November 12, 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
House Committee on Homeland Security
Washington DC 20515

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

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

The Honorable Adam B. Schiff
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:

The undersigned organizations thank you for your strong efforts to combat cyber threats and protect American businesses and citizens. The cybersecurity measures approved by the House and Senate would implement a legal framework critical to encourage industry to share voluntarily cybersecurity information with the federal government, helping to bolster efforts to guard against cyber-attacks.

However, we have significant concerns with Section 407 of S. 754, the Cybersecurity Information Sharing Act (CISA), which recently passed the Senate. This provision would require the Department of Homeland Security (DHS), relevant sector specific agencies (SSAs) and regulatory agencies to single out certain critical infrastructure entities and to report to Congress the extent of cybersecurity incident reporting by these entities. Section 407 would compel federal officials to assess the cybersecurity of these "covered" entities, develop a mitigation strategy for each of these entities and issue a recommendation to Congress whether to require a mandatory regulatory regime for the reporting of cyber intrusions by these entities to the government.

Section 407(b) runs counter to the *voluntary* nature of CISA and the House-passed bills as it would effectively coerce critical infrastructure entities to report cyber intrusions to DHS, SSAs and regulatory agencies by requiring that the data must be reported to Congress. We support and already engage in a strong voluntary partnership of information sharing with the U.S. Government that will grow stronger with the passage of CISA and the House bills.

Section 407(b) also presumes a deficiency in current cybersecurity capabilities of covered critical infrastructure entities. In fact, businesses are spending billions of dollars to counter cyber-attacks from nation-state adversaries, criminal organizations, and other malicious actors.

Section 407(c) would create de facto regulatory mandates, generate administrative burdens on critical infrastructure and potentially expose entities to liability. DHS, SSAs and regulatory agencies seemingly would have free rein to assess certain businesses' cybersecurity gaps and develop unilateral mitigation strategies for each critical infrastructure entity without input from industry. DHS and other agency requirements under Section 407 would not be synchronized with existing government rules and programs. Such DHS regulation has already been rejected several times by Congress and the Administration.

We strongly oppose Section 407 of the Senate-passed bill. As you work to reconcile the measures approved by the House and Senate, we respectfully urge that this provision be removed from the final version of the legislation.

We look forward to continuing to work with you on this specific issue and to safeguard U.S. businesses and the American people from cyber-attacks.

Sincerely,

American Bankers Association (ABA)
American Cable Association (ACA)
American Chemistry Council (ACC)
American Council of Life Insurers (ACLI)
American Fuel & Petrochemical Manufacturers (AFPM)
American Gas Association (AGA)
American Insurance Association (AIA)
American Petroleum Institute (API)
American Public Power Association (APPA)
American Water Works Association (AWWA)
ASIS International
Association of American Railroads (AAR)
Association of Metropolitan Water Agencies (AMWA)
CompTIA: Information Technology (IT) Industry & Association
Consumer Data Industry Association (CDIA)
CTIA – The Wireless Association
Edison Electric Institute (EEI)
Electronic Transactions Association (ETA)
Financial Services Roundtable (FSR)
GridWise Alliance
HITRUST- Health Information Trust Alliance
Information Technology Industry Council (ITI)
International Business Machines Corporation (IBM)
Large Public Power Council (LPPC)
National Association of Chemical Distributors (NACD)
National Association of Clean Water Agencies (NACWA)
National Association of Manufacturers (NAM)
National Association of Mutual Insurance Companies (NAMIC)
National Association of Water Companies (NAWC)
National Business Coalition on E-Commerce & Privacy
National Cable & Telecommunications Association (NCTA)
National Rural Electric Cooperative Association (NRECA)
NiSource Inc.
NTCA – The Rural Broadband Association
Property Casualty Insurers Association of America (PCI)
Security Industry Association
TechNet
Telecommunications Industry Association (TIA)
The Fertilizer Institute
The Options Clearing Corporation (OCC)
The Real Estate Roundtable
Transmission Access Policy Study Group (TAPS)
U.S. Chamber of Commerce
United States Telecom Association (US Telecom)
Utilities Telecom Council (UTC)
Water Environment Federation (WEF)

Cc: Members of the U.S. Congress