The Cyber Intelligence Sharing and Protection Act, H.R. 624

Problem

• Every day, foreign governments, terrorist organizations, and criminal groups attack the cyber networks in both the public and private sectors. These cyber attackers steal billions of dollars of America's intellectual property, national security intelligence, trade secrets, and corporate information. The attackers shut down websites, disrupt services, and corrupt huge masses of data.

• In the past year alone, cyber attackers have hit major oil companies, banks, newspapers, and government agencies. In addition to intellectual property and national security intelligence, personal financial, healthcare, and other private records are prime targets for attackers to steal. The private sector does what it can to protect its networks, but often it has limited information and can respond only to known threats.

• The Intelligence Community (IC) has timely, classified information about destructive malware waiting to strike our nation's cyber networks, but the federal government does not have the authority to share this "cyber threat intelligence" with the private sector so it can use it to protect its networks.

• This cyber threat intelligence is the information that companies and the government need to protect and defend their networks. It is primarily made up of numerical codes (zeroes and ones), without any personal information. It is often referred to simply as "signatures."

Solution

• *The Cyber Intelligence Sharing and Protection Act*, H.R. 624, provides the government, private entities, and utilities with clear authority to use this "cyber threat intelligence" to protect America's vital networks, including those that power our homes, provide our clean water, protect our bank accounts, defend our intellectual property, guard our national security information, and manage other critical services.

• On April 10, 2013, the Intelligence Committee passed the bill out of markup by a vote of 18-2. The markup adopted many amendments that enhance privacy and civil liberties protections, as detailed on the reverse page.

• This bipartisan legislation was developed in close consultation with a broad range of private sector companies and trade groups. Throughout, a dialogue has been maintained with privacy and civil liberties advocates, as well as the Executive Branch.

• CISPA lets private entities and the federal government share cyber threat information to help each other protect their networks. Private companies always can receive cyber threat information, but their decision to share information is totally voluntary, and there is no penalty for choosing not to share cyber threat information.

• CISPA does not alter federal agencies' existing authorities or provide any new authority to any federal agency. CISPA ensures that the government cannot install, employ, or otherwise use cybersecurity systems on private sector networks.

Protecting Privacy and Ensuring Oversight

• CISPA lets companies receive classified cyber threat intelligence to identify the malicious cyber "signatures" within their networks (or their clients' networks) and remove it before it can do any damage. Companies are encouraged to share cyber threat information with the government on a voluntary basis, so that the government can help protect other networks in the future. Companies may "anonymize" this information or strip it of all "personally identifiable information (PII)".

• During markup in April 2013, the Intelligence Committee added significant measures to enhance privacy and civil liberties for Americans.

• First, the government is now required to eliminate any personal information it receives that is not necessary to understand the cyber threat.

• Second, we have expanded our privacy protections and oversight requirements by adding an extra layer of review by the Privacy and Civil Liberties Oversight Board and requiring senior privacy officials from the government agencies to complete annual reviews evaluating the cyber threat information sharing regime's effect on privacy.

• Third, we have limited the government's permissible uses for cyber threat information by eliminating the national security use exception. The government now cannot retain or use a company's cyber threat information for anything other than cyber security purposes, investigating and prosecuting cybersecurity crimes, protection of minors, and protection of individuals from bodily harm.

• Fourth, we have limited the private sector's permissible uses for cyber threat information. Now, companies can use cyber threat information received from other private sector entities *only* for cyber security purposes.

• Fifth, we have explicitly prohibited providers and self-protected entities from using outside systems for cyber threat information purposes. In other words, they cannot "hack back" into computer systems that are not their own to retrieve information stolen from them.

• CISPA specifically protects privacy by prohibiting the government from using personal information from library and book records, gun sales, tax records, educational records, and medical records.

• The legislation gives companies the flexibility to choose which agency within the intelligence community they would like to work with to protect their cyber networks. This allows a company that has a pre-established relationship with a certain agency, for example a bank that currently works with the Treasury Department, to maintain this relationship.

• CISPA provides liability protection for companies that act in "good faith" when protecting their own networks or sharing cyber threat information with the government or other companies. However, this liability protection extends only to the identification and acquisition of cyber threat information – it does not extend to other private sector business activities. The bill also defines a "lack of good faith" – this lets public and private entities have clarity, certainty, and direction when making decisions about sharing cyber threat information, so that they can be sure to have liability protection only for appropriate activities.

• The bill does not give the government any authority to search or analyze the content of individual emails or load any monitoring software on to anyone's personal computer.

• Private companies' cyber threat information that they share with the government would be treated as proprietary information and exempt from disclosure under the Freedom of Information Act (FOIA). However, information that already is required to be disclosed under FOIA will remain obtainable.

• For a company to become "certified" and allowed to participate in the program, it must have personnel with appropriate security clearances following the guidelines provided by the Director of National Intelligence.

• This bill hopes to harness private sector innovation by allowing industry to expand its own cyber defenses with help from the federal government's cyber threat intelligence. The goal is to give companies the latest information in a timely manner so they can protect themselves from assaults on our nation's networks.

• CISPA has a five-year sunset provision, which ensures that Congress must review and evaluation the bill before renewing it in 2018.