FINANCIAL SERVICES ROUNDTABLE

February 4, 2015

Testimony of
Paul Smocer

On behalf of

BITS/ Financial Services Roundtable

Before the

United States Senate
Committee on Commerce, Science and Transportation

Hearing on

"Building a More Secure Cyber Future: Examining Private Sector Experience with the NIST Framework"

Chairman Thune, Ranking Member Nelson, Members of the Committee, thank you for this opportunity to appear before you today to address the important topic of cybersecurity and the evolution of public and private efforts to protect critical infrastructure from cyber threats.

My name is Paul Smocer, and I am the President of BITS, the technology policy division of the Financial Services Roundtable (FSR). FSR is a trade association representing the country's leading financial service companies. Our members include banking, insurance, asset management, finance, and payment companies. Cybersecurity has been a key focus area for FSR and our companies for decades. Since 1996, BITS has played an important leadership role in cybersecurity, fraud reduction, third-party vendor management, payments and emerging technologies. BITS addresses issues at the intersection of financial services, technology, and public policy.

Cyber Threat Environment

Late last year, with this Committee's stewardship, Congress passed the Cybersecurity Enhancement Act of 2014 (Public Law No: 113-274). We believe the Act's focus on supporting and facilitating an open and voluntary cybersecurity standards development process is an important step in improving the overall information security of our country's cyber ecosystem. Moreover, we applaud the Act's emphasis on cybersecurity research and development, cybersecurity career development, and cyber awareness and education. Indeed, with the passage of this Act, Congress has signaled its commitment to cultivate the public-private partnership - a partnership that is essential to our nation's security.

Even with these improvements, more needs to be done. The current cyber threat environment is grim. Each day, cyber risk grows as attacks increase in number, pace, and complexity. We are no longer in the days wherein the threat was confined to individual hacktivists and fraudsters. We are now in an era of attacks by not only organized crime syndicates, but also nation-states. Correspondingly, the attacks have grown beyond webpage vandalism and fraud into large-scale attacks that threaten the availability of services to citizens and threaten the privacy and accuracy of their information. Our sector is increasingly concerned with these threats, particularly with the potential for attacks that could undermine the integrity of the financial system through data manipulation or destruction. This growing threat affects all institutions in our sector regardless of size or type of financial institution including large and small, banks, credit unions, insurers and investment firms. Increasingly, and as we have recently witnessed, other sectors face these same threats.

As mentioned, with each day that passes, the cyber threat against our nation's critical infrastructure, private sector companies, and individuals' privacy intensifies. According to Symantec's 2014 "Internet Security Threat Report," the number of targeted spear-phishing campaigns in 2013 rose by 91% over the previous year. These campaigns are a key method used by cyber attackers to infiltrate victim's systems and gather information. In recent years, we have also witnessed serious and significant attacks from various nation-state actors and

organized criminals on the Estonian, Georgian, and Ukrainian telecommunications systems[1]; European power plants[2]; a U.S. public utility[3]; the NASDAQ[4]; Target and other major retailers and their customers.[5] Moreover, a recent report reveals that of the estimated $2-3 trillion generated annually from the "internet economy," cybercrime alone extracts between 15% and 20% of that total value.[6] In response, the private sector has increased its spending on cybersecurity, with one financial services firm spending as much as $250 million a year.

The quote often attributed to Willie Sutton that he robbed banks "because that's where the money is" reminds us as to why financial institutions are often the subject of cyber-attacks. Being a focus of the attacks is certainly one reason why the financial sector has historically led the way in making huge investments in not only security infrastructure and the best-qualified people to maintain the systems, but also in driving collaboration across industries and with the government. The primary reason for these investments though is the recognition that our customers trust us to protect them – to protect their investments, their records and their information. Individual financial institutions invest in personnel, infrastructure, services, and top of the line security protocols to protect their customers and themselves and to respond to cyber-attacks. These investments protect the individual institutions and their customers, but on its own, an individual institution generally only has the ability to protect what is within its "four walls of the company". However, as we all know, companies do not exist only within those walls. We are connected within our sector, across sectors, and with the government. This reliance on each other gives all of us a unique and critical role in the cyber landscape and requires coordinated action for the most effective response. Recognizing the cyber threat environment continues to expand in complexity and frequency and that individual institution efforts alone will not be enough, executives from the financial services sector have stepped up efforts to work together.

Financial Sector Collaborations

Our sector has facilitated a series of collaborations that resulted in a number of achievements, such as:

- The development of the Financial Services Information Sharing and Analysis Center (FS-ISAC) in 1999, which has grown in membership and capabilities since then, and

---

[1] Reuters, "Ukraine: Cyberattack on communications, MPs phones blocked," http://www.cnbc.com/id/101465198, (March 4, 2014).
[2] Symantec Security Response, "Dragonfly: Western Energy Companies Under Sabotage Threat," http://www.symantec.com/connect/blogs/dragonfly-western-energy-companies-under-sabotage-threat, (June 30, 2014).
[3] ICS-CERT Monitor, "Internet Accessible Control Systems At Risk," https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_%20Jan-April2014.pdf, (January-April 2014).
[4] Michael Riley, "How Russian Hackers Stole the Nasdaq," http://www.businessweek.com/articles/2014-07-17/how-russian-hackers-stole-the-nasdaq, (July 17, 2014
[5] Symantec Corporation, " Internet Security Threat Report 2014," http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf, (April 2014).
[6] Center for Strategic and International Studies , "Net Losses: Estimating the Global Cost of Cybercrime Economic impact of cybercrime II,http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf, (June 2014).

significantly helped the sector response to the 2012-2013 distributed denial of service attacks (DDoS) preventing wide-scale outages;
- Creation of Soltra Edge, an initiative that will help standardize and automate the flow of real-time cyber threat information;
- Collaborating with the merchant and retail community to share best practices on cybersecurity, information sharing and payments security; and
- The significant and coordinated financial services industry effort during the development of the NIST Cybersecurity Framework.

The NIST Cybersecurity Framework

Almost two years ago, President Obama issued Executive Order 13636, calling for the development of a voluntary cybersecurity framework by the National Institute of Standards and Technology (NIST). The executive order directed NIST to seek private sector input through a collaborative process. From the outset, BITS/FSR -- both as an organization and as a sector representative for the Financial Services Sector Coordinating Council (FSSCC) -- participated in the NIST Cybersecurity Framework's development by taking part in all six NIST-facilitated workshops, providing the perspective of our uniquely diverse membership to this important effort. We appreciated the opportunity to be one of the major contributors to NIST's hard work that almost a year ago today, resulted in NIST's release of the Framework for Improving Critical Infrastructure Cybersecurity.

The financial services sector is often credited, and rightly so, as being one of leaders in cybersecurity. That is why we wanted to be a part of the Framework's development. We wanted to ensure the eventual framework addressed our unique sector attributes, and we wanted to understand how it would harmonize our existing requirements. We recognized too that in an interconnected world, we as a sector are not an island unto ourselves. We need and rely on entities that provide us with information technology, power, telecommunications and other critical services. We applaud that NIST's process for developing the Framework engaged these other sectors during the Framework's drafting. NIST's successful approach at inclusion of so many essential parties is reflected in how broadly embraced the Framework has become across so many sectors.

With respect to the Framework, its true value is that it synthesizes a process for cyber risk management that is accessible from the boardroom to the operations floor, across not only individual enterprises but also entire sectors. It relies on international standards and is consistent with the regulatory requirements that have been in place for our sector for more than a decade. It is a "Rosetta Stone" in that it provides a common lexicon for categorizing and managing cyber risks across sectors and enterprises for various unifying risk management jargons and creates a common understanding around various risk management terms, methodologies, ideas and language.

As a result, we have heard from member financial institutions that in terms of internal enterprise usage, Chief Information Security Officers (CISOs) are using the Framework to communicate ideas and achieve "buy-in" for various cybersecurity initiatives. Externally, firms are beginning to use it to communicate expectations and requirements to vendors. That

said the Framework has only been in circulation for a relatively short time. This is an important fact for this Committee to keep in mind as it reviews the Framework at its anniversary. Because it has been only one year – one budget cycle for most firms – usage from institution to institution varies. Appropriately, the number of institutions that are aware and use the Framework, and the ways in which the Framework will be used, will evolve over time. An example of how the Framework continues to permeate new industries is its progressing role in the insurance space. The potential for the Framework to act as a baseline standard for cyber-insurance underwriters shows a new level of possibility and versatility for the voluntary standards.

Regarding the Framework development process, it was a success due in large part to its transparency and because it sought to harmonize various views into a cohesive whole. Indeed, BITS/FSR continues to participate in the evolution and maturation of the Framework through NIST's ongoing activities. For example, later this month we will be participating as a sector representative at NIST's "Cybersecurity and Consumer Protection Summit: Executive Technical Workshop on Improving Cybersecurity and Consumer Privacy" at Stanford University.

Just last week, BITS provided input to the Cybersecurity Forum for Independent and Executive Branch Regulators, which is comprised of all the independent regulators that are looking at ways to align and harmonize with the Framework and thus increase overall effectiveness and consistency of regulatory authorities' cybersecurity efforts pertaining to critical infrastructure. BITS reviewed how financial institutions manage cybersecurity risks, comply with comprehensive regulatory requirements, and collaborate to mitigate cyber risks. We urged the regulators to focus on harmonizing regulatory requirements to reduce regulatory compliance burdens and to focus resources on mitigating cyber risk.

However, the process has not been uniform across all stakeholders. In the year since the Framework's release, some federal and state agencies have charted similar yet divergent paths to enhancing cybersecurity that do not embrace the Framework's open and collaborative process, instead favoring agency-unique approaches that often do not align with the Framework. As a result, information security practitioners have had to devote their time to managing a patchwork of conflicting agency efforts and organizations have to invest funding in potentially duplicative efforts, which are significant drains on available resources. While some may say that is the "cost of doing business", such a statement ignores the current reality: There is already a recognized shortage of security professionals and money needing to be increasingly invested in cybersecurity limits investment in new products to serve consumers. Thus, we would urge this Committee, as part of its oversight function, to encourage agencies to focus more on coordination and harmonization.

Financial Top Level Domains

Like the process behind the NIST Framework, the financial services industry is no stranger to voluntary processes designed to benefit the greater good. I would like to highlight two of our most recent successes: .BANK and .INSURANCE, and Soltra Edge.

As background, in 2008, the Internet Corporation for Assigned Names and Numbers (ICANN) approved its new generic Top-Level Domains Program. This program in 2013 opened the door to a land rush on new top-level domains—the top-level domains we were accustomed to such as .COM and .ORG are no longer the only suffixes available. For a time we advocated against this domain name expansion especially as it related to financial services oriented domains out of concern for customer confusion, potential for increased malicious activity and ultimately increased costs to brand holders. When it became clear our concerns would not be addressed, the Financial Services Roundtable/BITS and the American Bankers Association, along with other financial services organizations, partnered to create a new registry operator dedicated specifically to the financial services sector - fTLD Registry Services, LLC.

This newly created organization submitted community-based applications for .BANK and .INSURANCE. I say community because unlike some entrepreneurs who have entered this space with little or no concern for protecting financial institutions or their customers, fTLD is dedicated to serving and protecting the global financial services industry. This is evidenced by the more than 120 financial services domestic and international entities who directly or through others endorsed our applications on behalf of the industry.

Besides being a financial services' owned, operated and governed registry, fTLD's domains of BANK and .INSURANCE will go beyond being simply an alternative to the legacy domains of .COM and .ORG. These domains will have robust operational requirements including eligibility, verification and name selection standards as well as enhanced technical requirements including, but not limited to, Domain Name Security Extensions (DNSSEC), strong encryption standards and email authentication requirements to mitigate for example phishing and spoofing activities. fTLD is also planning other innovative uses that will be announced at a later date. All of these enhanced requirements and capabilities could only happen when individual organizations voluntarily came together to work towards a better and safer Internet.

Secondly, I want to highlight Soltra Edge, a threat intelligence-sharing platform created by a joint venture between FS-ISAC and the Depository Trust and Clearing Corporation and voluntarily funded by contributions from the financial services community. Soltra Edge is a software solution that supercharges the current information-sharing model to make it more automated and collaborative so that trusted, actionable intelligence from disparate sources can be uniformly disseminated in near real time to defend more effectively against cyber threats. The software for Soltra Edge only takes a few minutes to download and install with the basic license completely free, making this solution accessible to the largest and smallest financial institutions.

While this effort started in the financial services sector, we expect the technology behind Soltra Edge to be adopted broadly by other critical sectors including healthcare, energy, transportation, retail and others.

Though Soltra Edge represents significant progress in closing the gap between threat intelligence sharing and implementing mitigating controls, a platform like this is still

constrained by legal limitations on what information can be shared. Congress has an important role to play in filling this gap. The passage of effective cyber threat information sharing legislation is a critical step to enabling optimal sharing capability.

The Public-Private Partnership: How Congress Can Help

While the NIST Cybersecurity Framework is a helpful tool, it is not the silver bullet that puts an end to the cyber threat. As such, an institution could use the NIST Cybersecurity Framework fully and it could still be compromised. Thus, more is needed, and Congress can help. At a basic level, policymakers can help by recognizing that the firm that experiences the cyber-attack -- be it a bank, retailer, or an entertainment firm -- is a victim. Political leaders and regulators should work to de-stigmatize attacks and encourage companies to come forward and share threat information that could help other companies protect themselves, their employees and their customers.

Despite the success of the information-sharing model used by the financial services sector, more can be done. We believe the Framework would be bolstered by the passage of effective cyber threat information sharing legislation. Our sector has been focused on this effort for many years and has continued to work closely with key committees in both the House and Senate. The legislation should not be delayed. BITS/FSR has supported several pieces of information sharing legislation developed by both the House and Senate. Most recently BITS/FSR has supported the cyber threat information sharing legislation passed by the Senate Intelligence Committee last year, the Cybersecurity Information Sharing Act of 2014 (CISA). BITS/FSR worked closely with former Chair Chambliss, Vice Chair Feinstein and their staff to develop the bipartisan bill. In our view, that bill encompassed key components to help enhance the volume and scope of threat information sharing. Furthermore, the legislation had the support of not only the financial services sector but also a wide range of critical infrastructure sectors. Congress must enact legislation that incentivizes the sharing and receiving of cyber threat indicators amongst companies within sectors, between sectors, and with the government. BITS/FSR believes that for legislation to be truly effective it must include the following provisions:

- Facilitate real-time sharing to enable institutions and government to act quickly;
- Provide a targeted level of liability and disclosure protections for cyber threat information sharing and receiving between individual institutions, through existing sharing mechanisms such as our FS-ISAC, private to government, and government to private;
- Offer a good faith defense for the sharing of threat information and data;
- Provide protection from disclosure through the Freedom of Information Act or to prudential regulators;
- Facilitate the appropriate declassification of information by the intelligence agencies and expedites the issuance of clearances to appropriate private sector individuals; and
- Include appropriate levels of privacy and civil liberties requirements.

BITS/FSR is encouraged by recent bipartisan progress and will continue to advocate for legislation that will allow our members to share cyber threat information with each other, various business sectors, the government, and law enforcement, to protect their customers.

Conclusion

In conclusion, the NIST Cybersecurity Framework benefits and strengthens the overall cybersecurity posture of critical infrastructure organizations, including those sectors on which financial institutions rely. The Framework will continue to play an important role as we continue to combat the growing threat of cyber-attacks. With that said, more can be done to encourage adoption of this voluntary Framework. This Committee should use its oversight authorities to encourage agencies to coordinate and harmonize cybersecurity requests, examinations, and guidance. Security professionals and investment dollars are constrained. When different regulators place duplicative burdens on security, that takes away from resources that could be devoted to preventing cyber-attacks. That, in turn, does not help any company and ultimately weakens our ability to protect the nation's critical infrastructure.

The risks associated with cyber-attacks and threats are vitally important to the private and public sectors. Protecting consumers, companies, and the nation must remain the focus. The ability to share information is at the core for our nation’s response to the current cyber threat.

Thank you again for inviting me to testify on this critical issue. Chairman Thune and Ranking Member Nelson, we look forward to working closely with you and the rest of the Committee on this important issue.