Testimony of

Doug Johnson

On behalf of the

Financial Services Sector Coordinating Council

Before the

U.S. Senate Committee on Homeland Security and Governmental Affairs

March 26, 2014

Testimony of
Doug Johnson
On behalf of the
Financial Services Sector Coordinating Council
Before the
U.S. Senate Committee on Homeland Security and
Governmental Affairs
March 26, 2014

Chairman Carper, Ranking Member Coburn, my name is Doug Johnson, vice president and senior advisor, risk management policy for the American Bankers Association. In that capacity, I currently lead ABA's enterprise risk, physical and cybersecurity, business continuity and resiliency policy and fraud deterrence efforts on behalf of our membership. I am testifying today in my capacity as vice chairman of the Financial Services Sector Coordinating Council (FSSCC), which advises the federal bank regulatory agencies on homeland security and critical infrastructure protection issues, and as a member of the board of directors of the Financial Services Information Sharing and Analysis Center (FS-ISAC), a private corporation that works with government to provide the financial sector with cyber and physical threat and vulnerability information as part of the nation's homeland security and critical infrastructure protection efforts.

I appreciate the opportunity to be here today representing the FSSCC and FS-ISAC. The American Bankers Association is proud of, and committed to, maintaining its leadership role in helping protect our nation's critical financial infrastructure. The deep involvement of ABA in both the FSSCC and the FS-ISAC is not unusual within the financial services sector. Many financial operators and trade associations are heavily involved in both. This collaboration includes financial organizations of all sizes. Our diverse sector is made up of organizations of all sizes and types, and ABA has been a primary driver behind expanding the FS-ISAC's reach from under 100 to over 4,700 members to ensure that vital cyber threat information, and the means to defeat those threats, reaches as many financial organizations as possible.

The financial sector shares the committee's commitment to strengthening public-private partnerships to reduce cyber risks to our nation's critical infrastructure. In my testimony, I will discuss:

- The cyber threats we face, both as an industry and as a nation;
- The role FSSCC and FS-ISAC play in fostering the public-private partnership's ability to address these threats; and
- The work currently underway through the National Institute of Standards and Technology (NIST) to create a cybersecurity framework for our nation to help us mitigate threats.

I. The Cyber Threat is Real and Growing

As you are aware, our nation's financial sector experienced a large number of disruptive cyber-attacks in 2012 and 2013, mostly in the form of distributed denial of service, or DDoS attacks. These attacks were designed to disrupt our sector's customer-facing online banking platforms and cause a periodic loss of availability for those customers. These attacks did not compromise the privacy of customer information or the integrity of bank systems. They were, however, large sustained attacks that challenged the resources of the money centers, as well as the regional, and community banks that were targeted.

Many of our efforts in the financial services sector are to ensure that attacks designed to disrupt users do not set the stage for data compromises or attacks on system integrity. We have seen some instances of blended attacks, where DDoS traffic is used as a diversion from a simultaneous attack on high value customers. We are also aware that a DDoS attack can be an attempt to test various points of entry within a financial institution's system for future, more sophisticated attacks. We are always alert for these possibilities and we expect the nature of attacks to change over time with a continued increase in sophistication and strength.

Our sector is also mindful of attacks that have occurred overseas which, if conducted against U.S. financial institutions, could have significant impact on systems and customers. An attack on Saudi Aramco in August of 2012, where a computer virus called Shamoon wiped the data off approximately 30,000 computers, and in March 2013, attacks against South Korean banks,

purportedly by North Korea, shut down ATM systems for several hours and disabled over 3,000 computers. These are just two examples of the types of attacks necessitating a high level of readiness on the part of our government and industries.

As exhibited by the recent breaches of merchant point-of-sale systems, we are also aware that our vulnerability to such attacks are, in many instances, based on security gaps that may exist on the part of merchants, our business or retail customers, or outsourced service providers. Many financial institutions, particularly those that are community-based, are also highly dependent on core banking system processors and internet banking service providers for cybersecurity protection. While the focus of this hearing is understandably on protecting critical infrastructure, it is also important that we strive to protect the entire financial and payment ecosystem and ensure that our partners in the payments system, our customers, critical service providers and other important business partners have appropriate protections against cybersecurity attacks.

II. The Financial Sector Actively Partners with the Public Sector to Address the Cyber Threat

The nature and frequency of the recent cyber-attacks have focused a great deal of financial institution attention on whether our institutions, regardless of size, are properly prepared for such events, and whether we are committing the appropriate level of resources to detect and defend against them. We also continuously assess and refine our preparedness to detect and respond to future attacks and actively engage our government partners in this process. These efforts build on a long-standing, collaborative imperative for the financial sector to protect institutions and customers from physical and cyber events. A significant protection infrastructure, in partnership with government, exists and is continually being improved.

As I have already indicated, in addition to my role at ABA, I am proud to currently serve as the vice chairman of FSSCC. I also serve on the board of its sister organization, FS-ISAC. ABA has been deeply involved in and supportive of these two organizations since their inception.

Established in 2002, FSSCC's mission is to strengthen the resiliency of the financial services sector against attacks and other threats to the nation's critical infrastructure by

proactively identifying threats and promoting protection, driving preparedness, and collaborating with the U.S. government. The council has over 60 volunteer member associations and financial institutions representing clearinghouses, commercial banks, credit rating agencies, exchanges/electronic communication networks, financial advisory services, insurance companies, financial utilities, government-sponsored enterprises, investment banks, merchants, retail banks, and electronic payment firms. During the past decade, the partnership has continued to grow, both in terms of the size and commitment of its membership and in the breadth of issues it addresses. Members commit their time and resources to FSSCC with a sense of responsibility to their individual firms and for the benefit of financial consumers and the nation.[1]

The FSSCC is considered the policy arm of the financial sector in terms of its engagement with the public sector and other critical sectors of the economy. As such, much of 2013 was dedicated to responding to the administration's executive order, particularly regarding the development of NIST's Preliminary Cybersecurity Framework. As I will discuss later in my testimony, our sector is supportive of the administration's and NIST's efforts and will remain engaged as we migrate toward the framework's implementation phase.[2]

FS-ISAC, considered the operational arm of the financial sector for critical infrastructure protection purposes, was established by the sector in response to 1998's Presidential Directive 63. That directive - later updated by 2003's Homeland Security Presidential Directive (HSPD) 7 and, most recently PPD 21 called upon the public and private sectors share information about physical and cybersecurity threats and vulnerabilities to help protect the U.S. critical infrastructure. Constantly gathering reliable and timely information from financial services providers, commercial security firms, federal, state and local government agencies, law enforcement and other trusted resources, the FS-ISAC is positioned to quickly disseminate physical and cyber threat alerts and other critical information throughout the financial sector. FS-ISAC has also recently taken over the role of coordinating crisis response for the sector, formerly a responsibility of FSSCC.

---

[1] A copy of the FSSCC 2012-2013 Annual Report is available here: http://fsscc.org/fsscc/reports/2013/FSSCC-Annual-Report-2012-2013.pdf.
[2] The FSSCC letter of support for the NIST Cybersecurity Framework is available here: http://fsscc.org/fsscc/news/2014/FSSCC-PressRelease-NIST_CSF.pdf.

The overall objective of FS-ISAC is to protect the financial services sector against cyber and physical threats and risk. It acts as a trusted third party that provides anonymity to allow members to share threat, vulnerability and incident information in a non-attributable and trusted manner. The FS-ISAC provides a formal structure for valuable and actionable information to be shared among members, the sector, and its industry and government partners, which ultimately benefits the nation. FS-ISAC information sharing services and activities include:

- Delivery of timely, relevant and actionable cyber and physical email alerts from various sources and an anonymous online submission capability to facilitate member sharing of threat, vulnerability and incident information in a non-attributable and trusted manner through the FS-ISAC Security Operations Center (SOC);
- Support for information exchanges with various special interest groups including the FSSCC, the FS-ISAC Threat Intelligence Committee, the Payment Processors Information Sharing Council (PPISC), the Clearing House and Exchange Forum (CHEF), the Business Resilience Committee (BRC), and the Payments Risk Council (PRC);
- Development of risk mitigation best practices, threat analysis, toolkits, and the preparation of cybersecurity briefings and white papers; and
- Development and testing of crisis management procedures for the sector in collaboration with the FSSCC and other industry bodies;

Our main government partner in FSSCC and FS-ISAC efforts is the Financial and Banking Information Infrastructure Committee (FBIIC), which is led by the U.S. Department of the Treasury and chartered under the President's Working Group on Financial Markets. FBIIC is charged with improving coordination and communication among financial regulators, enhancing the resiliency of the financial sector, and promoting the public/private partnership. The public sector's commitment to the public-private sector partnership outside of the already mature regulatory regime is essential to FSSCC's success.

In addition to FBIIC and Treasury, FSSCC and FS-ISAC also work closely with the Department of Homeland Security (DHS), United States Secret Service, Federal Bureau of Investigation (FBI), National Security Agency (NSA), Central Intelligence Agency (CIA), and

state and local governments. For example, in partnership with DHS, FS-ISAC two years ago became the third ISAC to participate in the National Cybersecurity and Communications Integration Center's (NCCIC) watch floor. FS-ISAC representatives, cleared at the Top Secret / Sensitive Compartmented Information (TS/SCI) level, now attend the daily briefs and other NCCIC meetings to share information on threats, vulnerabilities, incidents, and potential or known impacts to the financial services sector. Our presence on the NCCIC floor has enhanced situational awareness and information sharing between the financial services sector and the government with numerous examples of success. It is for this reason that the FSSCC supports formalization of the NCCIC through legislation.

As part of this partnership, FS-ISAC set up an email listserv with United States Computer Emergency Readiness Team (U.S. CERT) by which actionable incident, threat and vulnerability information is shared between FS-ISAC members and U.S. CERT in near real-time. This listserv also facilitates the information sharing that is already occurring between FS-ISAC members and the NCCIC watch floor or with other government organizations.

In addition, FS-ISAC representatives sit on the Cyber Unified Coordination Group (Cyber UCG). This group was set up under authority of the National Cyber Incident Response Plan (NCIRP) and has been actively engaged in incident response. Cyber UCG's response to, and communications with, various sectors following the DDOS attacks on the financial sector in late 2012 and early 2013 is one example of how this group is effective in facilitating relevant and actionable information sharing.

FS-ISAC and FSSCC have also worked closely with government partners to obtain over 250 Secret level clearances and a number of TS/SCI clearances for key financial services sector personnel. These clearances have been used to brief the private sector on new information security threats and provided useful information to implement effective risk controls to combat these threats.

The FS-ISAC also works very closely with the other critical infrastructure sectors through direct communication with other ISACs, as through the National Council of ISACs. Information about threats, incidents and best practices is shared daily among the ISACs via ISAC analyst calls and a cross-sector information sharing platform. The ISACs also come together during a crisis to coordinate information and share mitigation efforts, as applicable.

Cross-sector cooperation and coordination for homeland security and critical infrastructure protection also occurs through the Partnership for Critical Infrastructure Security (PCIS) Cross-Sector Council. The PCIS Cross Sector Council, through the membership of the individual sector coordinating councils such as the FSSCC, is the collective body of the private critical sectors identified in HSPD 7. The 20 sectors and sub-sectors have unanimously determined this Council to be their means of obtaining the objectives set forth in the Administration's 2013 revision of the National Infrastructure Protection Plan (NIPP) for consultations and collaborative efforts and unified engagement with the Federal government in fulfilling our joint critical infrastructure protection mission.

To reinforce this commitment, the Council is developing a new charter that ensures clarity on the Council's purpose, role, areas of focus, and governance. The Council is also drafting a Memorandum of Understanding with DHS's National Protection and Programs Directorate that: 1.) defines the purpose of the national-level public-private partnership; 2.) sets strategic priorities; 3.) recommends areas of emphasis for the collaborative effort to attain and advance these priorities; 4.) establishes rules of engagement through agreed best practices; and 5.) ensures effective coordination and consultation. We believe these actions will clarify and confirm the critical sectors' commitment to the council and the manner in which the council will operate and communicate - particularly with regard to its public sector partners.

III. The Financial Sector Supports the NIST Cybersecurity Framework

As mentioned earlier in my testimony, FSSCC and FS-ISAC continue to support the goals of the administration and Congress to limit cybersecurity threats to business, our government, and the American people through a more integrated approach.[3] We applaud the release of Executive Order 13636 and believe implementation of the cybersecurity framework envisioned in the order can be an important tool in improving our nation's overall cybersecurity.

[3] The FSSCC Comment Letter in Response to the NIST Request for Information, "Developing a Framework to Improve Infrastructure Cybersecurity" is available here: http://csrc.nist.gov/cyberframework/rfi_comments/040813_fsscc.pdf.

Through FSSCC, our sector is committed to working collaboratively with NIST to further improve the framework and our nation's overall cybersecurity posture. We offer the following recommendations to meet our mutual goals:

- **Encourage the development of sector-specific approaches to the framework.** Recognizing the uniqueness of each sector, the FSSCC will develop a sector profile that will map to the framework. An important component of this sector profile will be a determination of how well the framework maps to existing regulatory requirements. Although the financial sector's stringent regulatory requirements are not specifically itemized in the framework, they nonetheless map well to the framework core functions of identify, protect, detect, respond and recover. Many financial firms already organize their cybersecurity functions in a similar matter, for business as well as regulatory purposes.

- **Facilitate automated information sharing.** Typically the time associated with analyzing a specific cyber threat indicator is substantial. As a result, the "Roadmap" developed by NIST in conjunction with the Framework recognizes that the automated sharing of threat indicator information can provide organizations with timely, actionable information that they can use to detect and respond to cybersecurity events as they are occurring.

  FS-ISAC recognized this need over 18 months ago and embarked on the design and development of the financial sector's first Cyber Threat Intelligence Repository to automate threat intelligence sharing. Our goal with this automation solution is to help our sector increase the speed, scale and accuracy of information sharing and accelerate time to resolution.

- **Clarify liability protections for sharing cyber threat data.** The timely, voluntary sharing of threat information is critical to the government and the private sector in developing and deploying protective measures against malicious cyber activity. While the cyber threat data that are shared by the financial services sector are in machine language and not attributable to an individual, clarity concerning liability protections for the sharing of information are still extremely important and transcend our sector.

- **Foster the growth of existing ISACs and encourage the development of similar models for other sectors currently not deemed critical infrastructure.** Through its current role as the chair of the National Council of ISACs, the FS-ISAC strongly supports cross-sector information sharing initiatives. The FS-ISAC is also working with the retail sector to determine how we can best assist merchant information sharing needs.

- **Leverage existing audit and examination processes and encourage complementary, not redundant audit requirements when implementing the framework.** In my testimony I have noted that the framework fits well with existing financial sector regulatory requirements, but we are still concerned that efforts to implement the framework could create a separate certification process that would be layered over – and possibly complicating -existing cybersecurity examinations and extensive internal and external audits that financial sector firms already undergo. In particular, implementation of the framework should not require additional third party audits in order for a company to be eligible for any incentives where existing audit and regulatory examinations are already in place.

- **Create incentives that are tailored to address specific market gaps.** To the extent that adoption of the framework may be induced through incentives, such incentives should strive to be market-based rather than driven by the public sector. For example, insurance underwriters have, without government inducement, already been asking financial firms how they are planning to incorporate the framework into their cybersecurity protection schemes. Other market incentives include firms requiring their significant supply chain partners to incorporate the framework in some fashion. Only when it is determined that there are specific gaps within the market incentives process should the public sector consider stepping in.[4]

- **Foster Research and Development and Workforce Creation.** The NIST Roadmap for Improving Critical Infrastructure Cybersecurity, in its discussion of next steps, also highlights several research and development issues, such as authentication, as well as

[4] The FSSCC Comment Letter in response to the Department of Commerce's Notice of Inquiry: Incentives to Adopt Improved Cybersecurity Practices, is available here: http://www.ntia.doc.gov/files/ntia/fssccresponse-doc_noi.pdf.

cybersecurity workforce development. The FSSCC is fully supportive of enhancing cybersecurity research and development, and believes that a skilled workforce is critical as the cybersecurity threat and technology environment evolves. Through its R&D Committee, the council has also identified identity assurance and authentication as an area requiring specific R&D attention and welcomes the opportunity to work with NIST and other stakeholders on building a framework of authentication standards.

IV. Conclusion

Thank you for holding this important hearing. Financial service companies have made cybersecurity a top priority. We have invested an enormous amount of time, energy and money to put in place the highest level of security among critical sectors and exceed the most stringent regulatory expectations placed upon our sector.

We cannot, however, do this alone. As a nation we must compel appropriate international government bodies to align cyber security laws, law enforcement cooperation and mutual recognition, in addition actively prosecuting and punishing those responsible for committing cyber-crimes. Every nation must recognize that its place in the broader global economy depends on its contribution to the stability of and trust in the critical financial infrastructure that is the circulatory system of national and global economic growth. Enforced norms for global cybersecurity collaboration are an essential foundation of that principle.

We look forward to continuing to work with you toward our mutual goal of protecting our nation's critical assets.