Testimony of

Charles Blauner

On behalf of the

American Bankers Association

before the

Energy and Commerce Committee

of the

United States House of Representatives

Testimony of Charles Blauner

On behalf of the

American Bankers Association

before the

Committee on Energy and Commerce

of the

United States House of Representatives

May 21, 2013

Chairman Upton, Ranking Member Waxman, my name is Charles Blauner, Global Head of Information Security for Citi. In that capacity, I set Citi's information security strategy and am accountable for Citi's information security risk posture across all lines of business, functions, and regions. I appreciate the opportunity to be here today representing the American Bankers Association (ABA), which represents banks of all sizes and charters and is the voice for the nation's $14 trillion banking industry and its two million employees.

I would like to begin by commending the House for its recent passage of the Cyber Intelligence Sharing and Protection Act (CISPA). This legislation, if enacted, will greatly facilitate information sharing regarding the serious threats to our nation's critical infrastructures. We are also supportive of the Administration's executive order, which provides important direction to both the public and private sector, and like CISPA aims to enhance our nation's cybersecurity protections.

In addition to my role at Citi I am proud to currently serve as the Chairman of the Financial Services Sector Coordinating Council (FSSCC), which is the coordinator for Financial Services for the protection of critical infrastructure, focused on operational risks. Citi is extremely supportive of the FSSCC and its sister organization, the Financial Service Information Sharing and Analysis Center (FS-ISAC). ABA has also been deeply involved in these two organizations since their inception, and will be represented as the Vice Chair of the FSSCC starting in July of this year while continuing to serve on the FS-ISAC board. Companies and associations taking on these roles are but one example of the high level of collaboration within our sector when it comes to cybersecurity.

Cybersecurity is a top priority for banks and other financial services companies. We have invested an enormous amount of time, energy and resources to put in place the highest level of security among critical sectors, and we are subject to the most stringent regulatory requirements.

The public-private partnership has been critical to protecting firms in our industry against cyber threats and we pledge to continue this collaboration to further our mutual goals.

My testimony today focuses on four key points:

- How the organization and regulation of the financial services sector bolsters cybersecurity and reduces the risks associated with cyber attacks;

- How the development and implementation of the National Institute of Standards and Technology (NIST) Cybersecurity Framework should leverage existing standards, regulations, and processes;

- How timely cross-sector public-private information sharing is the key to cybersecurity protection; and lastly,

- What foundational work needs to be done to support our shared goal of enhanced cybersecurity.

I. The Organization and Regulation of the Financial Services Sector Bolsters Cybersecurity

As Congress and the Administration contemplate changes to the national cybersecurity framework, it is important to consider the cybersecurity measures collaboratively taken by our sector, through the operations of the FSSCC and the FS-ISAC—the private side of our sector—in conjunction with the Financial and Banking Information Infrastructure Committee (FBIIC)—the public side. Also important are the stringent laws and regulations within the financial services sector. This, along with our longstanding working relationship with the U.S. Department of the Treasury (our sector-specific agency regarding critical infrastructure protection) has been very effective.

Let me briefly describe the key components of the public-private partnership.

Financial Services Sector Coordinating Council: FSSCC's mission is to strengthen the resiliency of the financial services sector against attacks and other threats to the nation's critical infrastructure. The Council has 55 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.[1] During the past decade the partnership has continued to grow, both in terms of the size and commitment of its membership as well as 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. At a sector level, FSSCC's role is focused on strategy and policy.

Financial Service Information Sharing and Analysis Center: The FS-ISAC was established by the financial services sector in response to the Presidential Directive 63 of 1998. That directive—later updated by the Homeland Security Presidential Directive 7 in 2003—mandated that the public and private sectors share information about physical and cyber security 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. Compared to the FSSCC, the FS-ISAC's primary role is operational.

Financial and Banking Information Infrastructure Committee: FBIIC, led by Treasury and chartered under the President's Working Group on Financial Markets, is charged with improving coordination and communication among financial regulators, enhancing the resiliency of the financial sector, and promoting the public/private partnership. Essential to the FSSCC's success is the public sector's commitment to the public-private sector partnership outside of the already mature regulatory regime.

The deep involvement of ABA and Citi in both the FSSCC and the FS-ISAC is not unusual within the financial services sector. Many financial organizations are heavily involved in both. ABA, which represents banks of all sizes and types, has been a primary driver behind expanding the FS-ISAC's reach from under 100 in 2004, to over 4,000 member firms today to ensure that vital cyber threat information and the means to manage those threats reaches as many financial organizations as possible.

[1] A listing of FSSCC members is contained in Appendix 1.

The financial services sector develops and implements leading practices through the FSSCC, the FS-ISAC and the FBIIC. For example, under the joint partnership of the FSSCC and FBIIC, our sector has developed leading practices to assess and mitigate risks associated with the resiliency of the telecommunications infrastructure including critical undersea cables, pandemic flu preparations, and other important risks or threats facing the security and resilience of the sector.

The most recent example of the high degree of interaction and collaboration between these bodies is our sector's unified response to cyber attacks that have targeted the U.S. financial services sector since September, 2012. These attacks, against an increasing number of financial organizations, have at times impacted availability of consumer internet banking websites. From the very start of these attacks, the FS-ISAC was able to organize the affected organizations into a group to collaborate in real-time on measures to mitigate the attacks. Individual organizations were able to, through FBIIC and Treasury, request specific governmental technical assistance as necessary. Due to the tight relationship between the FS-ISAC and the FSSCC, actions such as these are factored into the actions taken by the FSSCC as the Council makes and refines legislative and administrative policy recommendations.

While the financial services sector is effectively organized for critical infrastructure protection purposes, the sector is also subject to federal and state laws, regulations, guidance, and examination standards relating to cybersecurity, many of which emanate from the general financial safety and soundness standards and customer information security provisions contained within the Gramm-Leach-Bliley Act of 1999. For example, financial institutions must comply with guidance produced by the Federal Financial Institution Examination Council (FFIEC), an organization made up of the agency heads of all the depository institution regulators. This guidance sets the standards for financial institution's information systems, outlining the minimum control requirements and directing a layered approach to managing information risks.

Likewise, the Securities and Exchange Commission (SEC) and the self-regulatory organizations (SROs), such as the Municipal Securities Rulemaking Board (MSRB), the Financial Industry Regulatory Authority (FINRA), and the National Futures Association (NFA), review the cybersecurity programs of exchanges, broker-dealers and clearing organizations as part of their ongoing supervisory exams and related activities. Insurance companies' privacy and security programs are subject to review by state insurance regulators. Health and long-term care insurers'

privacy and security programs also are subject to review by the Department of Health and Human Services (HHS).

As I will discuss in greater detail later in this statement, and as a recent GAO report outlines, financial sector regulations, guidance, and examination standards are substantially similar to the National Institute of Standards and Technology (NIST) Special Publication 800-53, mapping essentially to all of the recommended controls for federal information systems.[2] ***This is an extremely important point, as a key FSSCC recommendation regarding implementation of the NIST Cybersecurity Framework is that existing audit and examination processes be leveraged and complementary, and not have redundant audit requirements.***

II. Development and Implementation of the NIST Cybersecurity Framework Should Leverage Existing Standards, Regulations, and Processes

ABA continues to support the efforts 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 the Executive Order and believe implementation of the Cybersecurity Framework envisioned in the Order can be an important tool in improving our nation's overall cybersecurity.

NIST has said that, in conducting its work, it will consider integration of standards with existing frameworks. To this end, ***ABA believes it is particularly important that NIST's efforts to develop a Cybersecurity Framework complement and build upon existing cybersecurity standards adopted by the U.S. financial services industry.*** As already noted, the financial sector's critical infrastructure is subject to a significant number of federal and state laws, regulations, guidance, and examination standards relating to cybersecurity. We also agree with NIST that an important objective of its efforts should be to encourage widespread adoption of the Cybersecurity Framework across critical industries, as the financial industry's cybersecurity is contingent on the safety and security of other critical sectors, such as telecommunications and energy.

---

[2] GAO, *Critical Infrastructure Protection: Cybersecurity Guidance Is Available, but More Can Be Done to Promote Its Use*, GAO-12-92 (Washington, D.C.: December 9, 2011).

[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.

Collaboratively, through the FSSCC, ABA is committed to working with NIST in formulating and implementing this Framework and offers the following recommendations to improve cybersecurity to meet our mutual goals:

- **Develop sector-specific frameworks for protecting critical infrastructure.** Instituting a centralized Cybersecurity Framework would not be effective in recognizing the unique nature of and levels of protection within each critical sector. We strongly recommend that each Sector Coordinating Council take the lead in developing a framework that is specific to that sector so that critical infrastructure can be identified in a manner that is repeatable, transparent, and predictable.
- **Leverage primary regulatory authorities.** Any Cybersecurity Framework should ensure that each sector's primary regulatory authorities remain independent as the overseer and enforcement body for the critical sectors they regulate. This is necessary to ensure that the business continuity, resiliency, and critical infrastructure protection regulations that primary regulators enforce form the basis of any critical infrastructure protection standards imposed on that sector.
- **Leverage existing audit and examination processes and, encourage complementary, not redundant audit requirements when building voluntary cybersecurity practices.** Any Cybersecurity Framework should recognize that financial sector critical infrastructure firms already undergo extensive audits both internally and by third parties, of existing cybersecurity standards. We have, and continue to recommend, that any voluntary practices be consistent with existing financial sector regulatory requirements. 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 a Framework may be induced through incentives, such incentives should be tailored to address specific gaps within the market or provide benefits to a sector (or a portion thereof). To be effective they must be compelling enough to affect corporate investment behavior and be adaptable across sectors and business functions, allowing for a menu of incentives and not mandating a one size fits all approach. In addition, the

implementation of the Framework must provide benefits to firms that adopt it by reducing their compliance costs and minimizing the risk of legal action based on its application.[4]

Using the financial services sector as an example, it is widely acknowledged that the sector's existing regulatory requirements will ***exceed*** the baseline cybersecurity standards that NIST will ultimately recommend for the Framework. If the primary federal financial regulatory agencies come to this determination, as the Executive Order specifies, how can that determination be leveraged as part of or in lieu of a separate certification process? ***To not leverage the existing regulatory process as part of the certification process risks the development of a compliance exercise rather than a process that actually enhances cybersecurity for the organization.***

III. Timely Cross-Sector Information Sharing Throughout the Public-Private Partnership is Key to Cybersecurity Protection

As I have outlined, the financial services sector currently shares a significant level of threat data between institutions and across the sector through the FS-ISAC. We believe that existing information sharing and analysis mechanisms, such as those provided by the FS-ISAC, play a vital role in incident response coordination, information sharing and other operational activities for the financial services sector. Improving and encouraging information sharing is central to protecting the financial services sector and the nation.

A key factor in the success of information sharing in the financial services sector is trust. And trust takes time to develop. The ABA, FS-ISAC and FSSCC have worked hard to facilitate development of trust between its members, with other organizations in the financial services sector, with other sectors, and with government organizations such as law enforcement, regulators, and intelligence agencies for over a decade. Trust cannot be legislated, trust must be earned and we cannot afford to do anything that damages the levels of trust that have already been established.

It is of utmost importance to increase the volume, timeliness, and quality of threat information shared by U.S. law enforcement and intelligence agencies with private sector entities so that they may better protect themselves against cyber threats. We also support the intention of CISPA and the Executive Order to improve information sharing between the public and private sectors, and

[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/fssc_response_-_doc_noi.pdf.

especially the ability to more rapidly disseminate classified reports to entities authorized to receive them. We need our Government partners to expedite the processing of security clearances, and to declassify and more broadly disseminate threat information critical to enhancing our nation's ability to protect itself from cyber threats.

In June 2011, the FS-ISAC became the third ISAC to participate in the Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC). FS-ISAC representatives, cleared at the Top Secret / Sensitive Compartmented Information (TS/SCI) level, attend daily briefs and meetings to share information on threats and vulnerabilities. The presence at the NCCIC has greatly enhanced situational awareness and information sharing between the financial services sector and the government.

Again, ABA commends the House for passing the Cyber Intelligence Sharing and Protection Act. The timely, voluntary sharing of threat information is critical to the government and the private sector in developing and deploying protective measures and countermeasures against malicious cyber activity. While the cyber threat data that is shared by the financial services sector is machine language and not attributable to an individual, the provisions in the bill concerning liability protections for the sharing of information are extremely important and transcend our sector. This legislation provides important clarifications that will help facilitate increased cyber intelligence information sharing between the private and public sectors. We hope that this important piece of legislation will be signed into law.

IV. Foundational Work Needs to be Done to Support our Shared Goal of Enhanced Cybersecurity

Protecting our nation's critical infrastructure, including the Financial Services Sector, from the rapidly evolving cyber threat requires the ongoing development of technical capabilities and skilled resources which do not exist today.

The development of technical capabilities relies on a robust program of Research and Development (R&D) that can quickly yield new commercial products that can be leveraged to protect individual firms as well as critical shared infrastructure. To support this goal the FSSCC has published an "R&D Agenda" to help guide research sponsored by governmental agencies as well as universities and the private sector.

Beyond technical capabilities, another critical success factor is the availability of skilled resources. Simply put, demand for those resources outstrips supply today. In order to successfully meet the challenges posed, a coordinated effort is required to develop a skilled workforce that is up to the task of defending our nation and the Financial Services Sector from today's and tomorrow's cyber threats.

V. Conclusion

Cybersecurity is a top priority for banks and other financial services companies. We have invested an enormous amount of time, energy and resources to put in place the highest level of security among critical sectors, and we are subject to stringent regulatory requirements. We look forward to continuing to work with Congress and the Administration toward our mutual goal of protecting our nation's critical infrastructure.

Appendix One

Financial Services Sector Coordinating Council Membership

The Financial Services Sector Coordinating Council (FSSCC) fosters and facilitates financial services sector-wide activities and initiatives designed to improve Critical Infrastructure Protection and Homeland Security. The Council was created in June 2002 by the private sector, with recognition from the U.S. Treasury, to coordinate critical infrastructure and homeland security activities in the financial services industry.

Associations	Operators	Utilities and Exchanges
American Bankers Association	Allstate	BATS Exchange
American Council Life Insurers	Bank of America	CLS Services
American Insurance Association	BNY Mellon	CME Group
ASIS International	Citi	Direct Edge
BAI	Equifax	DTCC
	Fannie Mae	Intercontinental Exchange
BITS	Fidelity Investments	International Securities Exchange
ChicagoFIRST	Freddie Mac	NASDAQ
Consumer Bankers Associations	Goldman Sachs	National Stock Exchange
Credit Union National Association	JPMorgan Chase	NYSE Euronext
Financial Information Forum	MasterCard	Omgeo
FS-ISAC	Morgan Stanley	Options Clearing Corporation
Futures Industry Association	Navy Federal	The Clearing House
Independent Community Bankers Association	Northern Trust	
Investment Company Institute	PayPal	
	RBS	
Managed Funds Association	Sallie Mae	
NACHA	State Farm	
National Association of Federal Credit Unions	State Street	
National Armored Car Association	SunTrust	
National Futures Association		
SIFMA	Visa	
	Wells Fargo	