to the network devices storing that data is through software that is permitted to run on the network and connect to external destinations controlled by the hacker. Typically, these applications are allowed full outbound access through a firewall or proxy service facilitating the theft of that data.

There is a strong possibility that attackers will leverage highly publicized vulnerabilities such as Heartbleed, Shellshock (Bash), and POODLE to access a network.

Recommendations

- Perform Open Web Application Security Project (OWASP) audits on any web applications.[3]
- Implement all recommended vendor patches and test to ensure the patch is successfully integrated.
- Enforce up-to-date anti-virus (AV) signatures, but do not only rely on AV signatures alone.
- Test databases and web login portals against brute force password attacks.
- Monitor firewalls for outbound traffic to unknown or suspicious IP addresses and domains.
- Secure webservers that contain customer data. These include payment gateways and e-commerce applications.
- Ensure that no unauthorized code has been introduced to the production environment. Run a vulnerability scan against your approved applications. If any software is vulnerable, update and patch immediately. Re-run the vulnerability scan whenever new or updated applications are introduced.

Remote Access Controls

Criminals have successfully exploited databases and payment processing systems with remote access tools. There is a high probability that employees who have remote access to the company's network will be targeted especially if the attacker can steal virtual private network (VPN) logon credentials and leverage them to log in during normal business hours. For example, in August 2014, a health care provider's VPN credentials were stolen and hackers used these credentials to steal millions of patient's social security numbers.[4]

---

[2] http://go.alertlogic.com/rs/alertlogic1/images/alert-logic-spring-2014-CSR-pages-04-21-14.pdf?mkt_tok=3RkMMJWWfF9wsRolvKrKZKXonjHpfsX86OkuWqeg38431UFwdcjKPmjr1YAESMt0aPyQAgobGpSI5FEKSbnYRqJ4t6EOUg%3D%3D

[3] https://www.owasp.org/index.php/SQL_Injection

[4] http://www.reuters.com/article/2014/08/20/us-community-health-cybersecurity-idUSKBN0GK0H420140820

Implementing multi-factor authentication on remote access devices reduces the risk of attackers gaining access to the network. Too often, this added layer of security is not configured in remote access platforms, making it a common target for attackers in past data breaches. Appendix C contains examples for enabling and configuring multi-factor authentication for the popular and widely deployed Citrix platform XenApp. Most other remote access platforms provide similar support for multi-factor authentication.

Recommendations

- Corporate users who typically access a network externally should be forced to change their login credentials before and after the holiday season. Sophisticated criminal groups have likely already purchased stolen credentials to conduct an attack this season. Forcing regular password changes and enforcing complex password rules will help mitigate this risk.
- Multi-factor authentication should be required to mitigate risk for remote access. Many remote access appliances are provisioned to accept multi-factor authentication technology (See Appendix C).
- Segregate the payment processing systems from remote access applications when possible, and restrict the network resources remote access users can access.
- Implement all recommended vendor patches and test to ensure the patch is successfully integrated.
- Enforce up-to-date AV signatures, but do not only rely on AV signatures alone. Consider additional tools for the device being accessed such a host based intrusion prevention system (HIPS) and host based firewalls.
- Monitor the remote user accounts for login abnormalities such as frequent failed login attempts, logins during non-normal working hours, and abnormal duration of logon (e.g. very long or very short login sessions). Additionally, host based security logs should be enabled and reviewed.
- Lock accounts after multiple failed login attempts. The industry standard is not more than six failed login attempts.[5]
- Disable un-necessary services especially those that support remote access such as remote desktop protocol (RDP) and virtual network computing (VNC) when not required.
- Monitor firewalls for outbound traffic to suspicious IP addresses and domains.

Third Party Vendors

There is a strong possibility that third party vendors such as those involved in heating ventilation and air conditioning (HVAC), power, or other environmental and physical security controls on the network will be targeted. These vendors usually have login access to a central network or peripheral network that can be exploited to gain lateral access for payment information.[6] In December 2012, the cyber security firm Cylance stated that it found 12,000 US industrial control systems online indicating they can be

[5] https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf
[6] http://arstechnica.com/security/2012/12/intruders-hack-industrial-control-system-using-backdoor-exploit/

accessed externally and potentially targeted by an attacker.[7] The following May, Cylance researchers demonstrated vulnerabilities in an HVAC platform and successfully shut down a major technology company's air conditioning.[8]

Recommendations

- Vendors should not be allowed to remote access your network with out of date operating systems like Windows XP. For example, require Windows 7 or newer, or Mac OS 10.8.
- Identify third parties with remote access or physical access to the network perimeter.
- Require vendors to use multi-factor authentication for remote access when possible. If multi-factor authentication is not available to those vendors, then disable remote access services except when specifically requested and scheduled by the vendor. Force third parties to change their login credentials before and after the holiday season. Sophisticated criminal groups have likely already purchased stolen credentials to conduct an attack this season. Forcing regular password changes and enforcing complex password rules will help mitigate this risk.
- Enforce up-to-date AV signatures, but do not only rely on AV signatures alone.
- Establish baselines for each 3rd party vendor's normal network activity, including remote access and logins. Monitor their activity for anomalous behavior such as frequent failed login attempts, logins during non-normal working hours, and abnormal duration of logon.
- Evaluate and limit third party network access privileges. For example, whitelist third party network addresses on a firewall provisioned to control remote access by third parties.
- Segment the network if possible through the use of secured VPNs with managed access control.
- Conduct information security and risk assessments of all third party vendors that have access to your network.

PoS Management

In preparing for the holiday season, remember, the computers that run the PoS services must be secured like any other computer on your network. In a recent incident, investigated by Wapack Labs, the CEO of a small company used his company computer to surf the web. In doing so, a website containing spyware was accessed and the spyware was downloaded on the system. Unfortunately, the spyware downloaded the ZeuS crimeware and installed a serious piece of ransomware known as Cryptolocker. It cost the company $600 in ransom (paid in Bitcoin) plus $3,800 in forensic and cleanup fees. Every file on his laptop was encrypted, and when he connected to the corporate network, every one of his mapped drives were encrypted –including financials --all because he surfed the web from his company laptop.

During low volume hours, cashiers, clerks, and seasonal workers may find fun things to do on the web. Imagine if the attack described above occurred on a computer used to process payments or manage

[7] http://www.mocana.com/blog/2012/12/19/niagara-ax-framework-hack-more-serious-than-first-thought
[8] http://www.wired.com/2013/05/googles-control-system-hacked/

customer personally identifiable information (PII). How much more damaging and costly would that attack have been?

Recommendations

Overall

- Inventory and conduct a review of how customer data is stored, moved, and deleted. This should include the equipment and applications involved. It is likely that a sophisticated attacker will conduct reconnaissance on a target's network to identify where customer data is stored and how it is transmitted locally before being encrypted in a central database.

On the Network

- Ensure that your PoS systems have a firewall or proxy installed for protection.
- Deploy an appropriately configured intrusion prevention system (IPS).
- Employ proper network segmentation, such that PoS systems operate on a separate, protected subnet.
- All VPN access should be performed through the IPS and must use up-to-date authentication mechanisms.
- Segregate your PoS system from other network functions such as email and non-PoS related applications. If the PoS is attached to enterprise resource planning (ERP), inventory, or finance systems, use application gateways to ensure the PoS functionality is logically protected.
- Do not use PoS terminals or other computers with access to PoS systems for Internet surfing, checking email, or accessing social media.

Encryption

- Confirm what data is at rest on a PoS terminal and deploy endpoint encryption for those devices.
- Encrypting Card and PIN information before going into the payment terminal memory has been an effective technique to safeguard the payment data. There are several vendors who provide this technology and service.
- Some retailers have elected to replace their in store payment terminals with new technology to encrypt card account numbers and other track data as it is swiped in the mag stripe reader or read by the chip reader.

[**NOTE:** If the criminals capture the encrypted data it is typically not marketable in the criminal underground]

Internet Access and Software Updates

- If the PoS is processed by software operating on a single terminal consider not allowing that terminal Internet access, or restricting its internet access to only those destinations required for PoS functions (e.g. payment gateways).
- Consider requiring two or more employees approve any updates of the payment processing applications and, if possible, filter updates to that terminal's operating system (OS) though a controlled server on the network.

Physical Access and Multi-Factor Authentication

- Ensure that there are no active USB ports or other media drives open on a PoS terminal. If running a Windows OS, ensure that auto-run is disabled. Insider threats, both intentional and unintentional, are a real danger.
- Inform employees to be on the lookout for skimmers, USB sticks, or other devices connected to PoS systems. Check all PoS systems, including card swipe equipment, for connected devices on a regular basis (e.g. daily).
- Implement multi-factor authentication for the employees involved in managing the transactions of customer data and updating the applications protecting those transactions (See Appendix C).

White Listing

- If transactions are processed by a single software program operating on a single terminal, ensure that only that application is allowed to run on that terminal by enforcing a strict application white listing policy. If possible, log and configure alert updates for the security operations center for any changes made to that whitelisting policy by an individual user or business location.
- Record and change the default settings with any PoS hardware and software, including default passwords. Criminal groups have likely reviewed documentation and/or purchased the same software in order to exploit any default settings.

Anti-Virus and Key Logging

- Do not rely on AV signatures to find memory scraping malware. Criminals have customized this type of malware in recent attacks and likely tested this against the target network's AV solution.
- Implement anti-malware detection software that looks for anomalous and suspicious patterns of behavior.
- Enforce up-to-date anti-virus signatures to find older malware that is being reused. This may be targeted at smaller or medium sized businesses or used by criminal elements with less resources and time. For a list of recently observed PoS malware families please see Appendix B.
- Implement software to detect key-loggers on PoS terminals.
- If possible, deploy a host based intrusion prevention system (HIPS).

Points of Contact

For law enforcement assistance, please contact your local U.S. Secret Service Field Office/Electronic Crimes Task Force (ECTF) or the USSS toll free number at (877) 242-3375. The U.S. Secret Service has taken a lead role in mitigating the threat of financial crimes since the agency's inception in 1865. As technology has evolved, the scope of the U.S. Secret Service's mission has expanded from its original counterfeit currency investigations to also include emerging financial, electronic and cyber-crimes. As a component agency within the U.S. Department of Homeland Security, the U.S. Secret Service has established successful partnerships in both the law enforcement and business communities – across the country and around the world – in order to effectively combat financial crimes.

The FS-ISAC encourages member institutions to report any observed fraudulent activity through the FSISAC submission process and login at http://www.fsisac.com/. This reporting can be done with attribution or anonymously and will assist other members and their customer to prevent, detect and respond to similar activity. Non-members experiencing suspicious activity are encouraged to reach out to the FS-ISAC SOC at soc@fsisac.us or to call (877) 612-2622 – prompt 2.

Appendix A. Simple Network Controls for Small Merchants to Protect Customer Data

[NOTE: If you outsource your PoS solution, please work with your PoS or payment processor vendor to ensure that the following controls are implemented]

- Reset default passwords for vendor supplied equipment.
- Require regular password changes (at least every 90 days) and change all passwords before and after the holiday season.[9]
- Enforce strong passwords (e.g. at least seven characters in length with both numeric and alphabetic characters).[10]
- Inform employees to be on the lookout for skimmers, USB sticks, or other devices connected to PoS systems. Check all PoS systems for connected devices on a regular basis (daily is recommended), especially ahead of the holiday season.
- Segregate your PoS system from other computers on the network. Do not use PoS terminals for Internet surfing, checking email, or accessing social media.
    - If a PoS terminal must be used for legitimate non-PoS functions, implement a commercial or open source web protection tool on the PoS terminal to limit access to harmful and inappropriate websites
- If PoS services operate on an older operating system, update them immediately and configure auto-updates.
- Update all AV signatures and software on a PoS terminal daily.
- Implement multi-factor authentication for all remote access operations.
- Implement a unified threat management (UTM) device.
    - This is a device that "allows an administrator to monitor and manage a wide variety of security-related applications and infrastructure components through a single management console."[11] This simplifies the cyber security management process for any small and medium size business owner.
    - UTMs "are typically purchased as cloud services or network appliances, provide firewall, intrusion detection, antimalware, spam and content filtering and VPN capabilities in one integrated package that can be installed and updated easily."[12]
- If possible, hire an independent third party to assess your security needs.[13] After this inspection, consider hiring a monthly managed security service provider (MSSP) to manage based on the inspection results. MSSPs are out sourced services that manage network defenses such as firewalls and can typically be hired inexpensively. Below is a list of questions that the SANS cyber research institute has published for businesses evaluating a potential MSSP.[14]

---

[9] https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf
[10] Ibid.
[11] http://searchmidmarketsecurity.techtarget.com/definition/unified-threat-management
[12] Ibid.
[13] http://www.darkreading.com/risk/how-to-pick-the-best-mssp-for-your-smb/d/d-id/1138968?
[14] Ibid.

MSSP Evaluation Questions[15]

Business managers should consider the following questions before deciding to hire an MSSP.

- Does the service provider offer an assortment of solutions that can readily address a variety of environments or do they specialize in a one size fits all solution?
  - No service provider can be in expert in all possible solutions. They should, however, be able to offer a choice of products that can complement each other and provide a solution that offers an optimal amount of protection. [16]

- Do not overlook physical security. How secure is the facility from which the service is being provided?
  - Does the service provider utilize proper access controls and is access to management consoles provided only to those who need it.[17]

- What provisions are in place with respect to fault tolerance? How often are the security devices being polled and what process is in place for notification should a problem occur?
  - While a device may appear to be "up," any number of problems could arise. Is logging being checked periodically and how? Are critical processes that run on the sensor being monitored to determine if they are functioning properly? What about routine maintenance of the device such as checking for disk space? Is there a centralized log server in the event that the security device, itself, is compromised? How much activity is kept, that is, how far back is logging maintained? If a compromise is discovered well after the fact, can accurate data be pulled to help in the investigation?[18]

- Does the service provider have out-of-band access to managed devices?
  - Is there built-in redundancy or is the provider "blinded" and unable to access devices and receive alarms? If you run a high-profile site this is a potential point of attack.[19]

- Does the company specialize in security or is it merely and add-on to an existing business?

- How does the MSSP handle staff turnover? Are passwords routinely changed and do they utilize common passwords across multiple devices? Do they perform background checks on prospective employees and are they bonded?[20]

- What emphasis if any does the provider place on certifications?
  - While certifications do not in and of themselves guarantee expertise, they do provide a means of determining the level of knowledge that the staff has regarding intrusion detection. Look for non-vendor specific certifications, as well as vendor-specific certifications.[21]

---

[15] http://www.sans.org/security-resources/idfaq/mssp.php
[16] Ibid.
[17] Ibid.
[18] Ibid.
[19] Ibid.
[20] Ibid.
[21] Ibid.

- To what extent does the service provider provide continuing education or training for staff members?
    - Intrusion detection is a field that is rapidly advancing. The service provider should be able to readily address and provide information regarding new exploits. Part of the benefit of out-sourcing intrusion detection is that the service provider should be able to provide up-to-date information that would be beneficial in addressing new threats. By providing a proactive approach rather merely reactive, they can more readily determine "patterns of activity" that could pose a threat to an enterprise ahead of time.[22]

- Is the service provider capable of writing custom signatures that can address "zero-day exploits" or are they limited to the signature that are provided by the manufacturer of the intrusion detection system. What assurance is there that the devices that are being maintained are continually updated with the latest signatures?
    - An intrusion detection system that is not updated is comparable to virus protection software that is out of date. It can provide a false sense of security that can fail when it is needed the most.[23]

[22] Ibid.
[23] Ibid.

FINANCIAL SERVICES ISAC

R-CISC

Appendix B. List of Common PoS Malware Family Names

Table 1 contains a list of common PoS malware family names that have been used in the past. Sophisticated criminals will likely continue to use malware from one or more of these families, after testing a target's AV solution against their samples to evade detection.

[**NOTE:** Sophisticated criminals can make minor changes to existing families of malware, making it undetectable by signature-based AV solutions.]

Table 1. List of Common PoS Malware Family Names

Family Name	Description
Alina[24]	A family of PoS malware that targets applications containing Track data, applies basic encryption and exfiltrates the information. This malware has a command & control structure, which allows it to search for and install automatic updates when they are released.
Backoff PoS[25]	These variations have been seen as far back as October 2013 and continue to operate as of July 2014. In total, the malware typically consists of the following four capabilities. An exception is the earliest witnessed variant (1.4) which does not include keylogging functionality. Additionally, 1.55 'net' removed the explorer.exe injection component: • Scraping memory for track data • Logging keystrokes • Command & control (C2) communication • Injecting malicious stub into explorer.exe
BlackPoS/Kaptoxa[26]	BlackPOS infects computers running Windows that are part of PoS systems and have card readers attached to them. These computers are either infected by insiders or found during automated Internet scans because they have unpatched vulnerabilities in the operating system or use weak remote administration credentials. Once installed on a PoS system, the malware identifies the running process associated with the credit card reader and steals payment card Track 1 and Track 2 data from its memory. BlackPoS is a RAM scraper, or memory-parsing software, which grabs encrypted data by capturing it when it travels through the live memory of a computer, where it appears in plain text. The captured information is uploaded to a remote server via File Transfer Protocol (FTP).
Chewbacca[27]	Chewbacca appears to have been a short-lived malware designed to attack PoS systems and exfiltrate data over TOR. The malware itself has been well documented.
Decebal[28]	Romanian PoS malware released on January 3, 2014. It is written in Visual Basic Script and is capable of checking to see if the computer on which it's deployed is running any sandboxing or reverse engineering software. Decebal can also validate that the stolen payment card numbers are legitimate.

[24] https://www.hacksurfer.com/special-report-point-of-sale-malware.pdf
[25] https://www.us-cert.gov/ncas/alerts/TA14-212A
[26] https://www.hacksurfer.com/special-report-point-of-sale-malware.pdf.
[27] http://pages.arbornetworks.com/rs/arbor/images/Uncovering_PoS_Malware.pdf
[28] https://www.hacksurfer.com/special-report-point-of-sale-malware.pdf.

Dexter[29]	First discovered in December 2012, Dexter is a custom made malware tool used to infect point of sale systems. According to Seculert, Dexter steals the process list from the infected machine, while parsing memory dumps of specific POS software related processes, looking for Track 1 / Track 2 credit card data.
JackPoS[30]	JackPoS was likely first developed in October 2014 and developed through early 2014.[31] There are at least thirty three distinct malware samples of JackPoS in this timeframe.[32] Some indicators suggest that JackPoS has evolved from, or was inspired by the Alina PoS malware.[33] JackPoS is distributed by cybercriminals through drive-by attacks.[34] The malware is sometimes disguised as the Java Update Scheduler.[35] "Several of the found loaders used in detected 'Drive-by' download attack are written using obfuscated compiled AutoIt script, which became quite popular method to avoid AV detection in order to unpack additional binary malicious code and execute further instructions received from the command and control server."[36] "The bad actors have used some sophisticated scanning, loading, and propagating techniques to attack these vectors to look to get into the merchants system thru external perimeters and then move to card processing areas, which were possibly not separated in compliance with PCI polices."[37]
PoSCard Stealer[38]	PoSCardStealer is a name used by ESET, which appears to cover several types of PoS malware. Where the malware doesn't have another name known to ASERT, we will use "PoSCardStealer". Other anti-malware vendors use different naming schemes such as Troj/Trackr-K.
vSkimmer[39]	vSkimmer was disclosed by McAfee in March 2013. vSkimmer searches program memory for track data; however, it only looks for data matching Track 2 format. In addition to using HTTP to exfiltrate stolen data to a C2 server, vSkimmer can be configured to copy data to a specific USB device if it is unable to connect to the Internet. vSkimmer dumps its stolen data to a log file on a USB drive with a certain volume name.

[29] https://www.us-cert.gov/ncas/alerts/TA14-002A
[30] http://pages.arbornetworks.com/rs/arbor/images/Uncovering_PoS_Malware.pdf and http://news.softpedia.com/news/New-POS-Malware-JackPOS-Targets-Companies-in-Canada-Brazil-India-and-Spain-425871.shtml
[31] http://pages.arbornetworks.com/rs/arbor/images/Uncovering_PoS_Malware.pdf
[32] Ibid.
[33] Ibid.
[34] http://news.softpedia.com/news/New-POS-Malware-JackPOS-Targets-Companies-in-Canada-Brazil-India-and-Spain-425871.shtml
[35] Ibid.
[36] Ibid.
[37] Ibid.
[38] Ibid.
[39] http://www.secureworks.com/cyber-threat-intelligence/threats/point-of-sale-malware-threats/

Appendix C. Multi-Factor Authentication

This is an example of multi-factor authentication for a Citrix application.

[NOTE: Many Citrix remote access and virtualization solutions should support multi-factor authentication.]

Enable Two-Factor Authentication[40]

Use the Authentication Methods task in the Citrix Web Interface Management console to enable two-factor authentication for users, if required.

1. On the Windows Start menu, click All Programs > Citrix > Management Consoles > Citrix Web Interface Management.
2. In the left pane of the Citrix Web Interface Management console, click XenApp Web Sites and select your site in the results pane.
3. In the Action pane, click Authentication Methods and select the Explicit check box.
4. Click Properties and select Two-Factor Authentication.
5. Select the type of two-factor authentication you want to use from the Two-factor setting list and configure any additional settings as appropriate.

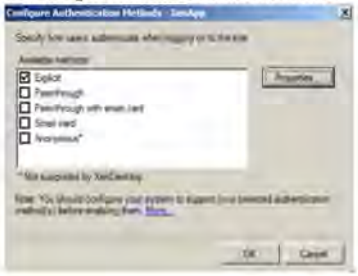
Configuring Two-Factor Authentication

The following steps were recommended by the security firms ActivIdentity Channel and Duo Security for configuring Citrix XenApp.[41] These include the following steps: configure Citrix radius settings, configure RADIUS shared Secret, and configure two-factor authentication settings.

For the XenApp:

1. Log in to the Citrix Web Interface Management Console.
2. Navigate to XenApp Web Sites and click on Authentication Methods.
3. Confirm that only Explicit is checked and click properties.

Figure 1. Configure Authentication Methods for XenApp[42]



[40] http://support.citrix.com/proddocs/topic/web-interface-hardwick/wi-enable-two-factor-authentication-gransden.html
[41] http://www.youtube.com/watch?v=ZRbi8JujO0 and https://www.duosecurity.com/docs/citrix_web_interface
[42] https://www.duosecurity.com/docs/citrix_web_interface

4. Click on Two-Factor Authentication and select RADIUS for the Two-factor Setting.

5. Add a RADIUS server and enter the AuthProxy IP address as the server address and 1812 for the server port. Configure the Timeout to 60 seconds and save your configuration.

Figure 2. XenApp Two-Factor Authentication[43]

[43] Ibid.

Figure 3. Adding the Radius Server IP Address[44]

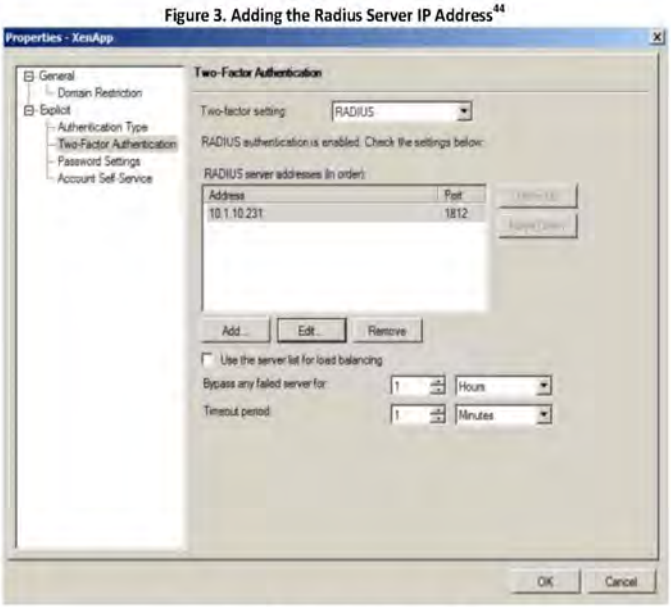
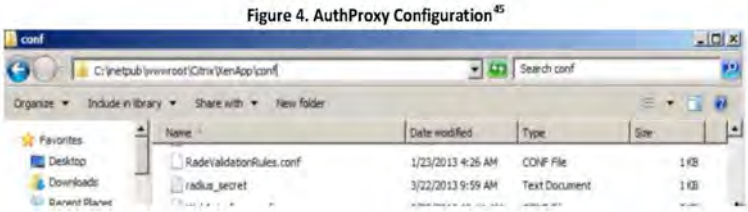


Figure 4. AuthProxy Configuration[45]



6. Create a new text file in the Citrix Web Interface \conf folder called radius_secret.txt. Type the radius_secret from the AuthProxy configuration in the radius_secret.txt file.

(The location for this file is given by the RADIUS_SECRET_PATH configuration value in the web.config file (for sites hosted on IIS) or web.xml file (for sites hosted on Java application servers). The location given is relative to the \conf folder for sites hosted on IIS and relative to the /WEB_INF directory for sites hosted on Java application servers.) Typically the location will be similar to: C:\inetpub\wwwroot\Citrix\Xenapp\conf.

[44] Ibid.
[45] Ibid.

7. On the Citrix Web Interface server open the web.config (IIS Hosted) or web.xml (Java Apps) file and add the Citrix Web Interface IP address as the "RADIUS_NAS_IP_ADDRESS".

Figure 5. Adding the Citrix Interface IP Address[46]

```
        <add key="RADIUS_SECRET_PATH" value="/radius_secret.txt"
/>
        <add key="RADIUS_NAS_IDENTIFIER" value="" />
        <add key="RADIUS_NAS_IP_ADDRESS" value="10.1.10.231" />
        <add key="AUTH:SERVER_ERROR"
value="/html/serverError.html" />
```

Two-Factor Authentication Tokens authentication methods for XenApp Web Sites[47]

- **Aladdin SafeWord for Citrix.** An authentication method that uses alphanumeric codes generated by SafeWord tokens and, optionally, PIN numbers to create a passcode. Users enter their domain credentials and SafeWord passcodes on the Logon screen before they can access applications on the server.
- **RSA SecurID.** An authentication method that uses numbers generated by RSA SecurID tokens (*tokencodes*) and PIN numbers to create a *PASSCODE*. Users enter their user names, domains, passwords, and RSA SecurID PASSCODES on the Logon screen before they can access resources on the server. When creating users on the RSA ACE/Server, user logon names must be the same as their domain user names. **Note:** When using RSA SecurID authentication, the system can generate and display a new PIN to the user. This PIN appears for 10 seconds or until the user clicks OK or Cancel to ensure that the PIN cannot be viewed by others. This feature is not available on PDAs.
- **RADIUS server.** An authentication method that uses the Remote Authentication Dial-in User Service (RADIUS) authentication protocol (as opposed to proprietary agent software). Both SafeWord and SecurID can be installed and configured to be presented as a RADIUS server. For Web Interface for Java Application Servers, RADIUS authentication is the only two-factor authentication option available.

[46] Ibid.
[47] http://support.citrix.com/proddocs/topic/web-interface-hardwick/wi-configure-two-factor-authentication-gransden.html