STATEMENT OF

BITS PRESIDENT PAUL SMOCER

ON BEHALF OF THE FINANCIAL SERVICES ROUNDTABLE

BEFORE THE

THE UNITED STATES HOUSE OF REPRESENTATIVES

PERMANENT SELECT COMMITTEE ON INTELLIGENCE

ADVANCED CYBER THREATS FACING OUR NATION

FEBRUARY 14, 2013

TESTIMONY OF PAUL SMOCER, BITS PRESIDENT

Thank you Chairman Rogers, Ranking Member Ruppersberger and Members of the Committee for the opportunity to testify before you today.

My name is Paul Smocer and I am the President of BITS, the technology policy division of The Financial Services Roundtable. BITS addresses issues at the intersection of financial services, technology and public policy, on behalf of its one hundred member institutions, their millions of customers, and all of the stakeholders in the U.S. financial system.

First, we would like to recognize the Chairman and Ranking Member, as well as several member of the Committee for your introduction of the Cyber Intelligence Sharing and Protection Act of 2013. We believe information sharing is a cornerstone of essential cybersecurity legislation. We have written a letter of support and ask that it be submitted to the record.

Overall, we believe this bill would increase the current level of information sharing, while recognizing and responding to the key privacy concerns. Increasing information sharing is essential for institutions to respond efficiently to the ever-evolving threat environment, and plays a critical role in improving our nation's cyber defenses.

We believe this legislation will:

- Modify current constraints to allow for improved information sharing,
- Enable existing information sharing and analysis mechanisms to gain access to important cyber threat information, and
- Increase threat information sharing between the public and private sectors.

In addition, however, we believe that several other legislative issues require action:

- Identify current sector models that have successfully implemented strong cybersecurity standards and robust implementation processes and leverage those models to other sectors,
- Increase funding for government for research to develop and test next generation security controls, and
- Update the criminal code to adequately include cybercrime and enhance law enforcement capabilities to investigate and prosecute criminals internationally.

Current Threat to Financial Services

For the financial services industry, cyber threats are a reality and a potential systemic risk to the industry. This is something that our institutions and our regulators both recognize. The Financial Stability Oversight Council (FSOC) [1], established under the Dodd-Frank Wall Street Reform and Consumer Protection Act to provide comprehensive monitoring of the stability of the financial systems, regularly discusses the risks of cyberattacks. Financial institutions are also subject to independent regulatory examinations focused on their cybersecurity risk assessments, controls, and compliance to existing regulations and regulatory guidance.

Our businesses are fully predicated on trust and confidence. The trusted transfers and transactions that occur hundreds of millions of times in a day are a requirement for modern capital markets and governments to conduct business, each riding on top of the backbone of cyberspace.

Cyber criminals are taking advantage of a global system, the Internet, which delivers services, products and functions to marketplaces around the world. The Internet has opened up previously untouchable markets and sources of revenues for large and small businesses alike. Legitimate users of the Internet enjoy increased speeds, improved processes, better understanding of their customer base and clear metrics for planning and product enhancements. Legitimate business is thriving on the Internet and it is driving additional requirements, innovations and new definitions of high performance. Unfortunately, threat actors are using the same Internet in similar ways, but for nefarious purposes. They are expanding their capabilities and exploiting the inherent trust we all have in the World Wide Web to conduct malicious activity.

Cyber threat actors largely fall into four high level categories: individual hackers, hacktivist collectives, criminal networks and nation state groups. Regardless of which category they fall into, they pose a significant, evolving risk and danger to the global marketplace. Threat actors conduct malicious activities that can result in a range of outcomes. These include theft of confidential data to preventing infrastructure critical to financial institutions from performing key functions, such as damaging the integrity of market data or preventing systems from being available to customers,

[1] The Council is comprised of 15 members appointed by the President from federal financial regulators, state regulators and an independent insurance expert.

shareholders and investors. Generally, threat actors have one of the three objectives in mind as they plan and coordinate their malicious activities:

1. Theft: Actions resulting in the theft of customer, proprietary, or confidential data or information.
2. Disruption: Actions intended to cause disruptions to systems and operations, denying authorized users access to the affected systems.
3. Destruction: Actions intended to compromise the integrity of or cause the destruction of data and systems.

Today threat actors have the same tools and the same advantages as Fortune 500 businesses and many governments. They have full and unfettered access to the Internet, sophisticated tools, in-depth knowledge of network topologies and closely integrated teams of experts. Threat actors are thriving on the global information superhighway, and pose a threat with far greater consequences than traditional threats the financial sector protected itself from in the past.

This new threat actor set is often protected from the reach of law, is provided sophisticated training, may even have the tacit approval and/or the financial backing of a nation state or states and are able conduct malicious activity globally. These threat actors are able to conduct focused operations and they are highly coordinated. Trained in the latest tactics, techniques and procedures, they enjoy near anonymity while traversing the global grid. Moreover, they are trained to obfuscate their work and to strategically exploit a network. Unlike traditional thieves, these threat actors are not always in this for financial gain. They are interested in achieving very specific outcomes, may take years to plan an activity and are strategically positioning within the context of the global risk climate.

Make no mistake about it, the financial sector remains concerned with the traditional threats to banking and finance; however, we have been and continue to add capability and capacity to handle the new operational realities of the interconnected global risk environment. To be clear, the risks poised against the sector are advanced.

Financial Services Sector Response

Individual financial institutions respond to these attacks through investments in personnel, infrastructure, services, and top of the line security protocols. These investments protect the individual institutions and their customers to the ability the institution is able to within the "four walls of the company". However, as we all know, the world we live in is not only within a company. We are connected within our sector, across sectors, and with the government. This reliance on each other gives each of us a unique and critical role in the cyber landscape and requires coordinated action for the most effective response. Our sector works collaboratively with our government partners to:

- Prepare for attacks by collecting, analyzing and disseminating threat information to the extent currently feasible, assessing systemic risks, and conducting joint exercises.
- Stay ahead of adversaries and reduce number of incidents by anticipating threats, implementing countermeasures and addressing critical vulnerabilities.
- Identify incidents as they occur by implementing key controls that would improve our ability to detect and block attacks at "net speed".
- Respond to incidents in the manner that will reduce the impact and risk to the financial institution and the sector.
- Improve security posture, and minimize impact through robust forensics, investigations and learned capability.

Given the interconnected nature of cyberspace, institutions recognize that the strongest preparations and responses to cyberattacks require collaboration beyond their own companies. As a result, as a sector a number of collaborative efforts exist. Through associations such as BITS, the Financial Services Sector Coordinating Council (FSSCC) and the Financial Services Information Sharing and Analysis Center (FS-ISAC), participants collectively identify threats to consumers, institutions and the sector to prepare for potential attacks. In the event of a cyberattack, information on the threat and strategies for responding is actively shared through various organizations and coordinated working alongside our sector specific agency, the Department of Treasury. These partnerships within the sector have been a major focus of the industry over the past decade and their ability to work efficiently in times of attack is essential to the industry's response.

Financial Services Information Sharing and Analysis Center (FS-ISAC)

The FS-ISAC coordinates information sharing today between financial institutions and the federal government, law enforcement and other critical infrastructure sectors. Information is shared through the traffic light protocol (TLP), which allows recipients of the threat data to know the sensitivity of the information they receive and their ability to share. Items designated green can be shared with the widest audience, yellow can be shared to those within the recipient's institution, and red cannot be shared. This allows for data to be distributed widely in the most secure fashion possible. The security designation of the information is determined by the contributing organization or institution. (http://www.fsisac.com/)

Financial Services Sector Coordinating Council (FSSCC)

The largest of these industry collaborations is perhaps the sector's Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC). This group consists of over 20 financial trade associations, ten of the largest US-based financial institutions and ten key participants operating in the financial infrastructure. Through the Council, these organizations come together to focus on key policy areas, threat and vulnerability, research and development and resiliency. (https://www.fsscc.org/fsscc/)

Financial and Banking Information Infrastructure Committee

In the spirit of public-private partnerships, the FSSCC works closely with its public sector partner Financial and Banking Information Infrastructure Committee (FBIIC), which is charged with improving coordination and communication among financial regulators, enhancing the resiliency of the financial sector, and promoting the public/private partnership. Chaired by the Treasury Department, this Committee includes sixteen government agencies with oversight for the entire financial sector including regulators within the capital markets. Working together, the Council and the Committee members focus on key cybersecurity issues affecting the industry and how to address them. (https://www.fbiic.gov/)

Importance of Sharing Threat Information

The important reality to acknowledge is that this is not a threat specific to financial services. The cyber threat affects multiple sectors, as characterized by the organizations represented by my fellow panelists. We all experience attacks and work within our sectors as the current law allows. Viruses, Trojans and other malicious software may be written to target a specific sector, but are often developed or leveraged to attack other sectors for additional purposes. Our attackers are looking for ways to be more efficient, so their ability to reuse these attacks on multiple sectors increases their efficiency. Our attackers share information related to their attacks. American businesses defending against cyberattacks need that same capability. The ability to share information across sectors and with the government is necessary to allow us to prepare effectively to recognize or respond to these attacks that hit across sectors. As our adversaries evolve, techniques become more complex, and coordinated attacks take place, we need to advance our ability to respond in a collective, coordinated fashion.

The ability to share information more broadly is critical to our response to future attacks. While we constantly review opportunities to improve the information shared within our industry, it is vital that our efforts also include sharing information across sectors and between the government and the private sector. Each company and public sector entity has a piece of the puzzle and an understanding of the threat. Our ability to share this information will greatly increase our preparation and response to threats.

Sharing of Data and Privacy

While we discuss the ability to share information, it is essential that we understand what information is being shared to ensure that we do not infringe on individuals rights to privacy. The reality is that the data being shared on threats are the technical details of malware, sources of malicious attacks and warnings of potential attacks (i.e. 'ones and zeros'). If we were comparing this to the world of physical crime, one could think of it as the sharing of ballistic data or modi operandi – information that does not relate to an individual, but that is important to understand both the criminal activity and to stop future risk. We need to consider too how we currently share alleged criminal actor information today when we respond to physical crimes. For example, if we have a surveillance photo of an individual who is suspected of committing a crime, we do not hesitate to post his or her photo in post offices, publicize on news shows or send to local police offices. That is not to suggest

individuals' privacy rights should be violated, but to suggest that if we use the model society uses to share information about physical crimes, we could advance the ability to share this information of known infiltrators to others, so that we do not fall victim to preventable attacks.

Securing Data

There are unfortunately many ironies when it comes to cybercrime. Unlike physical crime where we have evolved to recognizing the rights of the victim, when it comes to cybercrime, too often the victim is made to bear the blame for cyberattacks. Regardless of how much investment the victim has made to defend itself or how quickly it acted to fend off the attack, victims remain concerned about broadly reporting the crime or sharing details. They are concerned that they will be held liable for an attack against them regardless of the defenses they mounted or that it will publicly affect their reputation even in situations where they have fended off or stopped an attack. Likewise, there is a real concern by those who share data that a public disclosure of that sharing actually incites cyber attackers to target them even more as an act of revenge. Therefore, it is critical to assure that shared cyberattack data is properly protected and to provide organizations that do share with hold harmless protection. As we are an industry based on trust, it is essential that we continue to have the trust of consumers. It would harm the industry as a whole, if attacks successfully stopped by a specific institution were publicly disclosed. Ironically, though, sharing information even on these stopped attacks helps others, in the industry and beyond, to prevent such attacks from being successful against them.

Conclusion

In closing, please accept my thanks for the opportunity to testify to the Committee. We support the introduction of the Cyber Intelligence Sharing and Protection Act and look forward to working with the Committee Chair and Ranking Member on moving this bill forward.

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