

## **General Backgrounder on the Rogers-Ruppersberger Cybersecurity Bill**

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

- When these hackers steal intellectual property, they take new, high-paying jobs right along with it. Estimates of loss from 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 intellectual property can be used to attack the critical infrastructure we depend on every day.
- China is the world's most active and persistent perpetrator of 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.

**Intelligence Sharing to Help the Private Sector Protect Itself:** Today, the United States government protects itself against cyber espionage by using both classified and unclassified cyber threat information.

- However, the vast majority of the private sector doesn't get the benefit of the classified threat intelligence that the government already has in its possession.
  - If the government were able to share its classified threat information, the private sector would be able to better defend itself against nation-state actors in cyberspace.
  - An important experiment recently conducted by the Defense Department proves that this can work. The Defense Industrial Base Pilot program provided classified cyber threat intelligence to communications service providers who used it protect defense contractors. The pilot showed that sharing intelligence can enhance private cybersecurity without any government monitoring.
- In December 2011, the House Permanent Select Committee on Intelligence (HPSCI) passed the Cyber Intelligence Sharing and Protection Act to allow the government to provide classified cyber threat intelligence to the private sector.
  - The legislation was passed out of committee on a strong bipartisan vote of 17 to 1, and enjoys more than 100 bipartisan cosponsors, including 11 Committee chairmen.
- This important legislation would enable cyber threat sharing and provide clear authority for the private sector to defend its own networks, all while providing strong protections for privacy and civil liberties.
  - This bipartisan legislation was developed in close consultation with a broad range of private sector companies, trade groups, privacy and civil liberties advocates, and the Executive Branch. The bill continues to be revised based on discussions with numerous groups and key new changes are reflected in this document and related materials.

- The bill protects privacy by prohibiting the government from requiring private sector entities to provide information to the government, and by encouraging the private sector to “anonymize” or “minimize” the information it voluntarily shares with others, including the government. In addition, the bill requires an independent Inspector General audit of any voluntary information sharing with the government. (Amendment at markup)
- The bill has been amended to narrow its definitions to remove the term “intellectual property.” The definition was narrowed to avoid any misunderstanding and to clarify that it is intended only to defend against attempts by advanced cyber hackers, from countries like China, to gain unauthorized access to networks, including efforts to gain such access to steal private or government information. (New provision)
- The bill ensures the Department of Homeland Security will continue to play a key role by requiring it to generally receive cybersecurity information voluntarily shared with the government and by making clear that no new authorities are granted to the Defense Department or the Intelligence Community to direct private or public cybersecurity efforts. (New provision)
- The bill also significantly limits the federal government’s use of information voluntarily provided by the private sector, including a restriction on the government’s ability to search that data. (Amendment at markup)
- The bill enforces the restrictions on the government by levying penalties against the government through federal court lawsuits for any violations of those restrictions. (New provision)
- The bill provides positive authority to private sector entities to defend their own networks and those of their corporate customers, and to share cyber threat information with others in the private sector, as well as with the federal government on a purely voluntary basis.
  - Voluntary information sharing with the federal government improves the government’s ability to protect against foreign cyber threats.
- By allowing the private sector to expand its own cyber defense efforts and to employ classified information to protect systems and networks, this bill will harness private sector drive and innovation while also keeping the government out of the business of monitoring and guarding private sector networks.
  - This legislation will also help create a more robust private sector cybersecurity marketplace, and create new private sector jobs for cybersecurity professionals.
  - This bill will not require additional federal spending or the creation of a vast new government bureaucracy. It will impose no new regulations or unfunded mandates. To the contrary, it will be a critical, bipartisan first step toward enabling America’s private sector to do what it does best: create, innovate, and sell cybersecurity solutions.