November 19, 2015

The Honorable Richard Burr
Chairman
Senate Select Committee on Intelligence
Washington DC 20510

The Honorable Dianne Feinstein
Vice Chairman
Senate Select Committee on Intelligence
Washington DC 20510

The Honorable Michael T. McCaul
Chairman
House Committee on Homeland Security
Washington DC 20515

The Honorable Bennie G. Thompson
Ranking Member
House Committee on Homeland Security
Washington DC 20515

The Honorable Devin Nunes
Chairman
House Permanent Select Committee
on Intelligence
Washington DC 20515

The Honorable Adam B. Schiff
Ranking Member
House Permanent Select Committee
on Intelligence
Washington DC 20515

Dear Chairman Burr, Vice Chairman Feinstein, Chairman McCaul, Ranking Member Thompson, Chairman Nunes, and Ranking Member Schiff:

On behalf of our member firms, the undersigned financial trade associations are writing to present our views as you prepare to go to conference on the House and Senate cyber threat information sharing bills. The financial services sector shares your goal of enacting legislation that would enhance voluntary cyber threat information sharing among the private sector and the Federal government. For several years now, we have supported your efforts to pass legislation in both the House and Senate and overall, we are very pleased that strong bipartisan legislation has advanced to this point in the process.

In general, we believe the House and Senate bills are consistent with the goal of enhancing our nation's ability to defend against cyber attacks. However, we have significant concern with Section 407 of the Senate bill (S. 754). This provision is simply at odds with the overall goal of a comprehensive, voluntary information sharing framework, and should it survive the process, could jeopardize our support for the underlying Conference Report. Moreover, we are concerned that this provision has not been adequately vetted in the same manner as the rest of the legislation and therefore could have unintended consequences that would impact the effectiveness of voluntary information sharing.

Section 407 directs the Department of Homeland Security (DHS) and other Federal entities to assess the security of critical infrastructure entities and develop a security strategy for each entity "to ensure that, to the greatest extent feasible" a cyber incident would not have catastrophic

consequences. DHS would then be required to report its assessment and strategy for each entity to several Congressional Committees.

This has nothing to do with voluntary information sharing and, unfortunately, will result in additional regulation of our industry by DHS. Although Section 407 has been cast simply as a "reporting" provision, it would instead function as a regulatory mandate in practice: DHS would be developing security standards for those entities that DHS has identified as critical infrastructure.

While we have strong concerns about Section 407 and urge you to remove it entirely from the final conference report, we are very hopeful that you will be able to bring the other elements of the House and Senate bills together in one legislative package that we can strongly support. This should include:

- Broad authorization for monitoring and sharing Critical Threat Indicators (CTIs) and defensive measures and the operation of defensive measures.
- Liability protections that enhance voluntary sharing of critical information.
- Strong anti-trust and FOIA protections.
- Flexible avenues for sharing information quickly and effectively with the Federal government.
- Effective avenues for the Federal government to share threat information as quickly as possible with the private sector.
- A balanced approach to privacy issues that takes into consideration the need to effectively share critical threat information.
- Strong safeguards against unnecessary or duplicative mandates and regulation.

The threat of cyber-attacks is a real and omnipresent danger to the financial services sector, our members' customers and clients and to critical infrastructure providers upon which we and the nation as a whole rely. Each of our organizations and our respective member firms has made the protection of customer sensitive information top priority and we are committed to continuing to work with the Congress and the Administration so that effective cyber threat information sharing legislation can be enacted into law as soon as possible. It is critical that Cybersecurity information sharing legislation be enacted before the next crisis, not after, and we look forward to continuing to work with you on this important issue.

Sincerely,

American Bankers Association
American Insurance Association
Consumer Bankers Association
Credit Union National Association
Electronic Transactions Association
Financial Services Roundtable

Independent Community Bankers of America
Investment Company Institute
NACHA – The Electronic Payments Association
National Association of Federal Credit Unions
National Association of Mutual Insurance Companies
Property Casualty Insurers Association of America
Securities Industry and Financial Markets Association
The Clearing House
U.S. Securities Markets Coalition: BATS Options, BOX Options Exchange, Chicago Board Options Exchange, International Securities Exchange, NASDAQ Options Market, NASDAQ OMX PHLX, NYSE Arca, NYSE Amex, The Options Clearing Corporation

CC: Members of the United States Senate
Members of the United States House of Representatives