The Heritage Foundation

ISSUE BRIEF

No. 4269 | SEPTEMBER 2, 2014

Senate Cyber Information-Sharing Bill on the Right Track but Improvements Needed

David Inserra

On July 8, the Senate Intelligence Committee passed the Cybersecurity Information Sharing Act (CISA) of 2014. Cybersecurity information sharing is a valuable tool to enhance the security of businesses and the U.S. government. While sharing information on cyber threats and vulnerabilities is not a silver bullet, it keeps security personnel up to date with the constantly changing cyber environment and provides critical data to enhance their efforts to keep systems secure.

As with many policies, though, the devil is in the details. CISA takes the right approach, but it could be improved through clearer privacy provisions, broader use of shared information, and more protections from regulatory use.

Information Sharing 101

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.

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 hard drive.[1]

To make information sharing work, however, lawmakers should clear away ambiguity in current laws written back in the 1980s, a change that CISA and other information-sharing bills make.[2] Other details regarding liability protections, usage of shared information, privacy provisions, and mechanisms for sharing must also be decided. CISA handles some of these details well and others less so.

Liability Protections. CISA provides absolute 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.) If sharing occurs in a way not authorized by CISA, a good-faith defense is allowed, providing at least some defense to other sharing. Overall, this robust set of liability protections would help prevent the chilling of information sharing due to the threat of potential lawsuits.

Similarly, CISA provides Freedom of Information Act protections from shared data and does not allow regulators to use information directly against sharers or receivers of threat information to regulate their "lawful activities."[4] This construction, however, implies that regulators may directly use information against a regulated entity if they believe a law or regulation is not being followed. While law breaking

This paper, in its entirety, can be found at
http://report.heritage.org/ib4269

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

should not be encouraged, companies may be afraid to share information if they fear that doing so may indicate a regulatory breach, even if it is unintentional or unknown.

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

- Enhancing cybersecurity,
- Preventing or prosecuting cases involving death or serious bodily harm,
- Combatting serious threats to minors,
- Investigating and prosecuting case 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.[5]

This relatively broad list 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.

As a result, further expanding the authorized uses of information would enable law enforcement and security agencies to use shared information to combat additional crimes and security threats that might not fall within the authorization provided in CISA.[6]

Privacy and Security. Given the large amount of sensitive and personal data that is stored on computer systems, citizens should be concerned when they hear about the sharing of cyber information. 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 people who were attacked.

That said, when cybersecurity information is shared, some personal information might still be attached to it. While security personnel have no interest in this information, information sharing happens quickly and often automatically to ensure that constantly changing threats are countered as soon as possible.

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, since requiring every sharer to remove every piece of personal information would slow sharing.

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.[8]

1. See 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.
2. The Cybersecurity Information Sharing Act of 2014, S. 2588, § 4.
3. Ibid., § 6.
4. Ibid., § 5.
5. Ibid., § 5.
6. Protection from regulatory action as described earlier should remain, as use of information by regulatory agencies is different than stopping criminal activity or national security threats. A hypothetical crime that might not fall into CISA's authorized uses would be a planned larceny in which a hacker used a cyber attack to control the physical security of the bank. CISA's provisions would allow cyber threat information to be used to investigate the hack but not the likelihood of physical theft. While this or any other hypothetical might not be a perfect example, other serious crimes or threats could exist outside CISA's authorized uses, and government should be allowed to use shared information to protect against those threats.
7. Ibid., § 4.
8. Ibid., § 5.

DHS or a Public-Private Partnership. CISA designates the Department of Homeland Security (DHS) as the hub for sharing information with the government.[9] 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, but while DHS is the most appropriate government agency to house this hub, there are questions regarding DHS's ability to handle this responsibility.

An alternative solution is a public-private partnership organization including a board of representatives from DHS, other government agencies, the private sector, and privacy advocates.[10] Such an organization would have more oversight, encourage more collaboration, and, if properly structured, be more capable while not consuming more DHS resources.

Congressional Steps for Improvement

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

- **Restricting regulatory use of shared information.** While using shared information to better understand the state of cybersecurity and cyber threats can be helpful, companies should not fear that any information they share could result in regulatory action.
- **Broadening authorized uses of shared information.** CISA includes relatively broad areas where the government can use shared information, but broader non-regulatory use would be better at enhancing security. A better policy would be to allow government agencies to use and share information so long as one significant use is for a cybersecurity purpose.
- **Streamlining privacy provisions.** Privacy provisions that overly impede information sharing should be revised. Instead of requiring 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.

Improving Cybersecurity Through Information Sharing

CISA seeks to improve cybersecurity through information sharing and takes several steps in the right direction. Strong liability protections and relatively broad authorized uses could be improved by streamlining burdensome privacy provisions, strengthening protection from overbearing regulation, broadening authorized uses, and identifying a better mechanism for sharing.

*—**David Inserra** is a Research Associate for Homeland Security and Cybersecurity 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.*

9. Ibid., § 5.
10. Inserra and Rosenzweig, "Cybersecurity Information Sharing."