



**TELECOMMUNICATIONS
INDUSTRY ASSOCIATION**

1320 N. Courthouse Rd., Suite 200
Arlington, VA 22201 USA
www.tiaonline.org

Tel: +1.703.907.7700
Fax: +1.703.907.7727

February 25, 2015

The Honorable Michael McCaul
Chairman
House Committee on Homeland Security
Washington, D.C. 20510

The Honorable Bennie Thompson
Ranking Member
House Committee on Homeland Security
Washington, D.C. 20510

Dear Chairman McCaul and Ranking Member Thompson:

The Telecommunications Industry Association (TIA), the leading trade association for global manufacturers, vendors, and suppliers of information and communications technology (ICT), wishes to thank you for holding a hearing this week to examine the importance of successful information sharing in the protection of the United States from cybersecurity attacks, through your February 25, 2015 hearing titled "The Administration's Cybersecurity Legislative Proposal on Information Sharing." TIA and our member companies are committed to enhancing the national security through an improved ability for stakeholders to share timely cybersecurity information to improve detection, prevention, and mitigation of threats.

As the number and diversity of cyber-based threats to both businesses and the government continue to increase, it is more important than ever for Congress to act to enable the voluntary sharing of real-time bi-directional cybersecurity information amongst and between key government and industry partners (and their suppliers) by providing adequate liability protections while ensuring that an information sharing regime appropriately addresses privacy and civil liberties concerns. We underscore that liability protections are a crucial component of improved information sharing, and should provide needed legal clarity for organizations that need to share timely cyber threat information not only with the Department of Homeland Security's National Cybersecurity and Communications Integration Center (NCCIC) and designated information sharing and analysis organizations (ISAOs), but other key stakeholders as well. For example, TIA supported the Cyber Intelligence Sharing Protection Act (H.R. 3523) as well as the Cybersecurity Information Sharing Act of 2014 (S. 2588) in the previous Congress.

TIA also notes its support for existing public-private partnerships (many of which TIA and its members participate in heavily), as well as efforts of Federal agencies under existing laws and authorities, to facilitate information sharing and to improve cooperation in defense against cyber attacks. The actions of Congress in this space should augment and build upon the successes of these efforts.

Finally, TIA believes that information sharing should not be viewed as the end game. Rather, information sharing is a tool to achieve timely, reliable, and actionable situational awareness through information sharing, analysis, and collaboration. That is why it is important for Congress to, in addition to addressing information sharing, act in other important areas, such as to improve cybersecurity R&D, workforce training and education, and public awareness.

Thank you for your continuing hard work on this important national and economic security issue, and TIA looks forward to working with you moving forward.

Sincerely,

Scott Belcher
Chief Executive Officer
Telecommunications Industry Association