The Heritage Foundation
LEADERSHIP FOR AMERICA

ISSUE BRIEF

No. 3578 | APRIL 24, 2012

CISPA Amendments Make the Good Even Better

Paul Rosenzweig

Recognizing that the U.S. faces serious cybersecurity threats, Congress has wisely decided to take action in this important arena, and the House of Representatives will vote on multiple cybersecurity bills this week. It is just as important, however, that Congress take proper and helpful action.

House Permanent Select Committee on Intelligence chairman Mike Rogers (R–MI) and ranking member Dutch Ruppersberger (D–MD) have produced the Cyber Intelligence Sharing and Protection Act (CISPA). This bill is a smart, bipartisan product that makes it easier for the government and the private sector to share cyberthreat and vulnerability information.[1] A number of outside groups have raised concerns about the bill, and the sponsors have made some changes that warrant analysis of CISPA to see how well it addresses those concerns while still enhancing America's cybersecurity efforts.

The Benefits of Sharing Cyberthreat Information. CISPA removes the barriers between private-sector actors and other entities in government or the private sector. Currently, both the private sector and the government analyze threats and adjust their cyberdefenses to the threats and vulnerabilities they see. Ambiguities in liability and privacy laws prevent these actors from sharing this information with each other.

CISPA removes these ambiguities and would allow the government to share information with certified private-sector actors and private-sector actors to share cybersecurity threat information with other certified private actors and the federal government.[2] Nothing in the bill is a mandate. Any information shared with the federal government would be exempt from Freedom of Information Act requests and treated as proprietary information.

Additionally, CISPA protects private-sector actors from any liability resulting from sharing information. Without such a provision, a private actor would fear that sharing threat information could result in adverse consequences. For example, company A sees something dangerous and in good faith passes that information along to company B. Company B takes some action as a result of that information. As sometimes happens with intelligence sharing, the information might be wrong or incomplete, and company B might get hurt by the actions it took. Without liability protection, company B could potentially sue company A for damages.

As a whole, the authors of CISPA took a restrained, cooperative approach. Instead of mandating a certain answer to the nation's cybersecurity problems, CISPA recognizes that the private sector is already actively engaged in enhancing cybersecurity and could do more if it is given more information. The authors of CISPA should be congratulated for rejecting the view that congressional experts can come up with the "right" answer to America's cybersecurity woes but instead chose to tap the power and ingenuity of the American private sector.

Concerns and Changes. Though the first version of CISPA was a good effort, a number of privacy advocates and organizations raised some concerns about the bill. In response

This paper, in its entirety, can be found at **http://report.heritage.org/ib3578**

Produced by the Douglas and Sarah Allison Center for Foreign Policy Studies

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

to these concerns, CISPA was modified in several key ways over the past several months:

- Critics said that CISPA would penalize civilians who downloaded music and videos, much like the unhelpful Stop Online Piracy Act (SOPA) legislation earlier this session of Congress. CISPA was changed to address SOPA-like concerns regarding the blocking of accounts or access to websites believed to be infringing on intellectual property rights. CISPA does not allow for any blocking of websites or content but allows only for the sharing of cyberthreat information. To make this absolutely clear, the phrase "intellectual property" has been completely removed from the bill.

- Some were concerned that the government might coerce private-sector actors into giving information beyond what they wanted to give. A provision was added that the government cannot "require a private-sector entity to share information with the Federal Government; or condition the sharing of cyber threat information with a private-sector entity on the provision of cyber threat information to the Federal government."[3]

- Those concerned with CISPA argued that the bill allowed the government to use voluntarily shared information for purposes beyond cybersecurity. But this criticism misses the point that limiting how the government uses lawfully collected information re-erects the artificial walls between intelligence and law enforcement that were a partial cause of the failure to stop the 9/11 attacks. CISPA authorizes the use of shared information if one significant purpose of the use is "a cybersecurity purpose or the protection of the national security of the United States."

- CISPA was adjusted to provide greater oversight and accountability of the government's use of private information. In addition to oversight by the inspector general of the intelligence community, a provision was added that allows private-sector actors to sue the federal government for damages if they believe that their information has been used improperly.

- Civil liberties and technology advocates were concerned that the bill does not mandate that the private sector remove any personally identifiable information before sharing cyberthreat information with the government. While CISPA does not mandate the removal of such personal information, it allows and encourages "appropriate anonymization or minimization of" cyber threat information. A mandate to scrub all personal identifiable information would likely make it difficult if not impossible for private-sector actors to share certain critical threat details. The bill also requires that a cybersecurity provider obtain "the express consent" of an entity that it is protecting before sharing threat information, adding another level of protection to individuals' information.

- Additional changes were made to account for concerns that the National Security Agency or military intelligence should not be in charge of information sharing and that CISPA should instead guarantee civilian control of cybersecurity efforts. CISPA was amended to ensure that a civilian agency—the Department of Homeland Security—serve as a centralized repository of all information shared with the government.

Sensible Security. CISPA is a sensible and bipartisan bill designed to enhance U.S. cybersecurity efforts by providing private- and public-sector actors with threat information that can help them thwart incoming cyber-attacks. Through various amendments and changes, CISPA has addressed most, if not all, of the privacy concerns leveled against it. Importantly, these changes do not weaken the cybersecurity enhancements that the bill provides. CISPA avoids potentially harmful

1. See Paul Rosenzweig, "Congressional Cyber Initiative Shows Promise," Heritage Foundation *Web Memo* No. 3478, January 31, 2012, http://www.heritage.org/research/reports/2012/01/rogers-ruppersberger-bill-a-solid-cybersecurity-approach.
2. "Certified actors or entities" are those organizations or individuals who are able to possess a security clearance in order to safeguard the threat information they receive. If entities were not required to be certified, then shared threat information would be easily obtainable by hackers and malicious actors, who would then adjust their attacks, rendering the shared information less valuable.
3. Indeed, Chairman Rogers has pointed out that this anti-tasking provision is actually stronger than legislative language proposed by some of the privacy advocates.

regulations and uses the innovation and resourcefulness of the private sector to make the nation more secure.

*—**Paul Rosenzweig** is a Visiting Fellow in the Center for Legal and Judicial Studies and the Douglas and Sarah Allison Center for Foreign Policy Studies, a division of the Kathryn and Shelby Cullom Davis Institute for International Studies, at The Heritage Foundation.*