

BITS

FINANCIAL SERVICES
R O U N D T A B L E

July 26, 2011

ATTN: Alan Carroll, Subcommittee Clerk

United States House of Representatives
Committee on Homeland Security
Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies
H2-176 Ford House Office Building
Washington, DC 20515

Re: Response to Questions Posed on July 11 to Leigh Williams, BITS President

Dear Chairman King and Ranking Member Thompson,

Thank you once again for the invitation to address the Committee on the important subject of cybersecurity. Outlined are our responses to the questions posed in the attached July 11 letter.

1. You describe a large number of items members of the financial services sector undertake with respect to cybersecurity.

a. Can you compare these activities with those of the other sectors?

We are not in a position to compare the quality or quantity of cybersecurity efforts in other sectors to financial services, but we can identify some similarities and differences. As a similarity, we recognize that individual companies in telecommunications and information technology invest heavily in cybersecurity and resiliency. We understand that one difference is that financial institutions may do more collaborative work because they are so technically and commercially interconnected and because regulations tend to promote standardization.

b. Which of these activities are the product of voluntary action by the BITS community and which are the result of federal or state regulations?

At the institution level, most BITS members' cybersecurity programs are primarily motivated by business and customer interests. Regulations sometimes reinforce these motivations, but also sometimes require slightly different solutions. For example, under Gramm-Leach-Bliley, banks are required to have security programs that incorporate specific elements and that are reviewed by their boards. Without the regulation, the vast majority of banks would still have plans, but perhaps with different mixes of elements, and with review processes specific to their governance strategies. At the industry level – in efforts such as the mobile,

cloud, social networking and malware efforts mentioned in our June 24 testimony – virtually all of the collaboration is purely voluntary.

c. What is the cost of complying with these activities?

We do not have a specific estimate of regulatory compliance costs in cybersecurity. We do believe, however, that elevated compliance costs can crowd out risk management spending and investments in innovation, and can increase costs to customers and reduce institutions' returns.

2. Under the Administration's proposal what new cybersecurity activities would BITS members undertake that they are not now doing?

Under the Administration proposal, there would be at least two ways in which BITS members could more effectively share information with other sectors. First, because other sectors could be prompted to produce more information and DHS would be tasked with aggregating it, there would be more information available to exchange with our colleagues in other sectors. Second, the safe harbor and confidentiality provisions would reduce the risk of actively sharing information with the other critical infrastructures and with DHS.

3. You are endorsing the Administration's legislative proposal, which does not carve out the financial sector from its reach.

a. With this endorsement is it safe to assume that the financial industry will not be lobbying for a carve-out or any special treatment if the Administration's proposal moves forward?

BITS does not intend to advocate for the financial services sector to be carved out. BITS and its members do believe that the existing financial regulatory frameworks and the proposed approach will have to be reconciled. As we testified, this could be accomplished, for example, by recognizing where substantially similar requirements already exist, by leaving substantial authority within the sector, by requiring DHS to work through the sector specific agencies and primary regulators, or by DHS delegating authority back to the sector specific agencies and primary regulators.

4. Your testimony praises the Administration's legislative proposal for a variety of things like coordinating with companies and other agencies; however, it was my understanding that most, if not all, these activities are currently going on without this legislation.

a. Which specific provisions of the Administration's proposal will cause BITS members to make security improvements beyond their current activities and why is legislation required to get the BITS membership to undertake these activities?

Yes, BITS members are already satisfying many of the requirements of the Administration's proposal. The value of the proposal does not arise primarily from BITS members individually improving their security programs. Much of the value arises from companies in multiple industries and federal agencies with various missions working in closer cooperation on common problems. We think this is happening reasonably well within our sector, but we see room for improvement between sectors.

b. How much will these legislatively mandated activities by BITS members improve security?

While the mandates in the proposal may improve BITS members' cybersecurity practices, we see much of the potential improvement coming from enabling more voluntary collaboration. For example, as noted above, we would anticipate improved information-sharing and consequently better collective security among multiple sectors, including financial services.

In closing, we reaffirm our commitment to addressing this critical issue, and thank the Committee for its active engagement. Please feel free to contact me with any further questions or concerns at 202-589-2440 or leigh@fsround.org.

Sincerely,

A handwritten signature in black ink, appearing to read "Leigh Williams". The signature is fluid and cursive, with a long, sweeping tail on the final letter.

Leigh Williams
President