BITS
FINANCIAL SERVICES ROUNDTABLE

Sent via e-mail
September 13, 2010

Diane Honeycutt
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899
cybertaskforce@doc.gov

BITS appreciates the opportunity to comment on the Department of Commerce's Notice of Inquiry on Cybersecurity, Innovation, and the Internet Economy.[1] We encourage the Department's efforts to enhance commercial cybersecurity practices in the non-critical infrastructure and key resources sectors. We share the Department's concern that the Internet must remain an open and trusted infrastructure for commercial entities and individuals, and to that end, we welcome the creation of the Internet Policy Task Force ("Task Force").

Although BITS primarily represents "critical infrastructure" institutions in the financial services industry, we are responding to the Department of Commerce's ("Department") request for information about cybersecurity, generally, and in recognition of the Department's query about how it can "improve its execution of core cybersecurity responsibilities, including those supporting critical infrastructure and key resources sectors." 75 *Federal Register* 44219.

We also recognize that the Internet fuels communication and commerce across all sectors. Therefore, protecting all sectors is vitally important.

While we support the Department's review of cybersecurity and innovation, we are mindful of the influence of the Department of Homeland Security on our members, and we encourage collaboration amongst the departments to ensure duplicative or contradictory requirements are not developed for institutions identified as part of the nation's critical infrastructure.

---

[1] BITS is the technology policy division of The Financial Services Roundtable, created to foster the growth and development of electronic financial services and e-commerce for the benefit of financial institutions and their customers. BITS focuses on strategic issues where industry cooperation serves the public good, such as critical infrastructure protection, fraud prevention, and the safety of financial services by leveraging intellectual capital to address emerging issues at the intersection of financial services, operations and technology. BITS' efforts involve representatives from throughout our member institutions, including CEOs, CIOs, CISOs, and fraud, compliance, and vendor management specialists. For more information, go to http://www.bits.org/.

Responses to Specific Questions

- ***Quantifying the Economic Impact.*** The industry appreciates the benefits of aggregated data on cybersecurity investments and losses from cyber incidents, but recognizes the difficulty in collection.

  Currently, institutions utilize internal tracking of cyber incidents to understand their losses. Institutions provide data to industry surveys and notice of events consortiums, such as the Financial Services Information Sharing and Analysis Center (FS-ISAC). We are aware the American Banking Association, VISA and MasterCard accumulate data and report estimates of fraud losses.

  A major challenge in reporting is the definition of cyber incidents and the specific costs to include when evaluating a fraud loss. The definitions of incident and costs to include differ across the financial services sector, and would be increased with the inclusion of additional sectors. BITS and the Financial Services Technology Consortium (FSTC), our affiliate division at The Financial Services Roundtable, collaborate in various ways with the Anti-Phishing Working Group (APWG). The APWG, along with the standards bodies, is standardizing definitions and reporting fields.

  It is important for the Task Force to consider current mechanisms to supply this data and ways to leverage available resources for improved cybersecurity, before developing a new method of reporting and evaluation.

  We note that the proper protection of this data will remain an essential element in establishing effective approaches in this area.

- ***Raising Awareness.*** Education and awareness of customers have been and continue to be important to the financial services sector. We encourage the efforts of the National Cyber Security Alliance to educate consumers through their Stay Safe Online campaign. BITS has worked with partner organizations, including the American Bankers Association (ABA), to develop education and awareness courses and pamphlets for customers. The BITS Security Awareness Subgroup meets regularly to discuss opportunities and challenges for raising awareness among financial institution customers and employees.

- ***Global Engagement.*** National law enforcement (e.g., USSS, FBI) continue to increase their efforts to engage their global partners in cybersecurity efforts. We recognize the need to continue to increase this collaboration to more effectively identify and trace attacks and disable threatening sites. Increased partnership of international law enforcement is critical to ensure fraudsters face criminal charges for their crimes and receive appropriate sentencing.

- ***Authentication/Identity (ID) Management.*** The financial services sector constantly evaluates and tests new techniques to increase authentication security to mitigate risks, such as strong authentication as defined by the Federal Financial Institutions Examination Council (FFIEC) guidance, *Authentication in an Internet Banking Environment*. Similarly, the American National Standard Institute (ANSI) is in the process of defining standards for

proof and verification of personal identity. We encourage other sectors to evaluate and utilize strong authentication.

In closing, we would like to reiterate our support for the Department of Commerce's review of cybersecurity challenges and innovation and the creation of the Internet Policy Task Force.

Thank you for your consideration of our comments. If you have any further questions or comments on this matter, please do not hesitate to contact Leigh Williams, BITS President at 202-589-2440 or Leigh@BITS.org.

Sincerely,

Leigh Williams
President