STATEMENT

OF

BITS PRESIDENT LEIGH WILLIAMS
ON BEHALF OF THE FINANCIAL SERVICES ROUNDTABLE

BEFORE THE

UNITED STATES SENATE COMMITTEE ON
BANKING, HOUSING, AND URBAN AFFAIRS

CYBERSECURITY AND DATA PROTECTION IN THE FINANCIAL SECTOR

JUNE 21, 2011

TESTIMONY OF LEIGH WILLIAMS, BITS PRESIDENT

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

My name is Leigh Williams and I am 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.

From this perspective, I will briefly describe cybersecurity and data protection in financial services, including private sector efforts, sector-specific oversight and inter-sector interdependencies. I understand that the Committee is considering the cybersecurity legislative proposal delivered by the Obama Administration to the President of the Senate on May 12. I will explain why The Financial Services Roundtable supports that proposal, and I will comment on how the proposal can best leverage our current protections.

Financial Institutions' Voluntary Cybersecurity Efforts

In my view, within the financial services sector, the greatest amount of cybersecurity protection arises from voluntary measures taken by individual institutions for business reasons. To protect their retail customers, commercial clients and their own franchises, industry professionals – from Chief Information Security Officers to CIOs to CEOs – are increasingly focused on safeguards, investing tens of billions of dollars in data protection. They recognize the criticality of confidentiality, reliability and confidence to their success in the marketplace. This market-based discipline is enforced through an increasingly informed consumer base, and by a very active commercial clientele that often specifies security standards and negotiates for audit and notification rights.

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 implement our 2011 business plan, we are addressing the following items associated with protecting customer data:

- 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.
- Prevention of retail and commercial account takeovers.
- Security training and awareness.

While all of this institution-level and industry-level effort is voluntary – not driven primarily by regulation – it is not seen by industry executives as discretionary or optional. The market, good business practices and prudence all require it.

Oversight

To strengthen public confidence and to ensure consistency across a wide variety of institutions, self-regulatory organizations and government agencies codify and enforce a comprehensive system of requirements. Many of these represent the distillation of previously voluntary best practices into legislation introduced in this Committee, enacted into law, detailed in regulation, enforced in the field, with feedback to the Committee.

For example, Members of this Committee are very familiar with the provisions of Gramm-Leach-Bliley, the Financial Services Modernization Act of 1999 (GLB). GLB fostered the promulgation of Regulation P by the Federal Financial Institutions Examinations Council (FFIEC) and Regulation S-P by the Securities and Exchange Commission (SEC). These regulations were translated into examination guidance. That guidance is consulted by institutions as they manage security and privacy programs, comprised of risk assessments, strategic plans, control teams, authentication technologies, customer notices and many other elements. These elements are then audited by on-site examiners, who enforce the underlying requirements and promote safety and soundness in the institutions and across the industry. The sector-wide impact is assessed by our sector-specific agency, the U.S. Department of the Treasury. Finally, bringing the process full circle, this Committee oversees the agencies.

In addition to these Federal authorities, institutions are subject to self-regulatory organizations like the Financial Industry Regulatory Authority (FINRA), state regulators like the banking and insurance commissioners, independent auditors, outside Directors, and others.

These various oversight bodies, in addition to applying GLB, also apply the Fair and Accurate Credit Transactions Act (FACTA), Electronic Funds Transfers (Regulation E), Suspicious Activity Reporting (SARs), the International Organization for Standardization criteria (ISO), the Payment Card Industry Data Security Standard (PCI), BITS' own Shared Assessments and many, many more regulations, rules, guidelines and standards.

Inter-Sector Collaboration

Commensurate with the escalating cybersecurity challenges and increasing interconnectedness among sectors, more and more of our work entails public/private and financial/non-financial partnerships. Our Financial Services Sector Coordinating Council (FSSCC) of fifty-two institutions, utilities and associations actively partners with the seventeen agencies of the Finance and Banking Information Infrastructure Committee (FBIIC). (For additional detail on the FSSCC's perspective on cybersecurity, research and development, and international issues, 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.) Our Financial Services Information Sharing and Analysis Center (FS-ISAC) is in constant communication with the Department of Homeland Security (DHS), law enforcement, the intelligence community and ISACs from the other critical infrastructure sectors, to address individual incidents and to coordinate broader efforts.

Other examples of collaboration with non-financial partners, drawn just from BITS' 2011 agenda, include:

- 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 DHS and the Treasury.
- Multiple strategies for enhancing the security of financial Internet domains - with the Internet Corporation for Assigned Names and Numbers (ICANN) and Verisign, in partnership with the American Bankers Association (ABA) and in consultation with members of the FFIEC.
- 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).

Through the processes and initiatives above and in many other efforts, 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 the Committee considers action on cybersecurity, I urge Members to be conscious of the protections and supervisory structures 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 ecosystem, 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 FSSCC recently endorsed, along with three that it deemed problematic. I urge the Committee to consider the FSSCC's input, particularly in light of the FSSCC's 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 ecosystem, with the active engagement of sector-specific agencies and sector regulators.

Consistent with its comprehensive approach, the proposal strives to address cybersecurity both at the level of the entire ecosystem and also within specific sectors. For example:

- The Law Enforcement title refers to damage to critical infrastructure computers, but also to mail fraud and wire fraud.
- The Data Breach Notification title refers to sensitive personally identifiable information and Federal Trade Commission (FTC) enforcement, but also more specifically to financial account numbers, credit card security codes, the Fair Credit Reporting Act (FCRA), and an exclusion for entities covered under the Health Information Technology for Economic and Clinical Health Act (HITECH).
- The DHS Cybersecurity Authority title naturally stresses DHS' role, but it also mentions "other relevant agencies" and sector coordinating councils.
- Finally, the Regulatory Framework title focuses largely on DHS leadership and standardized evaluations, but it also mentions ISACs and sector-specific regulatory agencies, and provides for sector-level exemptions.

We believe that harmonizing the comprehensive approach with the need to incorporate sector-specific mechanisms will be one of the most important challenges as the Congress considers this proposal. We urge the Committee and the full Congress to leverage existing financial services protections and circumstances, and their analogs in other sectors, while preserving the comprehensive quality of the proposal. We offer the following two approaches as illustrations:

- *Establish a uniform standard with specified exceptions:* In the Data Breach Notification title, the FTC could enforce the requirements enacted under this bill, but defer to sector-specific regulators where substantially similar sector-specific rules and guidelines already are in place (e.g. the FFIEC could continue to enforce its 2005 interagency guidance, and the Department of Health and Human Services could continue to enforce HITECH).
- *Preserve sector autonomy with centralized information aggregation and coordination:* In the Regulatory Framework title, rather than requiring DHS to list critical infrastructure entities for every sector, the sector-specific agencies could make that determination, just as the Financial Stability Oversight Council is responsible for designating Systemically Important Financial Institutions.

Given the likely fluidity of the overall solution, we cannot yet make a definitive recommendation for either approach. We do believe that this question of sector/ecosystem balance warrants careful deliberation.

I will structure the remainder of my testimony as a brief commentary on a few key provisions of the proposal.

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.

Data Breach Notification

We support the migration to a uniform national standard for breach notification. Given existing state and financial services breach notification requirements, this migration will require both strong pre-emption and reconciliation to existing regulations and definitions of covered data. 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.

DHS Authority

We believe that two areas mentioned in this section – fostering the development of essential technologies, and cooperation with international partners – merit considerable investment. As DHS and the National Institute of Standards and Technology (NIST), pursue their research and development agendas, and as the Administration pursues its recently announced International Strategy for Cyberspace, we hope to see substantial resource commitments and advances in these areas.

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 of customer data, regardless of the servers' 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 the Senate Banking Committee's attention to this issue. For our part:

- We will continue to strengthen security with our members and partners,
- We will help answer this question of ecosystem/sector balance,
- And we will work to 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.