THE REPUBLICAN STUDY COMMITTEE
Rep. Steve Scalise, Chairman
Paul Teller, Executive Director
202.226.9717
rsc.scalise.house.gov

Legislative Bulletin……..……April 17, 2013

Contents:

H.R. 624 – Cyber Intelligence Sharing and Protection Act, Rules Committee Print (Rogers, R-MI)

Order of Business: The bill is scheduled to be considered on Wednesday and Thursday, April 17th and 18th, 2013, under a structured rule (H. Res. 164). The rule provides for one hour of general debate equally divided and controlled by the Chairman and Ranking Member of the House Permanent Select Committee on Intelligence. It makes in order as original text for the purpose of amendment an amendment in the nature of a substitute consisting of the text of Rules Committee Print 113-7. It provides for one motion to recommit with or without instructions and makes 12 amendments in order described within this Legislative Bulletin. ***The House amended and passed H. Res. 164 to permit an additional amendment offered by Homeland Security Committee Chairman Michael McCaul (R-TX) to be in order and considered for 10 minutes described below.***

Summary: H.R. 624 amends Title XI of the National Security Act of 1947 with a new section to permit and encourage the voluntary sharing of cyber threat information and intelligence between the private sector and the intelligence community. Specifically, it requires the Director of National Intelligence to establish procedures for such sharing with certified private-sector entities to further the goal of protecting U.S. national security and private-property and to better defend against cyber attacks from nation-state and non-nation state bad actors.

The bill also allows cyber security providers to obtain access to, and voluntarily share, cyber security information when they have the express consent of a protected entity to do so. It prevents cyber threat information sharing from being used to gain an unfair competitive advantage to the detriment of a sharing private entity. The shared cybersecurity information is prohibited from public disclosure typically permitted under the Freedom of Information Act (FOIA, 5 U.S.C. 552) or from being used by the federal government for regulatory purposes.

Federal and state civil and criminal liability protections are granted to certified private entities that, in "good faith," use cyber security systems to "identify or obtain cyber threat information or for sharing such information" as authorized in the bill or for "decisions made for cybersecurity purposes on cyber threat information identified, obtained, or shared." The bill defines a "Lack of Good Faith" for purpose of this liability protection to include "…any act or omission taken with

intent to injure, defraud, or otherwise endanger any individual government entity, private entity, or utility."

The bill has a sunset date of all authorities granted in the bill of five years after enactment. Committee report #113-39 for H.R. 624 describes the purpose and context of the bill below:

> "…while much cybersecurity monitoring and threat information takes place today within the private sector, real and perceived legal barriers to such efforts substantially hamper the efforts of even those in the private sector with the best of intentions. The Committee determined that these issues are best resolved by providing clear, positive authority to permit the monitoring—by the private sector—of privately-owned and operated networks and systems for the purpose of detecting and mitigating cybersecurity threats and to permit the voluntary sharing of information about those threats and vulnerabilities with others, including entities within the private sector and with the federal government. While some have suggested that the private sector needs more regulation or that the government should directly help defend certain portions of the private sector, the Committee's view is that the protection of the private sector is best left in private hands and before reaching for a regulatory 'stick,' the government should provide as much intelligence as possible, in usable form, to better enable voluntary private sector efforts…such an approach…best protects individual privacy and takes advantage of the natural incentives built into our economic system, including harnessing private sector drive and innovation."[1]

In the 112th Congress, the House passed a similar cybersecurity bill (H.R. 3523) with the same name by a vote of 248-168 on April 26, 2012. The RSC Legislative Bulletin for that bill can be viewed here. On April 10, 2013, the House Permanent Select Committee on Intelligence (HPSI) met in both open and closed sessions and ordered H.R. 624 out favorably by a vote of 18-2.

Additional Background: When the House considered H.R. 3523 last April, a significant portion of the debate centered on balancing the privacy and civil liberties interests against the establishment of procedures for the intelligence community to assist private industry and the federal government combat cybersecurity threats. As such, the House adopted a number of amendments aimed at protecting Americans' privacy and civil liberty rights. The adopted amendments incorporated into the House-passed H.R. 3523 (and included in H.R. 624) are briefly described below:

- **Pompeo (R, KS)**—An amendment to clarify that the bill's liability protection for information sharing extends only to cyber threat information identified and obtained under the bill's authorities. ***Agreed to by voice vote.***
- **Rogers (R, MI)—**An amendment to clarify that regulatory information already required to be provided remains obtainable under the Freedom of Information Act. ***Passed by a vote of 412-0.***
- **Quayle (R, AZ)**—An amendment to limit the government's use of cyber threat information to only five purposes including: (1) cybersecurity; (2) investigation and prosecution of cybersecurity crimes; (3) protection of individuals from the danger of death or physical injury; (4) protection of minors from physical or psychological harm; and (5) protection of the national security of the United States. ***Passed by a vote of 410-3.***

[1] Page 11 of Committee Report #113-39.

- **Amash (R, MI)**—An amendment to prohibit the government from using library and book records, information on gun sales, tax records, education records and medical records that it receives from private entities under the bill. ***Passed by a vote of 415-0.***
- **Mulvaney (R, SC)**—An amendment providing authority to the federal government to create reasonable procedures to protect privacy and civil liberties and prohibiting the federal government from retaining or using information shared pursuant to the bill's authorities for anything other than a use permitted in the bill. ***Passed by a vote of 416-0.***
- **Flake (R, AZ)**—An amendment requiring a list of all federal agencies receiving information shared with the government in the Inspector General of the Office of Intelligence Community's required report. ***Agreed to by voice vote.***
- **Pompeo (R, KS)**—An amendment clarifying that the bill does not create any new authorities to any federal agency including the Department of Defense, National Security Agency, or the Department of Homeland Security or the Intelligence Community, to install, employ, or use cybersecurity systems on private sector networks. ***Agreed to by voice vote.***
- **Woodall (R, GA)**—An amendment ensuring that those entities that choose not to participate in the voluntary sharing authorities included in the bill are not subject to new liabilities. ***Agreed to by voice vote.***
- **Goodlatte (R, VA)**—An amendment narrowing the bill's definitions regarding the information that may be identified, obtained, and shared. ***Passed by a vote of 414-1.***
- **Mulvaney (R, SC)**—An amendment creating a sunset date for the authorities created in the bill of five years after enactment of the bill into law. ***Passed by a vote of 413-3.***

At the full HPSI committee markup of H.R. 624 on April 10, 2013, the committee adopted further amendments to the base bill to address additional privacy and civil liberties concerns described below:

- ***Langevin (D, RI)***—An amendment that establishes that the bill does not provide any new authority and prohibits private entities to "hack back" against any cyber security attackers. ***Passed by voice vote.***
- **Heck (R, NV)** & ***Himes (D, CT)***—An amendment limiting the use of cyber information shared with and in the private sector by the recipients of such information to only "cybersecurity purposes." The Committee report explains that information sharing envisioned in the bill could be used by the private sector to better secure their networks. Concerns about the private sector selling consumer information for marketing purposes and other non-cybersecurity purposes led to this amendment being adopted at the markup. ***Passed by voice vote.***
- ***Himes (D, CT)***—An amendment requiring the establishment of federal government minimization procedures on the impact on privacy and civil liberties and to reasonably limit the receipt, retention, use, and disclosure of cyber threat information associated with specific persons whom are not necessary to protect systems or networks from cyber threats in a timely manner. These procedures must be designed so as not to delay or impede the flow of cyber threat information necessary to defend against a cyber threat. ***Passed by voice vote.***
- ***Sewell (D, AL)***—An amendment striking the government's national security use provision, which leaves four permissible uses for the sharing of cyber threat information including (1) cybersecurity; (2) the investigation and prosecution of cyber crimes; (3)

protection from the danger of serious bodily harm; & (4) the protection of minors from child pornography, exploitation, or serious threats of physical safety. Last Congress, an amendment offered by former Rep. Ben Quayle narrowed these purposes down to five uses, which included a "national security purpose." Concerns had arisen that such a use gave the federal government broad authority to do anything it wanted with information received under the guise of national security. ***The Rep. Sewell amendment passed in the Committee markup by a voice vote.***

- ***Thompson (D, CA)***—An amendment adding a requirement for the Intelligence Community Inspector General to consult with the Department of Defense and Department of Justice Inspectors General as well as the Privacy and Civil Liberties Board in its reporting requirements included in the bill. Additionally, it adds a new report by senior privacy and civil liberties officers to provide more oversight and accountability within the federal government for authorities included in the bill. ***Passed by voice vote.***

Amendments to H.R. 624 Ruled in Order (each debatable for 10 minutes):

1. **Rogers (R, MI)** – **Manager's Amendment**: Removes the ability for any government policies or procedures to be developed by the Director of National Security, in consultation with the Secretary of Homeland Security and the Attorney General, to use shared information that identifies a person from library circulation records, library patron lists, book sales records, book customer lists, firearm sales records, tax return records, educational records, or medical records.
2. ***Connolly (D, VA)*** – Clarifies that classified cyber threat intelligence may only be used, retained, or further disclosed by a certified entity for cybersecurity purposes. This provision adds a fourth criteria to the previous three criteria requiring that such intelligence may only be (1) shared by an element of the intelligence community with a certified entity or a person with an appropriate security clearance; (2) shared consistent with the need to protect the national security of the United States; & (3) used by a certified entity in a manner which protects such cyber threat intelligence from unauthorized disclosure.
3. ***Schneider (D, IL)*** – Permits independent contractors (along with employees or officers of a certified entity) to be eligible for security clearance purposes envisioned under the bill.
4. ***Langevin (D, RI)*** – Replaces the phrase "local" with "political subdivision of a State" when exempting shared cyber threat information from disclosure under a non-federal law that requires public disclosure of information by a public or quasi-public entity.
5. ***Conyers (D, MI), Schakowsky (D, IL), Jackson-Lee (D, TX), Johnson (D, GA), & Holt (D, NJ)*** – Strikes the civil and criminal liability protection provided to protected entities, self-protected entities, and cybersecurity providers (as well as their officers, employees, or agents) for decisions made for cybersecurity purposes and based on cyber threat information identified, obtained, or shared in the bill.
6. **Amash (R, MI), Massie (R, KY),** ***Polis (D, CO),*** **& Broun (R, GA)** – Same amendment language as the Manager's Amendment #1 described above. A Heritage Foundation article here is informative about concerns related to the privacy of personal records this amendment seeks to address.
7. ***Sinema (D, AZ)*** – Includes the Inspector General (IG) of the Department of Homeland Security along with the Intelligence Community IG to submit an annual report on the

uses of shared intelligence information to the House Committee on Homeland Security, the Senate Committee on Homeland Security and Government Affairs, and the congressional intelligence committees.

8. ***Sanchez (D, CA)*** – Includes the Privacy Officer and the Officer for Civil Rights and Civil Liberties of the Department of Homeland Security in issuing a report on assessing the privacy and civil liberties impact of H.R. 624.
9. **LaMalfa (R, CA) & Rogers (R, MI)** – Adds a new section to the bill stating, "Nothing in this section shall be construed to authorize the Department of Defense or the National Security Agency or any other element of the intelligence community to target a United States person for surveillance."
10. **Paulsen (R, MN)** – Adds a Sense of Congress at the end of the bill stating, "It is the sense of Congress that international cooperation with regard to cybersecurity should be encouraged wherever possible under this Act and the amendments made by this Act."
11. **Barton (R, TX)** – Adds a new section at the end of the bill explaining that nothing in H.R. 624 shall be construed to provide new or alter any existing authority for an entity to sell personal information of a consumer to another entity for marketing purposes.
12. ***Jackson-Lee (D, TX)*** –Adds a new section at the end of the bill explaining that nothing in H.R. 624 shall be construed to provide authority to a department or agency of the federal government to require a federally-contracted cybersecurity provider to provide information services to provide information about cybersecurity incidents that do not pose a threat to the federal government's information.
13. **McCaul (R, TX), Rogers (R, MI),** ***Ruppersberger (D, MD), & Thompson (D, CA)*** **–** Provides that the President designate an entity within the Department of Homeland Security to be the primary civilian federal agency to receive cyber threat information shared by the private sector. It also requires the President to designate an entity within the Department of Justice as the primary civilian federal agency to receive cyber threat information related to cybersecurity crimes that is shared by the private sector. The amendment calls for the establishment of sharing procedures to ensure that cyber threat information shared with federal agencies is also shared with national security departments and agencies in real time to promote shared situational awareness.[2] Requires the Secretary of Homeland Security to jointly establish, review, report to Congress on, and provide oversight regarding privacy and civil liberties protections with other defense-related federal agency Directors and Secretaries. The base bill either required consultation with the Homeland Security Department (DHS) or did not include DHS in such activities.

Potential Conservative and Civil Liberties Concerns:

Private Industry Personally Identifiable Information (PII) Minimization: Despite requiring federal agencies to strip PII from cyber information it receives, the bill does not require private sector entities to make reasonable efforts to remove PII unrelated to any cybersecurity threats. Other cybersecurity legislative efforts in the Senate have included provisions requiring this "reasonable effort" standard for the private sector. The HPSI committee received testimony

[2] Defined on page 12 of the amendment as "an environment where cyber threat information is shared in real time between all designated Federal cyber operations centers to provide actionable information about all know cyber threats."

indicating that such a standard is technically feasible and not an onerous requirement. A related amendment failed in H.R. 624's committee markup.

Cyber Information Sharing with Security Agencies v. Civilian Agencies: Whether intelligence gathering agencies within the Department of Defense should be prohibited from being the initial recipient of cyber security information sharing rather than civilian agencies, such as the Department of Homeland Security, has generated some debate. An amendment promoting this approach failed in H.R. 624's committee markup. **Addressed by the new McCaul amendment.**

Broad Definitions of Good Faith/Lack of Good Faith Liability Protections: Liability protection from civil or criminal charges against private companies' cyber information sharing is triggered as long as no "lack of good faith" is present. The bill defines this phrase as including "any act or omission taken with intent to injure, defraud, or otherwise endanger any individual, government entity, private entity, or utility." Whether this standard is vague and leaves potential users harmed by recklessness or neglect without recourse has generated some debate.

Committee Action: House Permanent Select Committee on Intelligence Committee Chairman Mike Rogers (R, MI) and Ranking Member Dutch Ruppersberger *(D, MD)* introduced H.R. 624 on February 13, 2013. On April 10, 2013, the full committee reported the amended bill out favorably by a vote of 18-2.

Administration Position: The Administration released a Statement of Administration Policy (SAP) on April 16, 2012, stating that President Obama's senior advisors would recommend he veto the bill in its current form.

Cost to Taxpayers: The Congressional Budget Office (CBO) released a cost estimate for H.R. 624 on April 12, 2013, estimating that implementing the bill would have a discretionary cost of $20 million over the 2014-2018 period assuming necessary appropriations.

Outside Organizations: TechNet, whose members include Google, Yahoo, Cisco, Oracle, and Microsoft, has come out in support of the bill. Additionally, HPSI has posted a listing of over 60 groups in support of the bill. The National Association of Manufacturers (NAM) supports and may key vote the bill. Thirty four civil liberties and tech organizations, including the ACLU, Center for Democracy and Technology, Competitive Enterprise Institute (CEI), Electronic Freedom Foundation, etc., released a letter opposing the bill. Freedom Works also opposes the bill in its current form.

Does the Bill Expand the Size, Scope, or Influence of the Federal Government?: The bill expands the role of the federal government by increasing federal involvement in domestic, private-sector, cybersecurity measures.

Does the Bill Contain Any New State-Government, Local-Government, or Private-Sector Mandates?: CBO explains that the bill would impose intergovernmental and private-sector mandates, as defined in the Unfunded Mandates Reform Act (UMRA) by extending civil and criminal liability protection to entities and cybersecurity providers that share or use cyber threat information. Also, it would impose additional government mandates on state governments by preempting state disclosure and liability laws. CBO cannot determine if the annual UMRA threshold for private sector mandates would be exceeded ($150 million in 2013, adjusted for

inflation), but it estimates that mandates on public entities would fall below the annual UMRA threshold for intergovernmental mandates ($75 million in 2013, adjusted for inflation).

Does the Bill Contain Any Earmarks/Limited Tax Benefits/Limited Tariff Benefits?: The Committee report states, "Pursuant to clause 9 of rule XXI of the Rules of the House of Representatives, the Committee states that the bill as reported contains no congressional earmarks, limited tax benefits, or limited tariff benefits."

Constitutional Authority: The Constitutional Authority Statement accompanying the bill upon introduction states: "Congress has the power to enact this legislation pursuant to the following: The constitutional authority on which this bill rests is the power of Congress to make all laws necessary and proper for executing powers vested by the Constitution in the Government of the United States, as enumerated in Article I, Section 8, Clause 18 of the United States Constitution."

RSC Staff Contact: Joe Murray, Joe.Murray@mail.house.gov, or 6-0678.

***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.*