112TH CONGRESS
2d Session
HOUSE OF REPRESENTATIVES
REPORT
112–454

PROVIDING FOR CONSIDERATION OF THE BILL (H.R. 3523) TO PROVIDE FOR THE SHARING OF CERTAIN CYBER THREAT INTELLIGENCE AND CYBER THREAT INFORMATION BETWEEN THE INTELLIGENCE COMMUNITY AND CYBERSECURITY ENTITIES, AND FOR OTHER PURPOSES; PROVIDING FOR CONSIDERATION OF MOTIONS TO SUSPEND THE RULES; PROVIDING FOR CONSIDERATION OF THE BILL (H.R. 4628) TO EXTEND STUDENT LOAN INTEREST RATES FOR UNDERGRADUATE FEDERAL DIRECT STAFFORD LOANS; AND FOR OTHER PURPOSES

APRIL 25, 2012.—Referred to the House Calendar and ordered to be printed

---

Mr. NUGENT, from the Committee on Rules, submitted the following

R E P O R T

[To accompany H. Res. 631]

The Committee on Rules, having had under consideration House Resolution 631, by a nonrecord vote, report the same to the House with the recommendation that the resolution be adopted.

SUMMARY OF PROVISIONS OF THE RESOLUTION

The resolution provides for consideration of H.R. 3523, the Cyber Intelligence Sharing and Protection Act of 2011, under a structured rule. The resolution provides one hour of general debate equally divided and controlled by the chair and ranking minority member of the Permanent Select Committee on Intelligence. The resolution waives all points of order against consideration of the bill. The resolution makes in order as original text for purpose of amendment the amendment in the nature of a substitute consisting of the text of Rules Committee Print 112–20 and provides that it shall be considered as read. The resolution waives all points of order against the amendment in the nature of a substitute. The resolution makes in order only those amendments printed in this report. Each such amendment may be offered only in the order printed in this report, may be offered only by a Member designated in this report, shall be considered as read, shall be debatable for the time specified in this report equally divided and controlled by the proponent and an opponent, shall not be subject to amendment, and shall not be subject to a demand for division of the question in the House or in the Committee of the Whole. The resolution waives all points of order against the amendments printed in this report. The resolution provides one motion to recommit with or without instructions.

Section 2 of the resolution provides that it shall be in order at any time through the legislative day of April 27, 2012, for the Speaker to entertain motions that the House suspend the rules, as though under clause 1 of rule XV, relating to the following measures: H.R. 2096, the Cybersecurity Enhancement Act of 2011; H.R. 3834, the Advancing America's Networking and Information Technology Research and Development Act of 2012; and H.R. 4257, the Federal Information Security Amendments Act of 2012.

Section 3 of the resolution provides for consideration of H.R. 4628, the Interest Rate Reduction Act, under a closed rule. The resolution provides one hour of debate equally divided and controlled by the chair and ranking minority member of the Committee on Education and the Workforce. The resolution waives all points of order against consideration of the bill and provides that it shall be considered as read. The resolution waives all points of order against provisions in the bill. The resolution provides one motion to recommit.

Section 4 of the resolution provides that the Committee on Appropriations may, at any time before 6 p.m. on Wednesday, May 2, 2012, file privileged reports to accompany measures making appropriations for the fiscal year ending September 30, 2013.

EXPLANATION OF WAIVERS

The waiver of all points of order against consideration of H.R. 3523 includes a waiver of clause 3(c)(4) of rule XIII, which requires a statement of general performance goals and objectives. The report filed by the Permanent Select Committee on Intelligence did not adequately fulfill this requirement.

Although the resolution waives all points of order against the amendment in the nature of a substitute to H.R. 3523 made in order as original text, the Committee is not aware of any points of order. The waiver is prophylactic in nature.

Although the resolution waives all points of order against the amendments printed in this report, the Committee is not aware of any points of order. The waiver is prophylactic in nature.

The waiver of all points of order against consideration of H.R. 4628 includes a waiver of clause 10 of rule XXI, prohibiting the consideration of a measure if the provisions of such measure have the net effect of increasing mandatory spending for the period of either the first five-year or ten-year period. While it is expected that H.R. 4628 would be in violation of the rule over the first five-year period, it is expected to have a net decrease in mandatory spending over the ten-year period.

The waiver of all points of order against consideration of H.R. 4628 also includes a waiver of section 302(f) of the Congressional Budget Act of 1974, prohibiting the consideration of a measure which causes the applicable allocation of new budget authority under subsections 302(a) or (b) to be exceeded.

If H.R. 4628 is considered before Friday, April 27, 2012, the waiver of all points of order will include a waiver of clause 11 of rule XXI, prohibiting the consideration of an unreported bill or joint resolution until the third calendar day on which it has been available.

Although the resolution waives all points of order against provisions in the H.R. 4628, the Committee is not aware of any points of order. The waiver is prophylactic in nature.

SUMMARY OF THE AMENDMENTS TO H.R. 3523 MADE IN ORDER

1. Langevin (RI), Lungren (CA): Would expand eligibility to participate in the voluntary information sharing program created in the bill to include critical infrastructure owners and operators, which allows entities that are not entirely privately owned, such as airports, utilities, and public transit systems, to receive vital cybersecurity information and better secure their networks against cyber threats. (10 minutes)

2. Conyers (MI): Would strike the exemption from criminal liability, strike the civil liability exemption for decisions made based upon cyber threat information identified, obtained, or shared under the bill, and ensure that those who negligently cause injury through the use of cybersecurity systems or the sharing of information are not exempt from potential civil liability. (10 minutes)

3. Pompeo (KS): Would make clear in the bill's liability provision that the reference to the use of cybersecurity systems is the use of such systems to identify and obtain cyber threat information. (10 minutes)

4. Rogers, Mike (MI), Ruppersberger (MD), Issa (CA), Langevin (RI): Would make clear that regulatory information already required to be provided remains FOIAable under current law. (10 minutes)

5. Jackson Lee (TX): Would authorize the Secretary to intercept and deploy countermeasure with regard to system traffic for cybersecurity purposes in effect identification of cybersecurity risks to federal systems. (10 minutes)

6. Quayle (AZ), Eshoo (CA), Thompson, Mike (CA), Broun (GA): Would limit government use of shared cyber threat information to only 5 purposes: (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. (10 minutes)

7. Amash (MI), Labrador (ID), Paul (TX), Nadler (NY), Polis (CO): Would prohibit the federal government from using, inter alia, library records, firearms sales records, and tax returns that it receives from private entities under CISPA. (10 minutes)

8. Mulvaney (SC), Dicks (WA): Would provide clear authority to the government to create reasonable procedures to protect privacy and civil liberties, consistent with the need of the government to protect federal systems and cybersecurity. Would also prohibit the federal government from retaining or using information shared pursuant to paragraph (b)(1) for anything other than a use permitted under paragraph (c)(1). (10 minutes)

9. Flake, Jeff (AZ): Would add a requirement to include a list of all federal agencies receiving information shared with the government in the report by the Inspector General of the Intelligence Community required under the legislation. (10 minutes)

10. Richardson (CA): Would make explicit that nothing in the legislation would prohibit a department or agency of the federal

government from providing cyber threat information to owners and operators of critical infrastructure. (10 minutes)

11. Pompeo (KS): Would clarify that nothing in the bill would alter existing authorities or provide new authority to any federal agency, including DOD, NSA, DHS or the Intelligence Community to install, employ, or otherwise use cybersecurity systems on private sector networks. (10 minutes)

12. Woodall (GA): Would ensure that those who choose not to participate in the voluntary program authorized by this bill are not subject to new liabilities. (10 minutes)

13. Goodlatte (VA): Would narrow definitions in the bill regarding what information may be identified, obtained, and shared. (10 minutes)

14. Turner (OH): Would make a technical correction to definitions in Section 2(g) to provide consistency with other cyber security policies within the Executive branch and the Department of Defense. (10 minutes)

15. Mulvaney (SC): Would sunset the provisions of the bill five years after the date of enactment. (10 minutes)

16. Paulsen (MN): Would encourage international cooperation on cyber security where feasible. (10 minutes)

TEXT OF AMENDMENTS TO H.R. 3523 MADE IN ORDER

1. AN AMENDMENT TO BE OFFERED BY REPRESENTATIVE LANGEVIN OF RHODE ISLAND OR HIS DESIGNEE, DEBATABLE FOR 10 MINUTES

Page 1, line 13, strike "UTILITIES" and insert "CRITICAL INFRASTRUCTURE OWNERS AND OPERATORS".

Page 2, line 1, strike "utilities" and insert "critical infrastructure owners and operators".

Page 3, line 13, strike "utility" and insert "critical infrastructure owner or operator".

Page 3, line 16, strike "utility" each place it appears and insert "critical infrastructure owner or operator".

Page 17, strike lines 12 through 16.

---

2. AN AMENDMENT TO BE OFFERED BY REPRESENTATIVE CONYERS JR. OF MICHIGAN OR HIS DESIGNEE, DEBATABLE FOR 10 MINUTES

Page 8, beginning on line 11 strike "or criminal".

Page 8, strike lines 17 through 23 and insert the following: "good faith for using cybersecurity systems or sharing information in accordance with this section unless such protected entity, self-protected entity, cyber security provider, or an officer, agent, or employee of a cyber security provider negligently shares information obtained in accordance with this section, and that negligence proximately causes injury.".

---

3. AN AMENDMENT TO BE OFFERED BY REPRESENTATIVE POMPEO OF KANSAS OR HIS DESIGNEE, DEBATABLE FOR 10 MINUTES

Page 8, beginning on line 18, strike "or sharing information" and insert "to identify or obtain cyber threat information or for sharing such information".

---

4. AN AMENDMENT TO BE OFFERED BY REPRESENTATIVE ROGERS OF MICHIGAN OR HIS DESIGNEE, DEBATABLE FOR 10 MINUTES

Page 9, beginning on line 2, strike "affect any" and insert "affect—".

Page 9, strike lines 3 through 5 and insert the following:

"(A) any requirement under any other provision of law for a person or entity to provide information to the Federal Government; or

"(B) the applicability of other provisions of law, including section 552 of title 5, United States Code (commonly known as the 'Freedom of Information Act'), with respect to information required to be provided to the Federal Government under such other provision of law.

---

5. AN AMENDMENT TO BE OFFERED BY REPRESENTATIVE JACKSON LEE OF TEXAS OR HER DESIGNEE, DEBATABLE FOR 10 MINUTES

Page 9, after line 5, insert the following:

"(c) CYBERSECURITY OPERATIONAL ACTIVITY.—

"(1) IN GENERAL.—In receiving information authorized to be shared with the Federal Government under this section, the Secretary of Homeland Security is authorized, notwithstanding any other provision of law, to acquire, intercept, retain, use, and disclose communications and other system traffic that are transiting to or from or stored on Federal systems and to deploy countermeasures with regard to such communications and system traffic for cybersecurity purposes provided that the Secretary certifies that—

"(A) such acquisitions, interceptions, and countermeasures are reasonable necessary for the purpose of protection Federal systems from cybersecurity threats;

"(B) the content of communications will be collected and retained only when the communication is associated with known or reasonably suspected cybersecurity threat, and communications and system traffic will not be subject to the operation of a countermeasure unless associated with such threats;

"(C) information obtained pursuant to activities authorized under this subsection will only be retained, used or disclosed to protect Federal systems from cybersecurity threats, mitigate against such threats, or, with the approval of the Attorney General, for law enforcement purposes when the information is evidence of a crime which has been, is being, or is about to be committed; and

"(D) notice has been provided to users of Federal systems concerning the potential for acquisition, interception, retention, use, and disclosure of communications and other system traffic.

"(2) CONTRACTS.—The Secretary may enter into contracts or other agreements, or otherwise request and obtain the assistance of, private entities that provide electronic communication or cybersecurity services to acquire, intercept, retain, use, and disclose communications and other system traffic consistent with paragraph (1).

"(3) PRIVILEGED COMMUNICATIONS.—No otherwise privileged communication obtained in accordance with, or in violation of, this section shall lose its privileged character.

"(4) POLICIES AND PROCEDURES.—The Secretary of Homeland Security shall establish policies and procedures that—

"(A) minimize the impact on privacy and civil liberties, consistent with the need to protect Federal systems and critical information infrastructure from cybersecurity threats and mitigate cybersecurity threats;

"(B) reasonably limit the acquisition, interception, retention, use, and disclosure of communications, records, system traffic, or other information associated with specific persons consistent with the need to carry out the responsibilities of this section, including establishing a process for the timely destruction on recognition of communications, records, system traffic, or other information that is acquired or intercepted pursuant to this section that does not reasonably appear to be related to protecting Federal systems and critical information infrastructure from cybersecurity threats and mitigating cybersecurity threats;

"(C) include requirements to safeguard communications, records, system traffic, or other information that can be used to identify specific persons from unauthorized access or acquisition; and

"(D) protect the confidentiality of disclosed communications, records, system traffic, or other information associated with specific persons to the greatest extent practicable and require recipients of such information to be informed that the communications, records, system traffic, or other information disclosed may only be used for protecting information systems against cybersecurity threats, mitigating against cybersecurity threats, or law enforcement purposes when the information is evidence of a crime that has been, is being, or is about to be committed, as specified by the Secretary.

Page 14, after line 24, insert the following:

"(2) COUNTERMEASURE.—The term 'countermeasure' means an automated action with defensive intent to modify or block data packets associated with electronic or wire communications, internet traffic, program code, or other system traffic transiting to or from or stored on an information system to counteract a cybersecurity threat.".

---

6. AN AMENDMENT TO BE OFFERED BY REPRESENTATIVE QUAYLE OF ARIZONA OR HIS DESIGNEE, DEBATABLE FOR 10 MINUTES

Page 9, strike lines 8 through 18 and insert the following:

"(1) LIMITATION.—The Federal Government may use cyber threat information shared with the Federal Government in accordance with subsection (b)—

"(A) for cybersecurity purposes;

"(B) for the investigation and prosecution of cybersecurity crimes;

"(C) for the protection of individuals from the danger of death or serious bodily harm and the investigation and

prosecution of crimes involving such danger of death or serious bodily harm;

"(D) for the protection of minors from child pornography, any risk of sexual exploitation, and serious threats to the physical safety of such minor, including kidnapping and trafficking and the investigation and prosecution of crimes involving child pornography, any risk of sexual exploitation, and serious threats to the physical safety of minors, including kidnapping and trafficking, and any crime referred to in 2258A(a)(2) of title 18, United States Code; or

"(E) to protect the national security of the United States.

Page 16, before line 1 insert the following:

"(4) CYBERSECURITY CRIME.—The term 'cybersecurity crime' means—

"(A) a crime under a Federal or State law that involves—

"(i) efforts to degrade, disrupt, or destroy a system or network;

"(ii) efforts to gain unauthorized access to a system or network; or

"(iii) efforts to exfiltrate information from a system or network without authorization; or

"(B) the violation of a provision of Federal law relating to computer crimes, including a violation of any provision of title 18, United States Code, created or amended by the Computer Fraud and Abuse Act of 1986 (Public Law 99–474).".

---

7. AN AMENDMENT TO BE OFFERED BY REPRESENTATIVE AMASH OF MICHIGAN OR HIS DESIGNEE, DEBATABLE FOR 10 MINUTES

Page 10, after line 10, insert the following new paragraph:

"(4) PROTECTION OF SENSITIVE PERSONAL DOCUMENTS.—The Federal Government may not use the following information, containing information that identifies a person, shared with the Federal Government in accordance with subsection (b):

"(A) Library circulation records.

"(B) Library patron lists.

"(C) Book sales records.

"(D) Book customer lists.

"(E) Firearms sales records.

"(F) Tax return records.

"(G) Educational records.

"(H) Medical records.

---

8. AN AMENDMENT TO BE OFFERED BY REPRESENTATIVE MULVANEY OF SOUTH CAROLINA OR HIS DESIGNEE, DEBATABLE FOR 10 MINUTES

Page 10, after line 10 insert the following:

"(4) NOTIFICATION OF NON-CYBER THREAT INFORMATION.—If a department or agency of the Federal Government receiving information pursuant to subsection (b)(1) determines that such information is not cyber threat information, such department

or agency shall notify the entity or provider sharing such information pursuant to subsection (b)(1).

"(5) RETENTION AND USE OF CYBER THREAT INFORMATION.—No department or agency of the Federal Government shall retain or use information shared pursuant to subsection (b)(1) for any use other than a use permitted under subsection (c)(1).

"(6) PROTECTION OF INDIVIDUAL INFORMATION.—The Federal Government may, consistent with the need to protect Federal systems and critical information infrastructure from cybersecurity threats and to mitigate such threats, undertake reasonable efforts to limit the impact on privacy and civil liberties of the sharing of cyber threat information with the Federal Government pursuant to this subsection.

Page 14, after line 13, insert the following:

"(4) USE AND RETENTION OF INFORMATION.—Nothing in this section shall be construed to authorize, or to modify any existing authority of, a department or agency of the Federal Government to retain or use information shared pursuant to subsection (b)(1) for any use other than a use permitted under subsection (c)(1).".

---

9. AN AMENDMENT TO BE OFFERED BY REPRESENTATIVE FLAKE OF ARIZONA OR HIS DESIGNEE, DEBATABLE FOR 10 MINUTES

Page 12, after line 18, insert the following new subparagraph:

"(E) a list of the department or agency receiving such information;

---

10. AN AMENDMENT TO BE OFFERED BY REPRESENTATIVE RICHARDSON OF CALIFORNIA OR HER DESIGNEE, DEBATABLE FOR 10 MINUTES

Page 14, after line 6, insert the following new subparagraph:

"(C) prohibit a department or agency of the Federal Government from providing cyber threat information to owners and operators of critical infrastructure;

---

11. AN AMENDMENT TO BE OFFERED BY REPRESENTATIVE POMPEO OF KANSAS OR HIS DESIGNEE, DEBATABLE FOR 10 MINUTES

Page 14, after line 13, insert the following:

"(4) LIMITATION ON FEDERAL GOVERNMENT USE OF CYBERSECURITY SYSTEMS.—Nothing in this section shall be construed to provide additional authority to, or modify an existing authority of, any entity to use a cybersecurity system owned or controlled by the Federal Government on a private-sector system or network to protect such private-sector system or network.".

---

12. AN AMENDMENT TO BE OFFERED BY REPRESENTATIVE WOODALL OF GEORGIA OR HIS DESIGNEE, DEBATABLE FOR 10 MINUTES

Page 14, after line 13 insert the following:

"(4) NO LIABILITY FOR NON-PARTICIPATION.—Nothing in this section shall be construed to subject a protected entity, self-

protected entity, cyber security provider, or an officer, employee, or agent of a protected entity, self-protected entity, or cybersecurity provider, to liability for choosing not to engage in the voluntary activities authorized under this section.

---

13. AN AMENDMENT TO BE OFFERED BY REPRESENTATIVE GOODLATTE OF VIRGINIA OR HIS DESIGNEE, DEBATABLE FOR 10 MINUTES

Page 14, after line 14 insert the following:

"(1) AVAILABILITY.—The term 'availability' means ensuring timely and reliable access to and use of information.

Page 15, strike lines 1 through 25 and insert the following:

"(2) CONFIDENTIALITY.—The term 'confidentiality' means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information.

"(3) CYBER THREAT INFORMATION.—

"(A) IN GENERAL.—The term 'cyber threat information' means information directly pertaining to—

"(i) a vulnerability of a system or network of a government or private entity;

"(ii) a threat to the integrity, confidentiality, or availability of a system or network of a government or private entity or any information stored on, processed on, or transiting such a system or network;

"(iii) efforts to degrade, disrupt, or destroy a system or network of a government or private entity; or

"(iv) efforts to gain unauthorized access to a system or network of a government or private entity, including to gain such unauthorized access for the purpose of exfiltrating information stored on, processed on, or transiting a system or network of a government or private entity.

"(B) EXCLUSION.— Such term does not include information pertaining to efforts to gain unauthorized access to a system or network of a government or private entity that solely involve violations of consumer terms of service or consumer licensing agreements and do not otherwise constitute unauthorized access.

"(4) CYBER THREAT INTELLIGENCE.—

"(A) IN GENERAL.—The term 'cyber threat intelligence' means intelligence in the possession of an element of the intelligence community directly pertaining to—

"(i) a vulnerability of a system or network of a government or private entity;

"(ii) a threat to the integrity, confidentiality, or availability of a system or network of a government or private entity or any information stored on, processed on, or transiting such a system or network;

"(iii) efforts to degrade, disrupt, or destroy a system or network of a government or private entity; or

"(iv) efforts to gain unauthorized access to a system or network of a government or private entity, including to gain such unauthorized access for the purpose

of exfiltrating information stored on, processed on, or transiting a system or network of a government or private entity.

"(B) EXCLUSION.—Such term does not include intelligence pertaining to efforts to gain unauthorized access to a system or network of a government or private entity that solely involve violations of consumer terms of service or consumer licensing agreements and do not otherwise constitute unauthorized access.

Page 16, strike line 5 and all that follows through page 17, line 2, and insert the following:

"(5) CYBERSECURITY PURPOSE.—

"(A) IN GENERAL.—The term 'cybersecurity purpose' means the purpose of ensuring the integrity, confidentiality, or availability of, or safeguarding, a system or network, including protecting a system or network from—

"(i) a vulnerability of a system or network;

"(ii) a threat to the integrity, confidentiality, or availability of a system or network or any information stored on, processed on, or transiting such a system or network;

"(iii) efforts to degrade, disrupt, or destroy a system or network; or

"(iv) efforts to gain unauthorized access to a system or network, including to gain such unauthorized access for the purpose of exfiltrating information stored on, processed on, or transiting a system or network.

"(B) EXCLUSION.—Such term does not include the purpose of protecting a system or network from efforts to gain unauthorized access to such system or network that solely involve violations of consumer terms of service or consumer licensing agreements and do not otherwise constitute unauthorized access.

"(6) CYBERSECURITY SYSTEM.—

"(A) IN GENERAL.—The term 'cybersecurity system' means a system designed or employed to ensure the integrity, confidentiality, or availability of, or safeguard, a system or network, including protecting a system or network from—

"(i) a vulnerability of a system or network;

"(ii) a threat to the integrity, confidentiality, or availability of a system or network or any information stored on, processed on, or transiting such a system or network;

"(iii) efforts to degrade, disrupt, or destroy a system or network; or

"(iv) efforts to gain unauthorized access to a system or network, including to gain such unauthorized access for the purpose of exfiltrating information stored on, processed on, or transiting a system or network.

"(B) EXCLUSION.—Such term does not include a system designed or employed to protect a system or network from efforts to gain unauthorized access to such system or network that solely involve violations of consumer terms of

service or consumer licensing agreements and do not otherwise constitute unauthorized access.

Page 17, after line 2 insert the following:

"(7) INTEGRITY.—The term 'integrity' means guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity.

---

14. AN AMENDMENT TO BE OFFERED BY REPRESENTATIVE TURNER OF OHIO OR HIS DESIGNEE, DEBATABLE FOR 10 MINUTES

Page 15, line 7, insert "deny access to or" before "degrade".
Page 15, line 20, insert "deny access to or" before "degrade".
Page 16, line 10, insert "deny access to or" before "degrade".
Page 16, line 21, insert "deny access to or" before "degrade".

---

15. AN AMENDMENT TO BE OFFERED BY REPRESENTATIVE MULVANEY OF SOUTH CAROLINA OR HIS DESIGNEE, DEBATABLE FOR 10 MINUTES

At the end of the bill, add the following new section:

SEC. 3. SUNSET.

Effective on the date that is five years after the date of the enactment of this Act—

(1) section 1104 of the National Security Act of 1947, as added by section 2(a) of this Act, is repealed; and

(2) the table of contents in the first section of the National Security Act of 1947, as amended by section 2(d) of this Act, is amended by striking the item relating to section 1104, as added by such section 2(d).

---

16. AN AMENDMENT TO BE OFFERED BY REPRESENTATIVE PAULSEN OF MINNESOTA OR HIS DESIGNEE, DEBATABLE FOR 10 MINUTES

At the end of the bill, add the following new section:

SEC. 3. INTERNATIONAL COOPERATION.

International cooperation with regard to cybersecurity should be encouraged wherever possible under this Act and the amendments made by this Act.

○