

The Rogers-Ruppersberger Cybersecurity Bill (H.R. 624)

The Cyber Threat: Every day U.S. businesses are targeted by nation-state actors like China, Iran and Russia for cyber exploitation and theft, resulting in huge losses of valuable trade secrets and sensitive customer information. This rampant industrial espionage costs American jobs.

- When these hackers steal these trade secrets, they take new, high-paying jobs right along with it. Estimates of loss from cyber economic espionage are hard to make, but range up to \$400 billion a year. **Just as important, many of the same vulnerabilities used to steal trade secrets can be used to attack the critical infrastructure we depend on every day.**
- China is the world's most active and persistent perpetrator of cyber economic espionage. U.S. companies have reported an onslaught of Chinese cyber intrusions that steal sensitive information like client lists, merger and acquisition data, pricing information, and the results of research and development efforts. This illegally-acquired information gives Chinese companies an unfair competitive advantage against the American companies from which it was stolen.

Legal Barriers Impede Cyber Cooperation: Most elements of the private sector are already working hard to make their networks more secure. They are too often hindered, however, by a lack of information about what attacks other American companies are experiencing and how they are coping with those attacks.

- Too often, companies that would like to share cyber threat information with other parts of the private sector or the government are prevented or deterred from doing so by a range of policy and legal barriers.
- Just as importantly, the U.S. Intelligence Community also collects classified information overseas about advanced foreign cyber hackers and their plans to attack the networks of American companies. Unfortunately, the government lacks clear, positive legal authority to grant security clearances and share that important information with private sector companies to help them better defend themselves against nation-state actors like China in cyberspace.

Information Sharing to Help the Private Sector Better Protect Itself: In April 2012, the full House of Representatives approved the Cyber Intelligence Sharing and Protection Act (CISPA) by a strong bipartisan vote of 248-168. The Senate failed to act on cybersecurity legislation in the last Congress, but CISPA was reintroduced in the House in February 2013.

- On April 10, 2013, the House Permanent Select Committee on Intelligence (HPSCI) passed CISPA out of committee on a bipartisan vote of 18 to 2.
- This important legislation enables cyber threat sharing within the private sector and, on a purely voluntary basis, with the government; all while providing strong protections for privacy and civil liberties.
 - The bill also provides the government clear authority to grant security clearances to the employees of private sector companies for cybersecurity threat sharing, and to share classified cyber threat information with those companies.

- Voluntary information sharing with the federal government helps improve the government’s ability to protect against foreign cyber threats and gives our intelligence agencies tips and leads to help them find advanced foreign cyber hackers overseas. This in turn allows the government to provide even better cyber threat intelligence back to the private sector to help it protect itself.
- This bipartisan legislation was developed with the input of a broad range of private sector companies, trade groups, privacy and civil liberties advocates, and the Executive Branch.
 - Based on helpful input from the privacy and civil liberties community, the HPSCI adopted an amendment during committee markup in December 2011 that significantly limited the government’s use of information voluntarily shared by the private sector.
 - Other significant privacy improvements were made to the bill during floor consideration in April 2011. The Chairman and Ranking Member remain open to constructive suggestions for other ways to further improve the bill.

Strong Protections for Privacy and Civil Liberties: The bill has very narrow definitions that permit only the voluntary sharing by the private sector of a very limited category of information—cyber threat information—and permits only the sharing of such information for cybersecurity purposes, a similarly limited term.

- The bill protects privacy by prohibiting the government from forcing private sector entities to provide information to the government, by mandating the government to “anonymize” or “minimize” any information it receives from the government, and by explicitly authorizing and encouraging the government to create procedures to protect privacy. It also strictly limits the private-to-private sharing to only cyber threat information to ensure no information can be used for other non-cyber purposes.
- The bill also puts in place strict restrictions on the use, retention, and searching of any data voluntarily shared by the private sector with the government.
- The bill enforces these strong privacy and civil liberties protections by permitting individuals to sue the federal government for damages, costs, and attorney’s fees in federal court.
- The bill also provides for strong public and Congressional oversight by requiring a detailed annual review by the Intelligence Community Inspector General (IG) of the government’s use of any information shared by the private sector, consultation with the Privacy and Civil Liberties Oversight Board and requiring the IG to provide recommendations to Congress—in an unclassified report—to better protect privacy and civil liberties.
- The bill will sunset in five years, permitting Congress to carefully review the use of the authorities provided by the bill and determine whether they should be extended or modified.

This bill is not a cure-all for our nation’s cyber problems, but it is a vital first step toward providing better protection for the networks and systems that Americans depend on every day.