House Passes H.R. 624,Cyber Intelligence Sharing and Protection Act; Obama Administration Responds

Alyssa Z. Hutnik

April 22, 2013

Last week, the U.S. House of Representatives passed the Cyber Intelligence Sharing and Protection Act (CISPA) (H.R. 624), introduced on February 13, 2013 by House Intelligence Committee Chairman Mike Rogers (R-MI) and Ranking Member Dutch Ruppersberger (D-MD). Passage of the bill occurred shortly after the White House threatened to veto CISPA in its current form, and has incited fierce opposition from several privacy and digital rights groups that have rallied – with limited success – for an Internet blackout today. The House had passed similar legislation (H.R. 3523) in the 112th Congress on April 26, 2012, in a measure that was not taken up by the Senate.

In pertinent part, the legislation would allow the federal government to share classified cyber threat intelligence with the private sector and would enable private sector entities to share cyber threat information with one another and with the federal government on a voluntary basis. The bill would limit information sharing of “cyber threat information” for certain enumerated purposes, including the investigation and prosecution of cybersecurity crimes and the protection of individuals from danger of death or serious physical injury.

Under the legislation, the Director of National Intelligence would be responsible for establishing procedures to enable the intelligence community to share classified cyber threat intelligence with private sector entities. The policies and procedures for the receipt, retention, use, and disclosure of cyber threat information shared with the federal government must be crafted in a manner that “minimize[s] the impact on privacy and civil liberties.” Further, the legislation would require a federal oversight program, including the issuance of two annual reports by designated agencies.

The legislation also would provide private sector entities immunity from civil or criminal liability, acting “in good faith,” (i) if they share cyber threat information with other private entities and with the federal government in accordance with the bill, or (ii) “for decisions made for cybersecurity purposes and based on cyber threat information identified, obtained, or shared.”

The legislation does not include four privacy amendments that were rejected earlier this month by the House Intelligence Committee. These amendments would have served to:

- Limit the sharing of private sector data to civilian agencies and specifically excluding the National Security Agency and the Defense Department (failed by a 4-14 vote)
- Direct the president to create a high-level privacy post that would oversee "the retention, use, and disclosure of communications, records, system traffic, or other information" acquired by the

federal government. This amendment also included "requirements to safeguard communications" that contain PII (failed by a 3-16 vote)

- Eliminate vague language that grants complete civil and criminal immunity to companies that "obtain" information about vulnerabilities or security flaws and make "decisions" based on that information (failed by a 4-16 vote), and
- Require that companies sharing confidential data "make reasonable efforts" to delete "information that can be used to identify" individual Americans (failed by a 4-16 vote).

On April 16, the White House issued a statement that the President would veto CISPA as currently drafted. Acknowledging the bipartisan consensus on the need for such legislation, the Administration believes CISPA does not sufficiently adhere to the following principles: (1) carefully safeguard privacy and civil liberties; (2) preserve the long-standing, respective roles and missions of civilian and intelligence agencies; and (3) provide for appropriate sharing with targeted liability protections. In particular, the Administration expressed concern over CISPA's overbroad scope of liability limitations and its failure to require private entities to take reasonable steps to remove PII when sending cybersecurity data to the government or other private sector entities. Further, the Administration seeks to preserve the "longstanding tradition" to treat the Internet and cyberspace as civilian spheres and recommends that information sharing for cybersecurity purposes from the private sector to the government enter the government through a civilian agency (*i.e.*, the Department of Homeland Security).

CISPA now moves to the Senate for consideration.

Written by Alysa Z. Hutnik