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

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

Prepared Testimony

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

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

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

History of Treasury's Role

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

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

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

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

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

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

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

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

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

Building Partnerships to Reduce Risk

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

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

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

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

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

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

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

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

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

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

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

Information Sharing

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

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

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

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

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

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

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

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

Incident Management

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

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

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

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

Best Practices

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

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

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

Conclusion

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

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