



Information Technology Industry Council

July 23, 2015

The Honorable Mitch McConnell
Majority Leader
United States Senate
Washington, D.C. 20510

The Honorable Harry Reid
Democratic Leader
United States Senate
Washington, D.C. 20510

Dear Majority Leader McConnell and Democratic Leader Reid,

On behalf of the members of the Information Technology Industry Council (ITI),¹ I write to express our support for S. 754, the Cybersecurity Information Sharing Act of 2015 (CISA), and urge you to bring it to the Senate floor for debate and vote. **Given the importance of cybersecurity threat information sharing to the high-tech industry, we will consider scoring votes in support of CISA in our 114th Congressional Voting Guide.**

ITI members contribute to making the U.S. information and communication technology (ICT) industry the strongest in the world in innovative cybersecurity practices and solutions. We firmly believe that passing legislation to help increase voluntary cybersecurity threat information sharing between the private sector and the federal government, and within the private sector, is an important step Congress can take to enable all stakeholders to address threats, stem losses, and shield their systems, partners and customers. It is important that the Senate act now to pass CISA and continue to move the legislative process forward, so that Congress can reconcile CISA with the House cybersecurity legislation, H.R. 1560, the Protecting Cyber Networks Act, and H.R. 1731, the National Cybersecurity Protection Advancement Act of 2015, and send a bill to the president.

ITI believes that legislation to promote greater cybersecurity threat information sharing should:

- Affirm that cybersecurity threat information sharing be voluntary;
- Promote multidirectional cybersecurity threat information sharing, allowing private-to-private, private-to-government and government-to-private sharing relationships;
- Include targeted liability protections;
- Utilize a civilian agency interface for private-to-government information sharing to which new liability protections attach;
- Promote technology-neutral mechanisms that enable cybersecurity threat information to be shared in as close to real-time as possible;
- Require all entities to take reasonable steps to remove personally identifiable information from information shared through data minimization; and
- Ensure **private** sector use of information received through private-to-private sharing is only for cybersecurity purposes, and **government** use of information received from the private sector is limited to cybersecurity purposes and used by law enforcement only:
 - For the investigation and prosecution of cyber crimes;

¹ **About ITI.** The Information Technology Industry Council (ITI) is the global voice of the tech sector. As the premier advocacy and policy organization for the world's leading innovation [companies](#), ITI navigates the relationships between policymakers, companies, and non-governmental organizations, providing creative solutions that advance the development and use of technology around the world. Visit www.itic.org to learn more. Follow us on Twitter for the latest ITI news [@ITI_TechTweets](#).

- For the protection of individuals from the danger of death or serious bodily harm and the investigation and prosecution of crimes involving such danger; and
- For the protection of minors from child pornography.

We appreciate the progress made by the Senate Intelligence Committee to include provisions that would protect personally identifiable information while also allowing for a cybersecurity threat information sharing framework that will enhance our ability to protect and defend our networks.

We look forward to working closely with you, your committee leadership, and the House of Representatives to further address outstanding issues in conference to ensure it adheres to our above cybersecurity threat information sharing principles. ITI remains committed to refining the legislation and supporting a final product that can best achieve our goal of promoting greater cybersecurity.

Sincerely,



Dean C. Garfield
President & CEO