THE REPUBLICAN STUDY COMMITTEE
Rep. Bill Flores, Chairman
Freedom ★ Liberty ★ Opportunity ★ Security
202.225.6105
rsc.flores.house.gov

H.R. 1560—Protecting Cyber Networks Act (Rep. Nunes, R-CA)

CONTACT: NICHOLAS RODMAN, NICHOLAS.RODMAN@MAIL.HOUSE.GOV, 6-8576

FLOOR SCHEDULE: SCHEDULED FOR CONSIDERATION ON APRIL 21, 2015 UNDER A CLOSED RULE THAT PROVIDES FOR ONE HOUR OF DEBATE

TOPLINE SUMMARY: H.R. 1560 would amend the National Security Act of 1947 by directing the Director of National Intelligence (DNI) to develop procedures to promote and share cybersecurity threat information that the federal government possesses with private entities, non-federal government agencies, state, tribal, or local governments, and information. H.R. 1560 would extend civil and criminal liability protection to cybersecurity providers and other entities that monitor, share, or use cyber threat information.

CONSERVATIVE CONCERNS: Some conservative shave deemed the government's efforts to maintain a balance between national security and privacy as unsatisfactory, due in part to concerns over the cost of these cybersecurity efforts, governmental duplication, and the erosion of privacy rights. H.R. 1560's liability protection provisions have also been an issue of concern. Other conservatives believe that the threat posed by cyberattacks on the U.S. economy, infrastructure, and overall national security remains an ever increasing danger and must be addressed through increased information sharing and liability protection

- **Expand the Size and Scope of the Federal Government?** No.
- **Encroach into State or Local Authority?** No.
- **Delegate Any Legislative Authority to the Executive Branch?** No.
- **Contain Earmarks/Limited Tax Benefits/Limited Tariff Benefits?** No.

COST: The Congressional Budget Office (CBO) estimates that implementing H.R. 1560 would cost $186 million over the 2016-2020 period, assuming appropriation of the estimated amounts.

H.R. 1560 would impose intergovernmental and private-sector mandates, as defined in the Unfunded Mandates Reform Act (UMRA), by extending civil and criminal liability protection to cybersecurity providers and other entities that monitor, share, or use cyber threat information.

DETAILED SUMMARY AND ANALYSIS: Section 2 would ensure that the federal government has and maintains the capability to share cyber threat indicators in real time consistent with the protection of classified information, and would require notification to entities when the federal government has shared indicators in error or in contravention of the law. Federal agencies are required to perform a review of cyber threat indicators they receive from non-federal entities before the agencies share those indicators within the government, to assess whether such threats contains any information that at the time of sharing is deemed to be personal information of or information identifying a specific person not directly related to a cybersecurity threat. The agency would then be required to remove such information.

Section 3 of the bill would authorize a private entity to monitor its on information system (an information contained in the system), and an information system of a non-federal entity or a federal entity, upon the written authorization from the entity. The bill would not authorize the federal government to monitor information that is not specified under the bill. Private entities are authorized to operate defensive measures on their own networks and the networks of non-federal entities that have consented.

Non-federal entities are not authorized to intentionally or recklessly operate any defensive measure that destroys, render unusable or inaccessible (in whole or in part), substantially harms, or initiates a new action, process, or procedure on any network that does not belong to them or to a non-federal entity that has not consented to the defense measure operation.

According to the committee, section 3 would not authorize ''hacking back'' or any other form of cyber operation that takes place on computers or networks without the consent of the owner of those computers or networks. A non-federal entity may share or receive cyber threat indicators or defensive measures for cybersecurity purposes with other non-federal entities under the guidelines and restrictions of the bill. This section would also allow a non-federal entity to share or receive cyber threat indicators with appropriate federal agencies, other than the Department of Defense (DOD) and the National Security Agency (NSA) (non-federal entities may share information with DOD and the NSA if authorized by preexisting or applicable law).

Section 4 would require the president to develop and submit to Congress policies and procedures relating to the receipt of cyber threat indicators and defensive measures by the federal government. The Attorney General of the United States is also mandated to develop and periodically review privacy and civil liberties guidelines that would govern the receipt, retention, use, and dissemination of cyber threat indicators obtained by the federal government. The attorney general must submit interim guidelines not later than 90 days after the bill's enactment.

H.R. 1560 would create a center within the Office of the Director of National Intelligence (ODNI) that would be responsible for analyzing and integrating information from the intelligence community on cyber threats, and would require the government to establish procedures for sharing information and data on cyber threats between the federal government and the private sector voluntarily. Under this section, the provision of a cyber threat indicator or defensive measure to the federal government would not constitute a waiver of any applicable privilege or protection provided by law, including trade secret protection.

Section 5 of the bill would allow the federal government to be liable if a department or agency intentionally or willfully violates the privacy and civil liberties guidelines issued by the attorney general, and establishes statutory damages if there is a violation.

Section 6 would offer liability protection for any private entity that monitors an information system and information conducted in good faith under the guidelines of the bill. The section would stipulate that nothing would be construed to require the legal 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 bill.

Section 7 would require the Director of National Intelligence to report biennially on the bill's implementation. The Privacy and Civil Liberties Oversight Board is also mandated to submit a report biennially to Congress and the president on the bill's impact on privacy and civil liberties.

Section 8 would require the Director of National Intelligence to submit a report to the congressional intelligence committees on cybersecurity threats, including cyberattacks, theft, and data breaches.

Section 9 would clarify that the bill does not authorize the DOD or the NSA or any other element of the intelligence community to target a person for surveillance, nor would it limit lawful disclosures of

communications or records, or permit the federal government to require or force a non-federal entity to provide information to the government.

According to H. Rept. 114-63 and the House Permanent Select Committee on Intelligence, the bill would encourage sharing of cyber threat indicators and defensive measures (1) between private companies; (2) between private companies to the federal government; and (3) between the federal government to private companies. More importantly, H.R. 1560 would seek to strengthen cybersecurity in light of the growing threat from cyber-attacks originating domestically and overseas from individuals, hostile regimes like China, North Korea, and Russia, and non-state actors like the ISIS, while at the time seeks to maintain the delicate balance between ensuring our national security and protecting our privacy rights.

According to the House Permanent Select Committee on Intelligence, the bill would ensure the protection of privacy by prohibiting the government from forcing private sector entities to provide information to the government. In addition, this legislation would impose strict restrictions on the use, retention, and searching of any data voluntarily shared by the private sector with the government. Furthermore, H.R. 1650 would enforce privacy and civil liberties protections by permitting individuals to sue the federal government for intentional privacy violations in federal court.

The House Report (H. Rept. 114-63) accompanying H.R. 1560 can be found here. A section by section, myth vs. fact, and bill summary from the House Permanent Select Committee on Intelligence can be found here. An Op-Ed from the chair and ranking member on the committee in The Hill can be found here. A Heritage Foundation research paper on the cybersecurity legislation can be found here. A Congressional Research Service report on Cybersecurity and Information Sharing comparing H.R. 1560 with H.R. 1731 can be found here.

OUTSIDE ORGANIZATIONS:

- **In Support:**
  Protecting America's Cyber Networks Coalition
  Financial Services Trade Associations
  Telecoms Associations
  US Telecom
  BSA/Software Alliance
  Oracle
  CA Technologies
  Information Technology Industry Council

- **In Opposition:**
  Generation Opportunity
  FreedomWorks
  Liberty Coalition
  R Street
  Open Technology Institute
  Technologists and Academics Letter

AMENDMENTS MADE IN ORDER:

- Nunes Amendment #5 (Manager's Amendment) would make technical changes to several sections of the bill and would clarify the liability protections for network monitoring by stating that nothing in the bill shall be construed to supersede any statute, regulation, or other provision of law of a state relating to the regulation of a private entity performing utility services, unless authorized under this bill.
- Cardenas Amendment #23 would instruct the Administrator of the Small Business Administration (SBA) to provide assistance to small businesses and small financial institutions to monitor information and

information systems, operate defensive measures, and share and receive cyber threat indicators and defensive measures. The SBA is required to submit to the president a report on the degree to which small businesses and small financial institutions are able to engage in cyber threat information sharing.

- Carson Amendment #7 would require the Inspector General of the Department of Homeland Security to conduct a review of the 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 such information.
- Mulvaney #22 would sunset the provisions of the bill after seven years.
- Jackson-Lee #13 would require the Government Accountability Office (GAO) to provide a report to Congress on the actions taken by the federal government to remove personal information from cyber threat indicators pursuant to the bill

COMMITTEE ACTION: This bill was introduced on March 24, 2015, by Representative Nunes and referred to the House Permanent Select Committee on Intelligence which reported and amended the bill on April 13, 2015.

ADMINISTRATION POSITION: A statement of administration policy can be found here. While largely in support, the administration has concerns with H.R. 1560's sweeping liability protections.

CONSTITUTIONAL AUTHORITY: Congress has the power to enact this legislation pursuant to the following: The intelligence and intelligence-related activities of the United States government support the national security interests of the United States, support and assist the armed forces of the United States, and support the President in the execution of the foreign policy of the United States. Article I, section 8 gives Congress the power "to provide for the common defense and general welfare of the United States." The Necessary and Proper Clause of that section also grants Congress the power "[t]o make all laws which shall be necessary and proper for carrying into Execution the foregoing Powers and all other Powers vested in this Constitution in the Government of the United States, or in any Department or Officer thereof."

NOTE*: RSC Legislative Bulletins are for informational purposes only and should not be taken as statements of support or opposition from the Republican Study Committee.*

###