STATEMENT

OF

BITS PRESIDENT LEIGH WILLIAMS
ON BEHALF OF THE FINANCIAL SERVICES ROUNDTABLE

BEFORE THE

SUBCOMMITTEE ON INTELLECTUAL PROPERTY,
COMPETITION AND THE INTERNET
AND SUBCOMMITTEE ON CRIME, TERRORISM AND HOMELAND SECURITY
OF THE JUDICIARY COMMITTEE
OF THE U.S. HOUSE OF REPRESENTATIVES

JOINT OVERSIGHT HEARING ON
CYBERSECURITY: INNOVATIVE SOLUTIONS TO CHALLENGING PROBLEMS

MAY 25, 2011

TESTIMONY OF LEIGH WILLIAMS, BITS PRESIDENT

Thank you Chairman Goodlatte, Chairman Sensenbrenner, Ranking Member Watt, and Ranking Member Scott for the opportunity to testify: first, on the financial services industry's commitment to cybersecurity; second, on the need for cybersecurity legislation; and third, in support of the Administration's cybersecurity proposal.

My name is Leigh Williams and I am president of BITS. As 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.

Financial Services Commitment to Cybersecurity

Given BITS' role in the financial services community, I have a firsthand appreciation for the industry's commitment to cybersecurity. The reliability of our systems, integrity of our data, and the continued confidence of our customers are absolute requirements at the level of individual institutions and the industry as a whole. I often hear professionals at all levels - from cybersecurity professionals to chief information officers to chief executives - attest that their institutions treat cybersecurity as an internally-driven business imperative, not an externally-imposed compliance mandate. Just last week, in a small meeting of chief information security officers, one phrased it this way: "Good risk management drives good practices. Good practices then result in compliance. Not the other way around."

At the industry level, BITS and several other coalitions facilitate a continuous process of sharing expertise, identifying and promoting best practices, and making these best practices better, to keep pace in a dynamic environment. For example, as BITS and our members execute against our 2011 business plan, we are addressing:

- Security standards in mobile financial services.
- Protection from malicious or vulnerable software.
- Security in social media.
- Cloud computing risks and controls.
- Email security and authentication.

- Security training and awareness.

In several other 2011 initiatives, BITS is working closely with our private sector and public sector partners:

- The Cyber Operational Resiliency Review (CORR) pilot, in which institutions may voluntarily request Federal reviews of their systems, in advance of any known compromise - with the Department of Homeland Security (DHS) and our Sector Specific Agency, the U.S. Department of the Treasury.
- Multiple strategies for enhancing the security of financial Internet domains - with the Internet Corporation for Assigned Names and Numbers (ICANN), the American Bankers Association (ABA) and Verisign.
- Cybersecurity exercises - with the forty-five institutions, utilities and associations of the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC) and the seventeen agencies of the Finance and Banking Information Infrastructure Committee (FBIIC).
- A comprehensive strategy for preventing, detecting and responding to account takeover - led by the Financial Services Information Sharing and Analysis Center (FS-ISAC), and joined by a strong contingent of institutions, associations and agencies.
- A credential verification pilot - with DHS and the Department of Commerce – building on private sector work that began in 2009, was formalized in a FSSCC memorandum of understanding in 2010, and was featured in the April 15, 2011 announcement of the National Strategy for Trusted Identities in Cyberspace (NSTIC).

In these representative initiatives from BITS' 2011 plan, and in many other efforts, the financial institutions, utilities, associations, service providers and regulators continue to demonstrate a serious, collective commitment to strengthening the security and resiliency of the overall financial infrastructure. As Congress considers action on cybersecurity, I urge Members to be conscious of the protections already in place and the collaborations currently underway, and to leverage them for maximum benefit.

Need for Legislation

Even given this headstart and substantial momentum, we believe that cybersecurity legislation is warranted. Strong legislation can catalyze systemic progress in ways that are well beyond the capacity of individual companies, coalitions or even entire industries. For example, comprehensive legislation can:

- Raise the quality and consistency of security throughout the full cyber eco-system, including the telecommunications networks on which financial institutions depend.

- Enhance confidence among U.S. citizens and throughout the global community.
- Strengthen the security of Federal systems.
- Mobilize law enforcement and other Federal resources.
- Enable and incent voluntary action through safe harbors and outcome-based metrics, rather than relying primarily on static prescriptions.

Attached to my testimony is a list of thirteen policy approaches that the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC) recently endorsed, along with three that it deemed problematic. For additional detail on the FSSCC's recommendations and its active role in cybersecurity, I refer the Committee to the April 15, 2011 testimony of FSSCC Chair, Jane Carlin, before the Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies of the House Homeland Security Committee. I urge the Judiciary Committee to consider the FSSCC's input, particularly in light of its leadership of the financial services industry on this issue.

Obama Administration Proposal

On May 12, 2011, on behalf of the Administration, the Office of Management and Budget transmitted to Congress a comprehensive legislative proposal to improve cybersecurity. The Financial Services Roundtable supports this legislation and looks forward to working for its passage. We support many of the provisions of this proposal on their individual merits, and we see the overall proposal as an important step toward building a more integrated approach to cybersecurity. Given that our member institutions operate nationally, are highly interdependent with other industries, and are already closely supervised by multiple regulators, we appreciate that this proposal promotes uniform national standards, throughout the cyber eco-system, with the active engagement of Sector Specific Agencies and sector regulators.

Recognizing that much of the legislative debate will begin to coalesce around the Administration's proposal, I will structure the remainder of my testimony as a brief commentary on its key provisions.

Law Enforcement

We support the proposal's clarification and strengthening of criminal penalties for damage to critical infrastructure computers, for committing computer fraud, and for the unauthorized trafficking in

passwords and other means of access. We also urge similar treatment for any theft of proprietary business information. With this extension, the law enforcement provisions will improve protections for both consumers and institutions, particularly when paired with expanded law enforcement budgets and the recruitment of personnel authorized in later titles. For purposes of this section and others, we presume that many, but not all, financial services systems and entities will be designated as critical infrastructure vital to national economic security, and we look forward to further work on the associated criteria.

Data Breach Notification

We support the migration to a cross-sector, uniform national standard for breach notification. Given existing state and financial services breach notification requirements, this migration will require both strong pre-emption and a reconciliation to existing regulations and definitions of covered data (please see the Federal Financial Institutions Examination Council Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice 2005-13). We support the exemptions for data rendered unreadable, in breaches in which there is no reasonable risk of harm, and in situations in which financial fraud preventions are in place. While we recognize that additional legislative and regulatory work remains on the notification issue, we see the essential approach as highly constructive, and we look forward to heightened accountability throughout the cyber eco-system.

DHS Authority

We support strengthening cybersecurity authorities within DHS – and the active collaboration of DHS with the National Institute of Standards and Technology (NIST), Sector Specific Agencies such as the Treasury Department, and sector regulators such as our banking, securities and insurance supervisors. This section demonstrates both the Administration's commitment to an integrated approach and the challenge of achieving it. Federal and commercial systems, financial and non-financial information, DHS planning and sector coordinating council collaboration, are all addressed here and all will need to be very carefully integrated. Within financial services, we are conscious of the many current mechanisms for oversight, information-sharing and collaboration, but we are also conscious of the need for better alignment with our partners in other sectors. We look forward to further work in this area of integration and harmonization, at both the legislative and implementation stages.

We also believe that two areas mentioned in this section – fostering the development of essential technologies, and cooperation with international partners – merit considerably more attention. As DHS

and NIST pursue their research and development agenda, and as the Administration pursues its recently announced International Strategy for Cyberspace, we hope to see substantial resource commitments and advances in these areas.

Regulatory Framework

We support all of the purposes of this section, including, especially: the consultation among Sector Specific Agencies, regulators and infrastructure experts; and the balancing of efficiency, innovation, security and privacy. We recognize that giving DHS a window into financial services' cybersecurity risks, plans and incident-specific information is an important element of building a comprehensive solution. Reconciling all of these elements – Treasury and our regulators' sector-specific roles, Homeland Security's integration role, and the dual objectives of flexibility and security – will be critically important if we are to capitalize on existing oversight, avoid duplication, and avoid the hazards of public disclosures of sensitive information.

Federal Information Security Policies

We are encouraged by the proposal of a comprehensive framework for security within Federal systems. As institutions report more and more sensitive personal and financial data to regulators (and directly and indirectly to DHS), it is critically important that this data be appropriately safeguarded. Protecting this data, modeling best practices, and using Federal procurement policies to expand the market for secure products, are all good motivations for adopting these proposed mandates.

Personnel Authorities

Because we recognize how difficult it is to recruit the most talented cybersecurity professionals, we support the expanded authorities articulated in this section. We particularly support reactivating and streamlining the program for exchanging public sector and private sector experts.

Data Center Locations

Consistent with our view of financial services as a national market, we support the presumption that data centers should be allowed to serve multiple geographies. We encourage Congress to consider extending this logic for interstate data centers to the international level, while recognizing that the owners, operators and clients of specific facilities and cloud networks must continue to be held accountable for their security, resiliency and recoverability, regardless of their geographic location or dispersion.

Conclusion

The Financial Services Roundtable and its members are fully committed to advancing cybersecurity and resiliency, and we very much appreciate your attention to this issue. To ensure ongoing progress on cybersecurity, the Roundtable will:

- Continue to facilitate collective security initiatives among its members and with its network of public and private sector partners.
- Support legislation that both improves the security of the overall cyber eco-system and leverages existing financial services protections.
- Collaborate with policymakers to refine, pass and implement the Administration's cybersecurity proposal.

Thank you for your time. I would be pleased to answer any questions you may have.

Financial Services Cybersecurity Policy Recommendations

Financial Services Sector Coordinating Council – April 15. 2011

Policy Approaches the FSSCC Supports:

- Federal leadership on a national cyber-security framework, implemented with the active involvement, judgment and discretion of Treasury and the other Sector Specific Agencies (SSAs).
- Commitment to two-way public/private information-sharing, leveraging the Information Sharing and Analysis Centers (ISACs), the US-CERT, safe harbors, clearances, and confidentiality guarantees. This must include sharing of actionable and timely information.
- Support focused efforts to address critical interdependencies such as our sector's reliance on telecommunications, information technology, energy and transportation sectors. Continue to leverage and expand on existing mechanisms (e.g., NSTAC, NIAC, PCIS).
- Involvement of Treasury and other SSAs in cyber emergencies.
- Federal cyber-security supply chain management and promotion of cyber-security as a priority in Federal procurement.
- Public education and awareness campaigns to promote safe computing practices.
- Attention to international collaboration and accountability in law enforcement, standards, and regulation/supervision.
- Increased funding of applied research and collaboration with government research agencies on authentication, access control, identity management, attribution, social engineering, data-centric solutions and other cyber-security issues.
- Increased funding for law enforcement at the international, national, state and local levels and enhanced collaboration with financial institutions, service providers and others that are critical to investigating cyber crimes and creating a better deterrent.
- Heightened attention to ICANN and other international Internet governance bodies to enhance security and privacy protection.
- Strengthening of government-issued credentials (e.g. birth certificates, driver's licenses and passports) that serve as foundation documents for private sector identity management systems.
- Enhanced supervision of service providers on whom financial institutions depend (e.g. hardware and software providers, carriers, and Internet service providers).
- Recognize the role of Federal financial regulators in issuing regulations and supervisory guidance on security, privacy protection, business continuity and vendor management for financial institutions and for many of the largest service providers.

Policy Approaches the FSSCC Opposes:

- Detailed, static cyber-security standards defined and maintained by Federal agencies in competition with existing, private standard-setting organizations.
- Establishment of vulnerability, breach and threat clearinghouses, unless security and confidentiality concerns can be definitively addressed.
- Sweeping new authority for Executive Branch to remove access to the Internet and other telecommunications networks without clarifying how, when and to what extent this would be applied to critical infrastructure.