114TH CONGRESS
1st Session
HOUSE OF REPRESENTATIVES
REPORT
114–88

PROVIDING FOR CONSIDERATION OF THE BILL (H.R. 1560) TO IMPROVE CYBERSECURITY IN THE UNITED STATES THROUGH ENHANCED SHARING OF INFORMATION ABOUT CYBERSECURITY THREATS, AND FOR OTHER PURPOSES, AND PROVIDING FOR CONSIDERATION OF THE BILL (H.R. 1731) TO AMEND THE HOMELAND SECURITY ACT OF 2002 TO ENHANCE MULTI-DIRECTIONAL SHARING OF INFORMATION RELATED TO CYBERSECURITY RISKS AND STRENGTHEN PRIVACY AND CIVIL LIBERTIES PROTECTIONS, AND FOR OTHER PURPOSES

APRIL 21, 2015.—Referred to the House Calendar and ordered to be printed

Mr. COLLINS of Georgia, from the Committee on Rules, submitted the following

R E P O R T

[To accompany H. Res. 212]

The Committee on Rules, having had under consideration House Resolution 212, 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. 1560, the Protecting Cyber Networks Act, 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 the purposes of amendment the amendment in the nature of a substitute recommended by the Permanent Select Committee on Intelligence now printed in the bill and provides that it shall be considered as read. The resolution waives all points of order against the amendment in a nature of a substitute. The resolution makes in order only those further amendments printed in part A of 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 part A of this report. The reso-

lution provides one motion to recommit with or without instructions.

Section 2 of the resolution provides for consideration of H.R. 1731, the National Cybersecurity Protection Advancement Act of 2015, 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 Committee on Homeland Security. The resolution waives all points of order against consideration of the bill. The resolution 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 114–12 and provides that it shall be considered as read. The resolution waives all points of order against that amendment in the nature of a substitute. The resolution makes in order only those further amendments printed in part B of 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 part B of this report. The resolution provides one motion to recommit with or without instructions.

Section 3 of the resolution directs the Clerk to, in the engrossment of H.R. 1560, add the text of H.R. 1731, as passed by the House, as a new matter at the end of H.R. 1560 and make conforming modifications in the engrossment. The resolution provides that upon the addition of the text of H.R. 1731, as passed by the House, to the engrossment of H.R. 1560, H.R. 1731 shall be laid on the table.

EXPLANATION OF WAIVERS

The waiver of all points of order against consideration of H.R. 1560 includes a waiver of clause 3(e)(1) of rule XIII (Ramseyer), requiring a committee report accompanying a bill amending or repealing statutes to show, by typographical device, parts of statute affected.

Although the resolution waives all points of order against the amendment in the nature of a substitute to H.R. 1560 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 to H.R. 1560 printed in part A of 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. 1731 includes a waiver of clause 3(e)(1) of rule XIII (Ramseyer), requiring a committee report accompanying a bill amending or repealing statutes to show, by typographical device, parts of statute affected.

The waiver of all points of order against the amendment in the nature of a substitute to H.R. 1731 made in order as original text includes a waiver of clause 7 of rule XVI, which requires that no motion or proposition on a subject different from that under consid-

eration shall be admitted under color of amendment. It is important to note that while the waiver is necessary, Rules Committee Print 114–12 contains the text of H.R. 1731 as reported.

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

The waivers of clause 3(e)(1) of rule XIII is provided because the submissions provided by the committees were insufficient to meet the standards established by the rule in its current form. The Committee on Rules continues to work with the House Office of Legislative Counsel and committees to determine the steps necessary to comply with the updated rule.

SUMMARY OF THE AMENDMENTS TO H.R. 1560 IN PART A MADE IN ORDER

1. Nunes (CA): 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. (10 minutes)

2. Cárdenas, Tony (CA): Instructs the 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 out reach to encourage small business and small financial institution participation. (10 minutes)

3. Carson (IN): 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. (10 minutes)

4. Mulvaney (SC): Sunsets the provisions of the bill after 7 years. (10 minutes)

5. Jackson Lee (TX), Polis (CO): 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. (10 minutes)

SUMMARY OF THE AMENDMENTS TO H.R. 1731 IN PART B MADE IN ORDER

1. McCaul (TX), Ratcliffe (TX): Makes technical corrections and further clarifies the provisions of the bill. (10 minutes)

2. Katko (NY), Lofgren (CA), Eshoo (CA), McClintock (CA): Amends Section 226 of the Homeland Security Act of 2002 by refining the definition of cyber "incident" to explicitly restrict information sharing to incidents that are directly related to protecting information systems. (10 minutes)

3. Langevin (RI): Clarifies that the term "cybersecurity risk" does not apply to actions solely involving violations of consumer terms of service or consumer licensing agreements. (10 minutes)

4. Jackson Lee (TX): Ensures that federal agencies supporting cybersecurity efforts of private sector entities remain current on innovation; industry adoption of new technologies; and industry best practices as they relate to industrial control systems. (10 minutes)

5. Castro (TX): Makes self-assessment tools available to small and medium-sized businesses to determine their level of cybersecurity readiness. (10 minutes)

6. Castro (TX), Cuellar (TX), Doggett (TX), Hurd (TX), Smith, Lamar (TX): Codifies the establishment of the National Cybersecurity Preparedness Consortium (NCPC) made up of university partners and other stakeholders who proactively coordinate to assist state and local officials in cyber security preparation and prevention of cyber attacks. (10 minutes)

7. Hurd (TX): Authorizes the existing Einstein 3A (E3A) program. (10 minutes)

8. Mulvaney (SC): Sunsets the provisions of the bill after 7 years. (10 minutes)

9. Hahn (CA): Directs the Secretary of Homeland Security to submit a report to Congress containing assessments of risks and shortfalls along with recommendations regarding cybersecurity at most at risk ports. (10 minutes)

10. Jackson Lee (TX), Polis (CO): Provides for a Government Accountability Office (GAO) report to Congress 5 years after enactment to assess the impact of this act on privacy and civil liberties. (10 minutes)

11. Jackson Lee (TX): Requires a report to Congress on the best means for aligning federally funded cybersecurity research and development with private sector efforts to protect privacy and civil liberties while assuring security and resilience of the Nation's critical infrastructure. (10 minutes)

PART A—TEXT OF AMENDMENTS TO H.R. 1560 MADE IN ORDER

1. AN AMENDMENT TO BE OFFERED BY REPRESENTATIVE NUNES OF CALIFORNIA OR HIS DESIGNEE, DEBATABLE FOR 10 MINUTES

Page 5, beginning line 16, strike "in accordance with" and insert "under".

Page 9, line 2, strike "and is limited to".

Page 9, beginning line 14, strike "the intentional or reckless operation of any" and insert "a".

Page 9, beginning line 17, strike "substantially harms, or initiates a new action, process, or procedure on" and insert ", or substantially harms".

Page 12, beginning line 2, strike "a non-Federal entity, if authorized by applicable law or regulation other than this Act, from sharing" and insert "otherwise lawful sharing by a non-Federal entity of".

Page 14, line 18, insert "or defensive measure" before "shared".

Page 23, line 19, strike "section 3(c)(2)" and insert "this Act".

Page 24, line 15, strike "section 552(b)(3)(B)" and insert "section 552(b)(3)".

Page 25, line 13, insert "investigating," after "to,".

Page 25, line 18, insert "investigating, prosecuting," after "to,".

Page 27, line 23, strike "subsection" and insert "section".

Page 27, beginning line 24, strike "of the violation" and all that follows through the period on page 28, line 2, and insert the following: "on which the cause of action arises.".

Page 28, line 4, strike "subsection" and insert "section".

Page 28, line 14, strike "in good faith".

Page 28, beginning line 22, strike "in good faith".
Page 33, line 16, insert "of such Act" before the semicolon.
Page 33, line 19, insert "of such Act" before the period.
Page 38, line 20, strike "threats," and insert the following: "threats to the national security and economy of the United States,".
Page 44, line 2, strike "activiy" and insert "activity".
Page 44, after line 23, insert the following:

(3) STATE REGULATION OF UTILITIES.—Except as provided by section 3(d)(4)(B), nothing in this Act or the amendments made by this Act shall be construed to supersede any statute, regulation, or other provision of law of a State or political subdivision of a State relating to the regulation of a private entity performing utility services, except to the extent such statute, regulation, or other provision of law restricts activity authorized under this Act or the amendments made by this Act.

Strike section 10.
Page 51, line 13, strike "electric".

---

2. AN AMENDMENT TO BE OFFERED BY REPRESENTATIVE CÁRDENAS OF CALIFORNIA OR HIS DESIGNEE, DEBATABLE FOR 10 MINUTES

Page 15, after line 7, insert the following:
(f) SMALL BUSINESS PARTICIPATION.—

(1) ASSISTANCE.—The Administrator of the Small Business Administration shall 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 under this section

(2) REPORT.—Not later than one year after the date of the enactment of this Act, the Administrator of the Small Business Administration shall 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 under this section. Such report shall include the recommendations of the Administrator for improving the ability of such businesses and institutions to engage in cyber threat information sharing and to use shared information to defend their networks.

(3) OUTREACH.—The Federal Government shall conduct outreach to small businesses and small financial institutions to encourage such businesses and institutions to exercise their authority under this section.

---

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

Page 37, after line 16, insert the following new clause:

(v) 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.

---

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

Add at the end the following new section:

SEC. 12. SUNSET.

This Act and the amendments made by this Act shall terminate on the date that is seven years after the date of the enactment of this Act.

---

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

Add at the end the following:

SEC. 12. COMPTROLLER GENERAL REPORT ON REMOVAL OF PERSONAL IDENTIFYING INFORMATION.

(a) REPORT.—Not later than three years after the date of the enactment of this Act, the Comptroller General of the United States shall submit to Congress a report on the actions taken by the Federal Government to remove personal information from cyber threat indicators pursuant to section 4(b).

(b) FORM.—The report under subsection (a) shall be submitted in unclassified form, but may include a classified annex.

PART B—TEXT OF AMENDMENTS TO H.R. 1731 MADE IN ORDER

1. AN AMENDMENT TO BE OFFERED BY REPRESENTATIVE MCCAUL OF TEXAS OR HIS DESIGNEE, DEBATABLE FOR 10 MINUTES

In section 2, strike the following:

(a) DEFINITIONS.—

(1) IN GENERAL.—Subsection (a) of the second section 226

In section 2, insert before subsection (b), the following:

(a) IN GENERAL.—Subsection (a) of the second section 226

In section 2(a), redesignate proposed subparagraphs (A) through (C) as proposed paragraphs (1) through (3), respectively, and move such provisions two ems to the left.

Page 3, line 23, insert ", or the purpose of identifying the source of a cybersecurity risk or incident" before the semicolon at the end.

Page 5, beginning line 6, strike "electric utility services" and insert "utility services or an entity performing utility services".

Page 5, line 15, insert "(including all conjugations thereof)" before "means".

Page 5, line 16, insert "(including all conjugations of each of such terms)" before the first period.

Page 6, beginning line 2, strike "striking the period at the end and inserting '; and'" and insert "inserting 'and' after the semicolon at the end".

Page 6, line 6, strike the first period and insert a semicolon.

Page 7, line 20, insert a colon after "paragraphs".

Page 8, line 23, strike "(d)" and insert "(d)(1)".

Page 11, line 6, insert "the first place it appears" before the semicolon.

Page 14, line 25, insert ", at the sole and unreviewable discretion of the Secretary, acting through the Under Secretary for Cybersecurity and Infrastructure Protection," after "subsection".

Page 15, line 8, insert ", at the sole and unreviewable discretion of the Secretary, acting through the Under Secretary for Cybersecurity and Infrastructure Protection," after "section".

Page 15, line 21, insert "at the sole and unreviewable discretion of the Secretary, acting through the Under Secretary for Cybersecurity and Infrastructure Protection," after "Center,".

Page 17, line 20, insert "or exclude" after "remove".

Page 17, line 23, strike "risks" and insert "risk".

Page 23, line 23, insert ", or" before "that".

Page 29, line 25, strike "paragraphs" and insert "subparagraphs".

Page 30, line 15, insert "or exclude" after "remove".

Page 32, line 4, insert "or exclude" after "remove".

Page 33, line 2, insert ", except for purposes authorized in this section" before the period at the end.

Page 34, line 16, insert "or exclude" after "remove".

Page 36, line 18, insert "in good faith" before "fails".

Page 39, beginning line 19, strike "of the violation of any restriction specified in paragraph (3), (6), or 7(B), or any other provision of this section, that is the basis for such action" and insert "on which the cause of action arises".

Page 41, strike lines 5 through 11.

Page 44, line 19, strike "(I)" and insert "(J)".

Page 44, beginning line 19, insert the following:

> "(I) PROHIBITED CONDUCT.—Nothing in this section may be construed to permit price-fixing, allocating a market between competitors, monopolizing or attempting to monopolize a market, or exchanges of price or cost information, customer lists, or information regarding future competitive planning.".

Page 46, line 7, insert "and" before "information".

Page 48, lines 9 through 10, move the proposed subparagraph (H) two ems to the left.

Page 48, lines 13 through 16, move the proposed subparagraphs (K) and (L) two ems to the left.

---

2. AN AMENDMENT TO BE OFFERED BY REPRESENTATIVE KATKO OF NEW YORK OR HIS DESIGNEE, DEBATABLE FOR 10 MINUTES

Page 1, line 12, insert the following (and redesignate subsequent subparagraphs accordingly):

(A) by amending paragraph (2) to read as follows:

"(2) the term 'incident' means an occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system, or actually or imminently jeopardizes, without lawful authority, an information system;".

---

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

In section 2(a)(1), redesignate subparagraphs (A) and (B) as subparagraphs (B) and (C), respectively.

In section 2(a)(1), insert before subparagraph (B), as so redesignated, the following:

(A) by amending paragraph (1) to read as follows:

"(1)(A) except as provided in subparagraph (B), the term 'cybersecurity risk' means threats to and vulnerabilities of information or information systems and any related consequences caused by or resulting from unauthorized access, use, disclosure, degradation, disruption, modification, or destruction of such information or information systems, including such related consequences caused by an act of terrorism;

"(B) such term does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement;".

---

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

Page 10, line 11, strike "and" at the end.
Page 10, line 16, insert "and" after the semicolon.
Page 10, beginning line 17, insert the following:

"(vi) remains current on industrial control system innovation; industry adoption of new technologies, and industry best practices;".

---

5. AN AMENDMENT TO BE OFFERED BY REPRESENTATIVE CASTRO OF TEXAS OR HIS DESIGNEE, DEBATABLE FOR 10 MINUTES

Page 11, line 22, insert before the semicolon at the end the following: ", and, to the extent practicable, make self-assessment tools available to such businesses to determine their levels of prevention of cybersecurity risks".

---

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

Page 52, beginning line 12, insert the following:

"SEC. 232. NATIONAL CYBERSECURITY PREPAREDNESS CONSORTIUM.

"(a) IN GENERAL.—The Secretary may establish a consortium to be known as the 'National Cybersecurity Preparedness Consortium' (in this section referred to as the 'Consortium').

"(b) FUNCTIONS.—The Consortium may—

"(1) provide training to State and local first responders and officials specifically for preparing and responding to cyber attacks;

"(2) develop and update a curriculum utilizing the National Protection and Programs Directorate of the Department sponsored Community Cyber Security Maturity Model (CCSMM) for State and local first responders and officials;

"(3) provide technical assistance services to build and sustain capabilities in support of cybersecurity preparedness and response;

"(4) conduct cybersecurity training and simulation exercises to defend from and respond to cyber-attacks;

"(5) coordinate with the National Cybersecurity and Communications Integration Center to help States and communities develop cybersecurity information sharing programs; and

"(6) coordinate with the National Domestic Preparedness Consortium to incorporate cybersecurity emergency responses into existing State and local emergency management functions.

"(c) MEMBERS.—The Consortium shall consist of academic, nonprofit, and government partners that develop, update, and deliver cybersecurity training in support of homeland security. Members shall have prior experience conducting cybersecurity training and exercises for State and local entities.".

Page 52, before line 17, insert the following:

"Sec. 232. National Cybersecurity Preparedness Consortium.".

---

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

Add at the end the following:

SEC. ___. PROTECTION OF FEDERAL INFORMATION SYSTEMS.

(a) IN GENERAL.—Subtitle C of title II of the Homeland Security Act of 2002 (6 U.S.C. 141 et seq.) is amended by adding at the end the following new section:

"SEC. 233. AVAILABLE PROTECTION OF FEDERAL INFORMATION SYSTEMS.

"(a) IN GENERAL.—The Secretary shall deploy and operate, to make available for use by any Federal agency, with or without reimbursement, capabilities to protect Federal agency information and information systems, including technologies to continuously diagnose, detect, prevent, and mitigate against cybersecurity risks (as such term is defined in the second section 226) involving Federal agency information or information systems.

"(b) ACTIVITIES.—In carrying out this section, the Secretary may—

"(1) access, and Federal agency heads may disclose to the Secretary or a private entity providing assistance to the Secretary under paragraph (2), information traveling to or from or stored on a Federal agency information system, regardless of from where the Secretary or a private entity providing assistance to the Secretary under paragraph (2) accesses such information, notwithstanding any other provision of law that would otherwise restrict or prevent Federal agency heads from disclosing such information to the Secretary or a private entity providing assistance to the Secretary under paragraph (2);

"(2) enter into contracts or other agreements, or otherwise request and obtain the assistance of, private entities to deploy and operate technologies in accordance with subsection (a); and

"(3) retain, use, and disclose information obtained through the conduct of activities authorized under this section only to protect Federal agency information and information systems from cybersecurity risks, or, with the approval of the Attorney General and if disclosure of such information is not otherwise prohibited by law, to law enforcement only to investigate, prosecute, disrupt, or otherwise respond to—

"(A) a violation of section 1030 of title 18, United States Code;

"(B) an imminent threat of death or serious bodily harm;

"(C) a serious threat to a minor, including sexual exploitation or threats to physical safety; or

"(D) an attempt, or conspiracy, to commit an offense described in any of subparagraphs (A) through (C).

"(c) CONDITIONS.—Contracts or other agreements under subsection (b)(2) shall include appropriate provisions barring—

"(1) the disclosure of information to any entity other than the Department or the Federal agency disclosing information in accordance with subsection (b)(1) that can be used to identify specific persons and is reasonably believed to be unrelated to a cybersecurity risk; and

"(2) the use of any information to which such private entity gains access in accordance with this section for any purpose other than to protect Federal agency information and information systems against cybersecurity risks or to administer any such contract or other agreement.

"(d) LIMITATION.—No cause of action shall lie against a private entity for assistance provided to the Secretary in accordance with this section and a contract or agreement under subsection (b)(2).".

(b) CLERICAL AMENDMENT.—The table of contents of the Homeland Security Act of 2002 is amended by inserting after the item relating to section 226 (relating to cybersecurity recruitment and retention) the following new item:

"Sec. 233. Available protection of Federal information systems.".

---

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

Add at the end the following new section:

SEC. ___. SUNSET.

This Act and the amendments made by this Act shall terminate on the date that is seven years after the date of the enactment of this Act.

---

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

Add the end the following:

SEC. ___. REPORT ON CYBERSECURITY VULNERABILITIES OF UNITED STATES PORTS.

Not later than 180 days after the date of the enactment of this Act, the Secretary of Homeland Security shall submit to the Committee on Homeland Security and the Committee on Transportation and Infrastructure of the House of Representatives and the Committee on Homeland Security and Governmental Affairs and the Committee on Commerce, Science and Transportation of the Senate a report on cybersecurity vulnerabilities for the ten United States ports that the Secretary determines are at greatest risk of a cybersecurity incident and provide recommendations to mitigate such vulnerabilities.

---

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

Add at the end the following:

SEC. ___. GAO REPORT ON IMPACT PRIVACY AND CIVIL LIBERTIES.

Not later than 60 months after the date of the enactment of this Act, the Comptroller General of the United States shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate an assessment on the impact on privacy and civil liberties limited to the work of the National Cybersecurity and Communications Integration Center.

---

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

Add at the end the following:

SEC. ___. REPORT ON CYBERSECURITY AND CRITICAL INFRASTRUCTURE.

The Secretary of Homeland Security may consult with sector specific agencies, businesses, and stakeholders to produce and submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report on how best to align federally-funded cybersecurity research and development activities with private sector efforts to protect privacy and civil liberties while assuring security and resilience of the Nation's critical infrastructure, including—

(1) promoting research and development to enable the secure and resilient design and construction of critical infrastructure and more secure accompanying cyber technology;

(2) enhancing modeling capabilities to determine potential impacts on critical infrastructure of incidents or threat scenarios, and cascading effects on other sectors; and

(3) facilitating initiatives to incentivize cybersecurity investments and the adoption of critical infrastructure design features that strengthen cybersesecurity and resilience.

○