Government entities and private-sector organizations in the United States now have a common framework that encourages the sharing of cybersecurity threat information among each other, thanks to new federal legislation. These guidelines also protect the privacy of personally identifiable information and provide liability protections to organizations that follow the framework and act in good faith.

Just before adjourning for the year, the US Congress passed the Cybersecurity Act of 2015 ([P.L. 114-113](https://www.congress.gov/bill/114th-congress/house-bill/11362)) on 18 December 2015, and President Barack Obama signed the measure into law later the same day. The legislation was tacked on to a massive omnibus appropriations bill at the last minute to facilitate consideration of the bill in the full House of Representatives and the Senate.

The Cybersecurity Act of 2015 aims to defend against cyberattacks by creating a framework for the voluntary sharing of cyber threat information between private entities and the federal government as well as within agencies of the federal government. Simultaneously, the legislation also aims to protect individuals’ privacy rights by ensuring that personal information is not unnecessarily divulged.

The goal of the legislation is to promote and encourage the private sector and the US government to exchange cyber threat information rapidly and responsibly. Under the Act, information about a threat found on one system can be quickly shared in order to prevent a similar attack or mitigate a similar threat to other companies, agencies and consumers. Privacy advocates counter that the new law authorizes and enables broader surveillance by the federal government and provides weak privacy protections.

The new law takes effect upon its enactment—18 December 2015—and runs through 30 September 2025.

[CONTINUED ON PAGE 2]
The legislation has had a rocky road to enactment. Bills similar to the Cybersecurity Act were proposed in previous sessions of Congress with little advancement. In January 2015, President Obama called for cyber information sharing legislation in his State of the Union Address.

In April 2015, the House of Representatives passed two separate versions of the legislation [H.R. 1560 and H.R. 1731], one put forth by the House Intelligence Committee and the other put forth by the House Homeland Security Committee.

The US Senate passed its version of the bill, the Cybersecurity Information Sharing Act (CISA) of 2015 [S. 754], on 27 October 2015 by a vote of 74 to 21. Following the Senate action, a conference committee was appointed to compile a compromise version that would pass muster in both the House and Senate.

Despite great progress in hammering out a deal, the legislation almost didn’t make it to the respective floors for a vote due to tight scheduling issues. At the last minute, the legislation was attached to a larger omnibus bill so it could be considered. As a result, neither chamber of Congress spent much time debating the compromise cybersecurity text being put forth for a vote.

Congressional Comment: House Permanent Select Committee on Intelligence Chairman Devin Nunes (R-CA) commented upon the passage of the bill, “The American people overwhelmingly agree that we need to improve our defenses against cyber attacks and to keep our Intelligence Community fully funded to track and neutralize terrorists. That consensus is reflected in the big, bipartisan majorities that approved these bills in Congress. I’m grateful to the Appropriations Committee for including these bills in the omnibus package, and I look forward to their swift passage into law.”

Survey Results:
According to the recent ISACA January 2016 Cybersecurity Snapshot survey, 72% of US respondents are in favor of the US Cybersecurity Information Sharing Act (CISA), 10% are not in favor and 15% are unsure. According to the same survey, 46% stated they would voluntarily share information as outlined by this legislation, 13% would not share, and 28% are unsure.
Under the Act, individual information may be provided to law enforcement if the identification of the responsible party that created the threat is known within the threat metadata.

Congressional Comment: Upon his nay vote on the legislation, Senator Ron Wyden (D-OR) stated, “Unfortunately, this misguided cyber legislation does little to protect Americans’ security, and a great deal more to threaten our privacy than the flawed Senate version. Americans demand real solutions that will protect them from foreign hackers, not knee-jerk responses that allow companies to fork over huge amounts of their customers’ private data with only cursory review.”

Private entities may also share threat indicators and defensive measures with other private entities; again, personal information must be removed and security controls should be in place.

Business Impact: If two or more private entities exchange cyber threat indicators or defensive measures, it will not be a violation of antitrust laws. Moreover, entities that share information with the federal government will continue to receive any applicable legal protections including trade secret protections.

The Act also promotes and facilitates the sharing of cyber threat indicators and defensive measures within the federal government. This includes the sharing of classified information with relevant federal entities (as well as non-entities) that have the requisite security clearances.

Comment: The removal of personal information from data shared by businesses with the federal government may appease some who had privacy concerns regarding similar legislative proposals. Despite this, however, many privacy advocates and even some members of Congress still have significant concerns about the value of the legislation.
The new law defines a **cybersecurity threat** as an action on or through an information system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system. A cybersecurity threat is not an action protected by the First Amendment to the Constitution of the United States (i.e., protection of free speech), nor does it include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement.

A **defensive measure** is defined as an action, device, procedure, signature, technique or other mechanism applied to an information system or information that is stored on, processed by, or transiting a system that detects, prevents or mitigates a known or suspected cybersecurity threat or security vulnerability. Under the legislation, **cyber threat indicator** is defined as information necessary to describe or identify:

- Malicious reconnaissance
- A method of defeating a security control or exploiting a vulnerability
- A security vulnerability
- A method of causing a user with legitimate access to an information system to unwittingly enable the defeat of a security control
- Malicious cyber command and control
- The actual or potential harm caused by an incident
- Any other attribute of a cybersecurity threat

**Comment:** Statements such as “any other attribute of a cybersecurity threat” may be construed by law enforcement in a broad manner, thereby allowing the government to include more information than may be necessary. It is unclear if the courts later will narrowly define this statement so as to protect the collection and dissemination of sensitive personal information.

### POLICIES AND PROCEDURES

The new Act does not specify many compliance-based rules; instead it provides directives to regulators who must detail the specifics in the form of policies and procedures to be issued. By mid-February 2016, the Attorney General and the Secretary of Homeland Security will develop interim policies and procedures relating to the receipt of cyber threat indicators and defensive measures and promoting the sharing of cyber threat indicators by the private sector with the federal government. By mid-June 2016, final policies and procedures must be released.

These policies and procedures must clarify:

- The types of information that would typically qualify as cyber threat indicators
- The types of information deemed personal to a specific individual or identifying a specific individual
- The types of protected information under privacy laws unlikely to be directly related to cybersecurity threats

In addition, the Attorney General and the Secretary of Homeland Security will develop privacy and civil liberties guidelines which will govern the receipt, retention, use, and dissemination of cyber threat indicators by a federal entity obtained from voluntary sharing of information by a private entity. The guidelines must include a process for the timely destruction of information not directly related to authorized uses, specify the length of time a cyber threat indicator may be retained, and provide requirements to safeguard cyber threat indicators containing personal information. Additionally, sanctions for misuse of information by officers, employees or agents of the federal government will be issued as part of the guidelines.

**Comment:** The sanctions to be imposed for misuse are not expounded in the legislation; instead the Attorney General and Secretary of Homeland Security will issue this guidance. Many believe, however, it is unlikely that the guidelines will criminalize such misconduct, as currently done with information shared regarding critical infrastructure, which can be subject to criminal penalties.
The guidelines must also be consistent with the Fair Information Practice Principles (FIPPs), and protect the confidentiality of cyber threat indicators containing personal information to the greatest extent practicable.

**Business Impact:** While the legislation does not describe what is meant by “greatest extent practicable,” liability protections contained in the Act will ensure that entities sharing potential cyber threat indicators are not held responsible for any misuse by those with whom the data were shared.

Finally, the guidelines must ensure that the dissemination of cyber threat indicators is consistent with the protection of classified and other sensitive national security information. The privacy and civil liberties guidelines must be reviewed at least once every two years.

In the same time frame as noted above, policies and procedures must also be issued for sharing information inside the federal government. These policies and procedures must:

- Affirm that cyber threat indicators shared with the federal government by a private entity are shared in an automated fashion with all appropriate federal agencies
- Ensure that cyber threat indicators are shared with the appropriate federal agencies in real time and only subject to delay based on controls established, uniformly applied, and agreed to unanimously by the heads of included federal entities
- Establish audit capabilities
- Provide appropriate sanctions for officers, employees or federal agents who knowingly and willfully conduct unauthorized activities

**Comment:** “Appropriate federal agency” is defined to include the Department of Commerce, the Department of Defense, the Department of Energy, the Department of Homeland Security, the Department of Justice, the Department of the Treasury, and the Office of the Director of National Intelligence.

**Business Impact:** Because the legislation mandates that the shared cyber threat indicators and defensive measures will be received by and shared among many federal agencies, businesses need to balance the risks and rewards of sharing that information.
Information shared with the federal government, and by extension with state, tribal or local governments, may only be used for:

- Identifying a cybersecurity threat and/or its source
- Identifying a security vulnerability
- Responding to, preventing or mitigating a specific threat of death, bodily harm or economic harm
- Responding to, investigating or prosecuting a serious threat to a minor
- Preventing, investigating, disrupting or prosecuting a fraud/identity theft action; an espionage or censorship action; or a protection of trade secret action

**Business Impact:** Information shared with state, tribal or local governments may be used to investigate and prosecute alleged cyber criminals. Information shared, however, cannot be used by a state, tribal or local government to regulate directly the lawful activity of any entity, although such information may be used to inform the development or implementation of regulations.

Information shared with the federal government is not subject to disclosure under the Freedom of Information Act, at the federal, state, tribal or local levels.

**LIABILITY PROTECTIONS**

The sharing of information is completely voluntary, but companies who share cyber threat indicators or defensive measures will receive legal liability safeguards if they comply with the appropriate privacy protections. The Cybersecurity Information Sharing Act maintains that no cause of action shall lie or be maintained in any court against any entity for the monitoring of information systems, nor for the sharing or receipt of cyber threat indicators or defensive measures, if the information is shared in accordance to the procedures outlined in the Act.

**Comment:** It is unclear whether the liability protections offered in the Act will be enough enticement for businesses to participate in the program. Many companies, however, view liability protection as a minimum requirement to take part in any information-sharing arrangement.
It remains to be seen whether the Cybersecurity Act of 2015’s voluntary scheme for sharing cyber information will create the necessary incentives to overcome the legal and non-legal disincentives that have previously deterred a more robust dissemination of this information. Because the goals of cyber information legislation are often diametrically opposed, it may simply be impossible for information-sharing legislation to simultaneously promote the rapid and robust collection and dissemination of cyber-intelligence by the federal government, while also ensuring that the government respects the property and privacy interests implicated by such information sharing.

CONCLUSION

By mid-February 2016, the Director of National Intelligence, the Secretary of Homeland Security, the Secretary of Defense, and the Attorney General will jointly develop and issue procedures to facilitate and promote the timely sharing of classified cyber threat indicators and defensive measures possessed by the US government with representatives of relevant entities that have the appropriate security clearance. In addition, procedures for the sharing of declassified and unclassified cyber threat indicators and defense measures with a broader audience, including the private sector, will be developed.

Business Impact: Companies that lack requisite security clearance may have little incentive to partner with governmental agencies. Not until these procedures are developed will companies be able to qualify the threat indicators to determine the value of sharing information.

The Act also encourages the US government to share periodically cybersecurity best practices developed through ongoing analysis of cyber threat indicators, defensive measures and information relating to cybersecurity threats.

OTHER PROVISIONS

The Cybersecurity Act of 2015 also includes provisions that amend the Homeland Security Act of 2002 to promote the national advancement of cybersecurity by making it consistent with CISA. Additionally, a report on cybersecurity vulnerabilities of US ports as well as a report on the security of mobile devices of the federal government are mandated. Finally, the Act requires an assessment of the federal cybersecurity workforce.

Comment: According to global respondents to a recent ISACA survey, 48% of organizations plan to hire new cybersecurity staff in 2016, but 94% expect it will be difficult to find skilled candidates.