The Heritage Foundation

ISSUE BRIEF

No. 4381 | APRIL 10, 2015

Senate Cyber Information Sharing Bill: Good Start but Can Be Improved

David Inserra

In March 2015, the Senate Intelligence Committee considered and passed the Cybersecurity Information Sharing Act (CISA) of 2015. Essentially the same as CISA 2014 from the previous Congress, CISA encourages information sharing between the government and private sector to improve security.[1] By providing security personnel with information on cyber threats and vulnerabilities, security can keep up with the ever-changing risks in cyberspace.

As such, information sharing is a first step toward cybersecurity, but it needs to be enabled and encouraged. CISA does this by affirmatively giving public and private organizations the ability to share information and providing clear liability protection for such sharing. CISA could, however, benefit from clearer regulatory protections and privacy provisions, as well as enabling broader use of shared information.

Information Sharing Basics

Cybersecurity threats and vulnerabilities are constantly being found, exploited, and fixed—but often not before serious damage is done. When any organization finds a threat or vulnerability, sharing the technical data on that threat or vulnerability with others can help them prepare for the threat or remedy the vulnerability, thus preventing harm.

This paper, in its entirety, can be found at
http://report.heritage.org/ib4381

The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002
(202) 546-4400 | heritage.org

It is important to note that information sharing is focused on the technical data of where an attack came from, what the target was, and how it works, not the contents of an e-mail or a hard drive.[2]

To be most effective, information sharing bills have to get certain key details correct regarding liability protections, usage of shared information, privacy provisions, and mechanisms for sharing. CISA handles these issues well but could be improved in some areas.

Liability Protection. CISA provides strong liability protection for information sharing that follows CISA's procedures—so long as such sharing is not grossly negligent or an act of willful misconduct.[3] Such a high bar of protection ensures that companies that share or receive information will not be sued for merely trying to improve their and other's cybersecurity. A lower standard, such as "good faith," may sound strong, but it is much easier for a tort lawyer to insinuate a lack of good faith than it is to prove willful misconduct or gross negligence. Overall, this level of liability protection will ensure that information sharing is less hindered by the threat of potential lawsuits.

Similarly, CISA provides Freedom of Information Act protections for shared data[4] and does not allow regulators to use information to directly regulate the lawful activities of sharers or receivers of threat information.[5]

Authorized Uses. CISA allows the government to use information gained by information sharing for several purposes, including:

- Enhancing cybersecurity,

- Identifying a cyber threat from a foreign adversary or terrorist,
- Preventing or prosecuting cases involving death, serious bodily harm, or other violent felonies,
- Stopping or mitigating threats of serious economic harm,
- Combatting serious threats to minors,
- Investigating and prosecuting cases of fraud and identity theft, and
- Protecting the U.S. from and taking action against those who engage in espionage and the theft of trade secrets.[6]

This list is slightly expanded from the last iteration of CISA and allows the government to use information not only for cybercrime, but also for other serious crimes. Since information sharing is focused on technical data, not personal content, the broad use of this technical data to protect U.S. citizens and companies from harm entails little risk to privacy. While further expanding the authorized uses of shared information might further enable law enforcement and security agencies to combat certain additional crimes, CISA has a sufficiently broad list that should be adequate for security purposes.

Privacy and Security. Any cybersecurity information sharing legislation will necessarily touch on issues of privacy and what kind of information is being shared with whom. It is important, however, to remember that most information that is shared is technical data, not the content of e-mails or even the real identities of the people who were attacked.

That said, when cybersecurity information is shared, some personal information or information that could be used to identify an individual or company might still be attached to it—information that is of no interest to security personnel. CISA requires companies to remove all personal data before they share cybersecurity information.[7] Removing this information is worthwhile, but it must be balanced with the need for rapid information sharing. Information sharing needs to happen quickly and as automatically as possible to ensure that constantly changing threats are countered.

One potential solution to this issue, that improves both security and privacy and that CISA alludes to, is the development and adoption of automated and/or structured threat sharing technologies that remove personal information. Structured Threat Information eXpression (STIX) is one such example that acts as a common cyber threat language[8] and provides a mechanism (TAXII) for quickly and even automatically analyzing, sharing, and receiving threat information.[9] STIX can improve privacy by providing clear guidelines and structures that share cyber threat and vulnerability information but not personal and extraneous information.

CISA also includes numerous reviews and reports on the effects on privacy. While CISA's impact on privacy should be understood through regular oversight and reporting, seemingly repetitive

1. Much of what follows is adapted from Heritage analysis of CISA from the last Congress since little has changed on substantive points. For more information on Heritage's prior analysis, see: David Inserra, "Senate Cyber Information Sharing Bill on the Right Track but Improvements Needed," Heritage Foundation *Issue Brief* No. 4269, September 2, 2014, http://www.heritage.org/research/reports/2014/09/senate-cyber-information-sharing-bill-on-the-right-track-but-improvements-needed.
2. David Inserra and Paul Rosenzweig, "Cybersecurity Information Sharing: One Step Toward U.S. Security, Prosperity, and Freedom in Cyberspace," Heritage Foundation *Backgrounder* No. 2899, April 1, 2014, http://www.heritage.org/research/reports/2014/04/cybersecurity-information-sharing-one-step-toward-us-security-prosperity-and-freedom-in-cyberspace .
3. The Cybersecurity Information Sharing Act of 2015, S. 754, § 6.
4. Ibid, § 5.
5. Ibid, § 4.
6. Ibid, § 5.
7. Ibid, § 4.
8. The MITRE Corporation, "STIX Language," Structured Threat Information eXpression, March 25, 2015, https://stix.mitre.org/index.html (accessed on April 7, 2015).
9. The MITRE Corporation, "TAXII Specifications," Trusted Automated eXchange of Indicator Information, March 25, 2015, http://taxii.mitre.org/ (accessed on April 7, 2015).

reporting requirements are unnecessary and should be streamlined.

CISA includes other privacy provisions that are appropriate and helpful, including:

- Time limits on retaining cyber threat information,
- Requirements that privacy and civil liberties officers and inspectors general report on how shared information is being used and how it is affecting the privacy of individuals, and
- A requirement that the government notify an entity when it shares information not related to a cyber threat.[10]

DHS or a Public-Private Partnership. CISA designates the Department of Homeland Security (DHS) as the hub for sharing information with the government.[11] This hub would immediately share information with other federal agencies, and in a process to be determined, information would then be shared with the private sector.

Having a central hub can help facilitate the spread of information. While the DHS is the most appropriate government agency to house this hub, there are questions regarding the DHS's ability to handle this responsibility. Its capabilities have been growing and improving, however, and it is likely the best choice, though DHS still has substantial room for growth with regard to its cyber capabilities and policies.[12]

Congressional Steps for Improvement

Overall, CISA is a step in the right direction, but it could be improved. Congress should:

- **Broaden authorized uses of shared information.** CISA includes relatively broad areas where the government can use shared information. An even better policy would be to allow government agencies to use and share information so long as one significant use is for a cybersecurity purpose.
- **Streamline privacy provisions.** Privacy provisions that overly impede information sharing should be revised. Instead of requiring that all information be scrubbed of all personal data, a more appropriate standard is to require the reasonable removal of personal information in a way that does not slow sharing. The adoption of STIX or other automated systems to scrub personal data from shared information should also be encouraged. Additionally, duplicative privacy provisions and reporting requirements should be streamlined.

Improving Cybersecurity Through Information Sharing

Information sharing, while not a silver bullet, is an important first step toward cybersecurity, and CISA's policies are aimed at taking that step. Strong liability protections and relatively broad authorized uses could be improved by streamlining privacy provisions, clarifying protection from overbearing regulation, broadening authorized uses, and continuing to improve the DHS's cyber capabilities.

*—**David Inserra** is a Research Associate for Homeland Security and Cyber Security in the Douglas and Sarah Allison Center for Foreign and National Security Policy, of the Kathryn and Shelby Cullom Davis Institute for National Security and Foreign Policy, at The Heritage Foundation.*

10. The Cybersecurity Information Sharing Act of 2014, § 5.
11. S. 754, §5.
12. David Inserra, "Congress Should Refocus DHS on Crucial Cybersecurity Reforms," Heritage Foundation *Issue Brief* No. 4335, January 26, 2015, http://www.heritage.org/research/reports/2015/01/congress-should-refocus-dhs-on-crucial-cybersecurity-reforms.