Information Technology Industry Council

# ITI Position on Cyber Threat Information Sharing: February 2015

## Overview

***Protecting and defending networks is essential.*** Protecting and defending networks is essential to cybersecurity. A critical and commercially acceptable component of protection and defense is effective, voluntary sharing of information on cyber risks (such as threats, vulnerabilities, and incidents) with those who can help manage these threats, or who also might fall victim. The goal is to arm appropriate stakeholders with needed information to make decisions and take necessary actions to maintain situational awareness (know who is trying to get in, or who made it in, their networks), defend their networks, respond to threats and incidents (for example, block a certain threat or remediate it), and manage and mitigate cyber risks. These actions reduce potential costs to the entity in question and also will improve cybersecurity for the greater good, as additional entities can move more quickly to stem losses and protect their systems, partners, and customers.

Sharing is a tool, not an objective. Sharing relevant, actionable, and real-time cyber threat information with appropriate stakeholders enables them to take expeditious steps to address cyber threats from adversaries. If entities do not know the threats to their networks, it is much harder to protect or defend against them, or to even know if an incident has occurred. The sooner appropriate stakeholders have this information, the more quickly it can be used to help the broader cyber-ecosystem and the public at large, including to address cyber crime.

***What changes will help?***

Legal changes: Entities must be able to voluntarily provide information at an earlier stage without fear of legal or regulatory repercussions. Thus, private sector entities should have limited liability protections when they voluntarily disclose threat information to the federal government or other private entities for the purpose of improving cybersecurity.

Other changes: ITI also supports efforts to expedite the sharing of actionable cyber threat information from the government to appropriate stakeholders in the private sector. To that end, we appreciate the efforts the administration has made to improve this process over the past few years. We also support changes to the U.S. national industrial security program to allow for security clearances at the individual level to allow for receipt by additional appropriate stakeholders of classified cybersecurity threat information.

## ITI positions on key topics

- **ITI supports multidirectional cyber threat information sharing.**
  - Private-to-private, private-to-government, and government-to-private all are important sharing relationships that help stakeholders protect and defend their networks.

- **ITI believes cyber threat information sharing must be voluntary.**

- **ITI supports robust privacy protections.** Sharing cybersecurity threat information should go hand-in-hand with robust protections related to personal information. Recognizing that useful cybersecurity threat information is technical in nature and would not include personally identifiable information, we also acknowledge there are concerns about personally identifiable information being shared. Thus, we support legislative language that crisply and sharply provides the privacy protections needed. These fall under a few categories, below:

    - **Data minimization requirements – minimization by private sector:**
        - ITI supports reasonable, clearly written data minimization requirements for private entities that share with the government or other private sector entities.
    - **Data minimization requirements – minimization for further sharing:**
        - ITI supports reasonable, clearly written data minimization requirements for any recipients of cyber threat information who wish to further share this information.
    - **Use of cybersecurity threat information shared:**
        - Information shared must only be used for cybersecurity purposes.
        - Government use of information received from the private sector should be limited to four key areas:
            - For cybersecurity purposes;
            - And, may be used by law enforcement
                - for the investigation and prosecution of cybersecurity crimes;
                - for the protection of individuals from the danger of death or serious bodily harm and the investigation and prosecution of crimes involving such danger of death or serious bodily harm; and
                - for the protection of minors from child pornography.

- **ITI supports targeted liability protections.**
    - Cyber threat information voluntarily shared or received 1) should not be used for federal, state, or local regulatory purposes; 2) should not be used for civil or criminal causes of action against the sharing entity; and 3) should be exempt from FOIA.
    - ITI supports clarification in legislation that cybersecurity threat information voluntarily shared or received by a private entity with another private entity is exempt from U.S. antitrust laws.
        - ITI welcomed and appreciates the April 2014 U.S. Department of Justice (DOJ) and Federal Trade Commission (FTC) Antitrust Policy Statement on Sharing of Cybersecurity Information. However, if possible, we would prefer this clarification be codified into law.

- **Liability protections should cover both sharing and receipt of cyber threat information.**

- **For private-to-government information sharing to which new liability protections attach, ITI supports a civilian government agency interface.**

- **ITI supports new liability protections for private-to-private information sharing, if it is carefully constructed.**

- **Entities that voluntarily share cyber threat information should be able to put reasonable restrictions on how that information is further shared.**

- **ITI supports targeted policies/legislation that address identified obstacles that need to be fixed to improve the system of voluntary sharing.**

- **ITI supports lawful cross-border sharing among all interested stakeholders, regardless of national borders or company ownership.**

***For more information contact Sarah Beth Groshart at sgroshart@itic.org or Danielle Kriz at dkriz@itic.org***