

## [H.R. 1560, the Protecting Cyber Networks Act](#)

### FLOOR SITUATION

On Wednesday, April 22, 2015, the House will consider [H.R. 1560](#), *the Protecting Cyber Networks Act*, under a [structured rule](#), which makes in order five amendments. The bill was introduced on March 24, 2015 by Rep. Devin Nunes (R-CA) and was referred to the Permanent Select Committee on Intelligence, which ordered the bill reported, as amended, by voice vote on March 26, 2015.

### SUMMARY

H.R. 1560 establishes procedures to improve cybersecurity in the United States by enhancing the sharing of information about cybersecurity threats between the private sector and, on a voluntary basis, with the Federal government while protecting the privacy and civil liberties of American citizens.

The bill:

- Enables private companies to share a limited category of information—called cyber threat indicators—with each other and, on a purely voluntary basis, with civilian entities of the Federal government for cybersecurity purposes.
- Protects privacy by prohibiting the government from forcing private sector entities to provide information to the government.
- Requires companies to remove personal information before they share cyber threat indicators with the government.
- Requires the Federal agency that receives cyber threat indicators to perform a second check for personal information before sharing them with other relevant Federal agencies.
- Strictly limits the private-to-private sharing to only cyber threat indicators and defensive measures to combat a threat. The legislation does not allow for the sharing of information for non-cyber purposes.
- Imposes strict restrictions on the use, retention, and searching of any data voluntarily shared by the private sector with the government.
- Provides liability protection for private companies that monitor an information system or share or receive cyber threat indicators or defensive measures.

- Does not shield a company from willful misconduct in the course of sharing cyber threat indicators. The bill enforces privacy and civil liberties protections by permitting individuals to sue the Federal government for intentional privacy violations in Federal court.
- Provides for strong public and congressional oversight by requiring a detailed biennial Inspectors General (IG) report of appropriate Federal entities of the government’s receipt, use, and dissemination of cyber threat indicators. The [Privacy and Civil Liberties Oversight Board](#) (PCLOB) must also submit a biennial report on the privacy and civil liberties impact of the Act.

Specifically:

Section 2 provides that the [Director of National Intelligence](#) (DNI) should, in consultation with the heads of the Departments of Homeland Security, Treasury, Justice, Commerce, and Defense (“appropriate Federal entities”), establish procedures to facilitate and promote the timely sharing of cyber threat indicators with the private sector.

The procedures would promote the sharing of: classified cyber threat indicators with representatives of the private sector with appropriate security clearances; classified cyber threat indicators that may be declassified and shared at an unclassified level; and any information in the possession of the Federal government about imminent or ongoing cyber threats that may allow private companies to prevent or mitigate those threats. The procedures must also ensure the Federal government creates and maintains the capability to share cyber threat indicators in real time with the private sector, consistent with the protection of classified information.

The procedures drafted by the DNI require Federal agencies to perform a review of cyber threat indicators they receive from the private sector before the agencies share those indicators within the Federal government. In that review, the receiving agencies will assess whether—despite the private sector’s own requirement to conduct a similar review—the cyber threat indicators contain any personal information or information identifying a specific person that does not directly relate to a cyber-threat. If so, the Federal government must remove that information.

Section 3 authorizes private entities to engage in defensive monitoring of their own networks and the networks of non-Federal entities that have consented to such monitoring. The bill does not authorize the Federal government to conduct surveillance of any person. The section also authorizes private entities to operate defensive measures on their own networks and the networks of non-Federal entities that have consented to the operation of such defensive measures. The bill does not authorize non-Federal entities to operate such a measure in a manner that destroys, renders unusable, or inaccessible (in whole or in part), or substantially harms, a network that does not belong to them or to a non-Federal entity that has not consented to the operation of those defensive measures.

Section 4 requires the President to develop and submit to Congress policies and procedures for the receipt of cyber threat indicators and defensive measures by the Federal government; requires the Attorney General, in consultation with the heads of other appropriate Federal entities, to develop and periodically review privacy and civil liberties guidelines; establishes the Cyber Threat Intelligence Integration Center within the Office of the DNI; specifies that the sharing of a cyber-threat indicator with the Federal government does not constitute a waiver of any applicable privilege or protection provided by the law; and, lays out the purposes for which

the Federal government may use a cyber threat indicator it receives from a non-Federal entity under the Act.

Section 5 creates a private cause of action against the Federal government if a department or agency intentionally or willfully violates the privacy and civil liberties guidelines issued by the Attorney General under Section 4(b) of the Act. The section also establishes statutory damages for a violation of the Attorney General guidelines, provides for reasonable attorney fees for injured persons, specifies the possible venues for an action, and creates a statute of limitations for the new cause of action. Lastly, Section 5 clarifies that this cause of action is the exclusive means available to a complainant seeking a remedy for a violation of the Act by a department or agency of the Federal Government.

Section 6 provides that no cause of action shall lie or be maintained in any court against any private entity that monitors an information system or shares or receives cyber threat indicators or defensive measures. Nothing in Section 6, however, shall be construed to require the dismissal of a cause of action against a non-Federal entity that has engaged in willful misconduct in the course of conducting activities authorized by the Act.

Section 7 requires a biennial report by the DNI on implementation of the Act. The section also requires two reports on privacy and civil liberties: (1) one by the Privacy and Civil Liberties Oversight Board to Congress on the privacy and civil liberties impact of the Act, to be submitted biennially, and, (2) one by the Inspectors General of relevant Federal entities to Congress on the receipt, use, and dissemination of cyber threat indicators shared with the Federal government under the Act, to be submitted biennially.

Section 8 requires the DNI, within 180 days of enactment, and in consultation with the heads of appropriate elements of the Intelligence Community, to submit a report on cybersecurity threats, including cyber-attacks, theft, and data breaches, to the House and Senate congressional intelligence committees. The report must be submitted in unclassified form but may include a classified annex.

Section 9 specifies, among other things, that nothing in the Act authorizes the Department of Defense or any element of the Intelligence Community, including the National Security Agency, to target a person for surveillance.

Section 10 contains conforming amendments.

Section 11 defines a number of key terms used in the Act.

Click [here](#) for a summary and [here](#) for a detailed section-by-section analysis of the legislation provided by the Intelligence Committee. The transcript of the Committee's mark-up of the bill can be found [here](#).

## **BACKGROUND**

Today, hardly a day goes by without news of a cyberattack on an American business or government agency. High-profile attacks are commonplace. Both in the boardroom and around the kitchen table, Americans suffer the impact of cyberattacks. Whether carried out by foreign governments or criminals, these attacks steal Americans' identities, credit card information, tax refunds, and countless other kinds of private information. In just the past year, attackers have shown they can adeptly carry

out criminal activity, including theft and espionage, on computer networks inside the United States.<sup>1</sup> These attacks violate Americans' privacy on a massive scale and cost thousands of American jobs.<sup>2</sup>

Some cyberattacks are sponsored by foreign governments. China, Russia, North Korea, and Iran have created highly skilled cyberwarfare units that directly target American businesses for their most valuable intellectual property. In May 2014, for instance, Federal prosecutors charged five military officers from Unit 61398 of the Third Department of the Chinese People's Liberation Army with computer hacking and economic espionage against the U.S. nuclear power, metals, and solar products industries. The sheer number of attacks against American companies—at least thousands each day—harms our economy and thus our national security.<sup>3</sup>

Other attacks are carried out by criminal organizations. A recent *Washington Post* [report](#) suggested that more than 3,000 companies were alerted to cyberattacks by Federal agents in 2013. And that number represents only the number of cases in which the Federal government learned that an attack occurred. Companies must defend their networks around the clock on all fronts, but an attacker only needs to succeed once to cause tremendous damage. The ability to share cyber threat information and solutions will significantly help security officials throughout both the private sector and the government defend their networks, and thereby defend Americans' most private information and most valuable intellectual property.<sup>4</sup>

The Federal government already provides significant support and assistance to private companies to address cyberattacks. However, real and perceived legal barriers to cybersecurity monitoring and information sharing constrain companies with even the best of intentions. American businesses have sought positive legal authority to monitor their networks and to share and receive cyber threat indicators and defensive measures. Voluntary information sharing between companies helps businesses defend themselves against cyberattacks, and voluntary, two-way information sharing with the Federal government can help the government disseminate cyber threat information with greater speed and accuracy. H.R. 1560 is designed to encourage this sharing and help businesses improve their defenses against cyberattacks, while providing strong protections for privacy and civil liberties.<sup>5</sup>

## COST

The Congressional Budget Office (CBO) [estimates](#) that implementing the bill would cost \$186 million over the 2016 to 2020 period, assuming appropriation of the estimated amounts. The bulk of this cost relates to the establishment of the Cyber Threat Intelligence Integration Center. CBO also found that enacting H.R. 1560 would affect direct spending and revenues because the bill would allow information to be shared with the government and to be used in investigating and prosecuting certain crimes. CBO expects that that any additional revenue and direct spending would not be significant. However, because the bill would affect direct spending and revenues, pay-as-you-go procedures apply.

---

<sup>1</sup> Heritage Foundation: "[Cyber Attacks on U.S. Companies in 2014](#)." October 27, 2014.

<sup>2</sup> [House Report 114-63](#) at 14.

<sup>3</sup> Id.

<sup>4</sup> Id.

<sup>5</sup> Id. at 14 and 15.

## AMENDMENT SUMMARY

- 1) [Rep. Devin Nunes \(R-CA\) Amendment](#) - Makes technical changes to several sections of the bill. Clarifies the authorization for the use of defensive measures. Further clarifies the liability protections for network monitoring and sharing and receipt of cyber threat indicators and defensive measures.
- 2) [Rep. Tony Cardenas \(D-CA\) Amendment](#) - Instructs the Small Business Administration (SBA) to provide assistance to small businesses and small financial institutions to participate under this section, instruct the SBA to generate a report about such entities participation and instruct the federal government to engage in outreach to encourage small business and small financial institution participation.
- 3) [Rep. Andre Carson \(D-IN\) Amendment](#) - Adds the requirement that the Inspector General report on current procedures pertaining to the sharing of information, removal procedures for personal information or information identifying a specific person, and any incidents pertaining to the improper treatment of information.
- 4) [Rep. Mick Mulvaney \(R-SC\) Amendment](#) - Sunsets the provisions of the bill after 7 years.
- 5) [Rep. Shelia Jackson Lee \(D-TX\) Amendment](#) - Directs the Government Accountability Office (GAO) to provide a report to Congress on the actions taken by the Federal Government to remove personal information from data shared through the programs established by this statute.

## STAFF CONTACT

For questions or further information please contact [Jerry White](#) with the House Republican Policy Committee by email or at 6-5539.