

113TH CONGRESS
1ST SESSION

H. R. 624

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.

IN THE HOUSE OF REPRESENTATIVES

FEBRUARY 13, 2013

Mr. ROGERS of Michigan (for himself and Mr. RUPPERSBERGER) introduced the following bill; which was referred to the Select Committee on Intelligence (Permanent Select)

A BILL

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.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Cyber Intelligence
5 Sharing and Protection Act”.

1 **SEC. 2. CYBER THREAT INTELLIGENCE AND INFORMATION**
2 **SHARING.**

3 (a) IN GENERAL.—Title XI of the National Security
4 Act of 1947 (50 U.S.C. 442 et seq.) is amended by adding
5 at the end the following new section:

6 “CYBER THREAT INTELLIGENCE AND INFORMATION
7 SHARING

8 “SEC. 1104. (a) INTELLIGENCE COMMUNITY SHAR-
9 ING OF CYBER THREAT INTELLIGENCE WITH PRIVATE
10 SECTOR AND UTILITIES.—

11 “(1) IN GENERAL.—The Director of National
12 Intelligence shall establish procedures to allow ele-
13 ments of the intelligence community to share cyber
14 threat intelligence with private-sector entities and
15 utilities and to encourage the sharing of such intel-
16 ligence.

17 “(2) SHARING AND USE OF CLASSIFIED INTEL-
18 LIGENCE.—The procedures established under para-
19 graph (1) shall provide that classified cyber threat
20 intelligence may only be—

21 “(A) shared by an element of the intel-
22 ligence community with—

23 “(i) a certified entity; or

24 “(ii) a person with an appropriate se-
25 curity clearance to receive such cyber
26 threat intelligence;

1 “(B) shared consistent with the need to
2 protect the national security of the United
3 States; and

4 “(C) used by a certified entity in a manner
5 which protects such cyber threat intelligence
6 from unauthorized disclosure.

7 “(3) SECURITY CLEARANCE APPROVALS.—The
8 Director of National Intelligence shall issue guide-
9 lines providing that the head of an element of the
10 intelligence community may, as the head of such ele-
11 ment considers necessary to carry out this sub-
12 section—

13 “(A) grant a security clearance on a tem-
14 porary or permanent basis to an employee or
15 officer of a certified entity;

16 “(B) grant a security clearance on a tem-
17 porary or permanent basis to a certified entity
18 and approval to use appropriate facilities; and

19 “(C) expedite the security clearance proc-
20 ess for a person or entity as the head of such
21 element considers necessary, consistent with the
22 need to protect the national security of the
23 United States.

24 “(4) NO RIGHT OR BENEFIT.—The provision of
25 information to a private-sector entity or a utility

1 under this subsection shall not create a right or ben-
2 efit to similar information by such entity or such
3 utility or any other private-sector entity or utility.

4 “(5) RESTRICTION ON DISCLOSURE OF CYBER
5 THREAT INTELLIGENCE.—Notwithstanding any
6 other provision of law, a certified entity receiving
7 cyber threat intelligence pursuant to this subsection
8 shall not further disclose such cyber threat intel-
9 ligence to another entity, other than to a certified
10 entity or other appropriate agency or department of
11 the Federal Government authorized to receive such
12 cyber threat intelligence.

13 “(b) USE OF CYBERSECURITY SYSTEMS AND SHAR-
14 ING OF CYBER THREAT INFORMATION.—

15 “(1) IN GENERAL.—

16 “(A) CYBERSECURITY PROVIDERS.—Not-
17 withstanding any other provision of law, a cy-
18 bersecurity provider, with the express consent
19 of a protected entity for which such cybersecu-
20 rity provider is providing goods or services for
21 cybersecurity purposes, may, for cybersecurity
22 purposes—

23 “(i) use cybersecurity systems to iden-
24 tify and obtain cyber threat information to

1 protect the rights and property of such
2 protected entity; and

3 “(ii) share such cyber threat informa-
4 tion with any other entity designated by
5 such protected entity, including, if specifi-
6 cally designated, the Federal Government.

7 “(B) SELF-PROTECTED ENTITIES.—Not-
8 withstanding any other provision of law, a self-
9 protected entity may, for cybersecurity pur-
10 poses—

11 “(i) use cybersecurity systems to iden-
12 tify and obtain cyber threat information to
13 protect the rights and property of such
14 self-protected entity; and

15 “(ii) share such cyber threat informa-
16 tion with any other entity, including the
17 Federal Government.

18 “(2) SHARING WITH THE FEDERAL GOVERN-
19 MENT.—

20 “(A) INFORMATION SHARED WITH THE
21 NATIONAL CYBERSECURITY AND COMMUNICA-
22 TIONS INTEGRATION CENTER OF THE DEPART-
23 MENT OF HOMELAND SECURITY.—Subject to
24 the use and protection of information require-
25 ments under paragraph (3), the head of a de-

1 partment or agency of the Federal Government
2 receiving cyber threat information in accordance
3 with paragraph (1) shall provide such cyber
4 threat information to the National Cybersecu-
5 rity and Communications Integration Center of
6 the Department of Homeland Security.

7 “(B) REQUEST TO SHARE WITH ANOTHER
8 DEPARTMENT OR AGENCY OF THE FEDERAL
9 GOVERNMENT.—An entity sharing cyber threat
10 information that is provided to the National Cy-
11 bersecurity and Communications Integration
12 Center of the Department of Homeland Secu-
13 rity under subparagraph (A) or paragraph (1)
14 may request the head of such Center to, and
15 the head of such Center may, provide such in-
16 formation to another department or agency of
17 the Federal Government.

18 “(3) USE AND PROTECTION OF INFORMA-
19 TION.—Cyber threat information shared in accord-
20 ance with paragraph (1)—

21 “(A) shall only be shared in accordance
22 with any restrictions placed on the sharing of
23 such information by the protected entity or self-
24 protected entity authorizing such sharing, in-

1 including appropriate anonymization or minimiza-
2 tion of such information;

3 “(B) may not be used by an entity to gain
4 an unfair competitive advantage to the det-
5 riment of the protected entity or the self-pro-
6 tected entity authorizing the sharing of infor-
7 mation;

8 “(C) if shared with the Federal Govern-
9 ment—

10 “(i) shall be exempt from disclosure
11 under section 552 of title 5, United States
12 Code (commonly known as the ‘Freedom of
13 Information Act’);

14 “(ii) shall be considered proprietary
15 information and shall not be disclosed to
16 an entity outside of the Federal Govern-
17 ment except as authorized by the entity
18 sharing such information;

19 “(iii) shall not be used by the Federal
20 Government for regulatory purposes;

21 “(iv) shall not be provided by the de-
22 partment or agency of the Federal Govern-
23 ment receiving such cyber threat informa-
24 tion to another department or agency of

1 the Federal Government under paragraph
2 (2)(A) if—

3 “(I) the entity providing such in-
4 formation determines that the provi-
5 sion of such information will under-
6 mine the purpose for which such in-
7 formation is shared; or

8 “(II) unless otherwise directed by
9 the President, the head of the depart-
10 ment or agency of the Federal Gov-
11 ernment receiving such cyber threat
12 information determines that the provi-
13 sion of such information will under-
14 mine the purpose for which such in-
15 formation is shared; and

16 “(v) shall be handled by the Federal
17 Government consistent with the need to
18 protect sources and methods and the na-
19 tional security of the United States; and

20 “(D) shall be exempt from disclosure
21 under a State, local, or tribal law or regulation
22 that requires public disclosure of information by
23 a public or quasi-public entity.

24 “(4) EXEMPTION FROM LIABILITY.—No civil or
25 criminal cause of action shall lie or be maintained in

1 Federal or State court against a protected entity,
2 self-protected entity, cybersecurity provider, or an
3 officer, employee, or agent of a protected entity, self-
4 protected entity, or cybersecurity provider, acting in
5 good faith—

6 “(A) for using cybersecurity systems to
7 identify or obtain cyber threat information or
8 for sharing such information in accordance with
9 this section; or

10 “(B) for decisions made based on cyber
11 threat information identified, obtained, or
12 shared under this section.

13 “(5) RELATIONSHIP TO OTHER LAWS REQUIR-
14 ING THE DISCLOSURE OF INFORMATION.—The sub-
15 mission of information under this subsection to the
16 Federal Government shall not satisfy or affect—

17 “(A) any requirement under any other pro-
18 vision of law for a person or entity to provide
19 information to the Federal Government; or

20 “(B) the applicability of other provisions of
21 law, including section 552 of title 5, United
22 States Code (commonly known as the ‘Freedom
23 of Information Act’), with respect to informa-
24 tion required to be provided to the Federal Gov-
25 ernment under such other provision of law.

1 “(c) FEDERAL GOVERNMENT USE OF INFORMA-
2 TION.—

3 “(1) LIMITATION.—The Federal Government
4 may use cyber threat information shared with the
5 Federal Government in accordance with subsection
6 (b)—

7 “(A) for cybersecurity purposes;

8 “(B) for the investigation and prosecution
9 of cybersecurity crimes;

10 “(C) for the protection of individuals from
11 the danger of death or serious bodily harm and
12 the investigation and prosecution of crimes in-
13 volving such danger of death or serious bodily
14 harm;

15 “(D) for the protection of minors from
16 child pornography, any risk of sexual exploi-
17 tation, and serious threats to the physical safe-
18 ty of minors, including kidnapping and traf-
19 ficking and the investigation and prosecution of
20 crimes involving child pornography, any risk of
21 sexual exploitation, and serious threats to the
22 physical safety of minors, including kidnapping
23 and trafficking, and any crime referred to in
24 section 2258A(a)(2) of title 18, United States
25 Code; or

1 “(E) to protect the national security of the
2 United States.

3 “(2) AFFIRMATIVE SEARCH RESTRICTION.—
4 The Federal Government may not affirmatively
5 search cyber threat information shared with the
6 Federal Government under subsection (b) for a pur-
7 pose other than a purpose referred to in paragraph
8 (1)(B).

9 “(3) ANTI-TASKING RESTRICTION.—Nothing in
10 this section shall be construed to permit the Federal
11 Government to—

12 “(A) require a private-sector entity to
13 share information with the Federal Govern-
14 ment; or

15 “(B) condition the sharing of cyber threat
16 intelligence with a private-sector entity on the
17 provision of cyber threat information to the
18 Federal Government.

19 “(4) PROTECTION OF SENSITIVE PERSONAL
20 DOCUMENTS.—The Federal Government may not
21 use the following information, containing informa-
22 tion that identifies a person, shared with the Federal
23 Government in accordance with subsection (b):

24 “(A) Library circulation records.

25 “(B) Library patron lists.

1 “(C) Book sales records.

2 “(D) Book customer lists.

3 “(E) Firearms sales records.

4 “(F) Tax return records.

5 “(G) Educational records.

6 “(H) Medical records.

7 “(5) NOTIFICATION OF NON-CYBER THREAT IN-
8 FORMATION.—If a department or agency of the Fed-
9 eral Government receiving information pursuant to
10 subsection (b)(1) determines that such information
11 is not cyber threat information, such department or
12 agency shall notify the entity or provider sharing
13 such information pursuant to subsection (b)(1).

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

19 “(7) PROTECTION OF INDIVIDUAL INFORMA-
20 TION.—The Federal Government may, consistent
21 with the need to protect Federal systems and critical
22 information infrastructure from cybersecurity
23 threats and to mitigate such threats, undertake rea-
24 sonable efforts to limit the impact on privacy and
25 civil liberties of the sharing of cyber threat informa-

1 tion with the Federal Government pursuant to this
2 subsection.

3 “(d) FEDERAL GOVERNMENT LIABILITY FOR VIOLA-
4 TIONS OF RESTRICTIONS ON THE DISCLOSURE, USE, AND
5 PROTECTION OF VOLUNTARILY SHARED INFORMATION.—

6 “(1) IN GENERAL.—If a department or agency
7 of the Federal Government intentionally or willfully
8 violates subsection (b)(3)(C) or subsection (c) with
9 respect to the disclosure, use, or protection of volun-
10 tarily shared cyber threat information shared under
11 this section, the United States shall be liable to a
12 person adversely affected by such violation in an
13 amount equal to the sum of—

14 “(A) the actual damages sustained by the
15 person as a result of the violation or \$1,000,
16 whichever is greater; and

17 “(B) the costs of the action together with
18 reasonable attorney fees as determined by the
19 court.

20 “(2) VENUE.—An action to enforce liability cre-
21 ated under this subsection may be brought in the
22 district court of the United States in—

23 “(A) the district in which the complainant
24 resides;

1 “(B) the district in which the principal
2 place of business of the complainant is located;

3 “(C) the district in which the department
4 or agency of the Federal Government that dis-
5 closed the information is located; or

6 “(D) the District of Columbia.

7 “(3) STATUTE OF LIMITATIONS.—No action
8 shall lie under this subsection unless such action is
9 commenced not later than two years after the date
10 of the violation of subsection (b)(3)(C) or subsection
11 (c) that is the basis for the action.

12 “(4) EXCLUSIVE CAUSE OF ACTION.—A cause
13 of action under this subsection shall be the exclusive
14 means available to a complainant seeking a remedy
15 for a violation of subsection (b)(3)(C) or subsection
16 (c).

17 “(e) REPORT ON INFORMATION SHARING.—

18 “(1) REPORT.—The Inspector General of the
19 Intelligence Community shall annually submit to the
20 congressional intelligence committees a report con-
21 taining a review of the use of information shared
22 with the Federal Government under this section, in-
23 cluding—

1 “(A) a review of the use by the Federal
2 Government of such information for a purpose
3 other than a cybersecurity purpose;

4 “(B) a review of the type of information
5 shared with the Federal Government under this
6 section;

7 “(C) a review of the actions taken by the
8 Federal Government based on such information;

9 “(D) appropriate metrics to determine the
10 impact of the sharing of such information with
11 the Federal Government on privacy and civil
12 liberties, if any;

13 “(E) a list of the departments or agencies
14 receiving such information;

15 “(F) a review of the sharing of such infor-
16 mation within the Federal Government to iden-
17 tify inappropriate stovepiping of shared infor-
18 mation; and

19 “(G) any recommendations of the Inspec-
20 tor General for improvements or modifications
21 to the authorities under this section.

22 “(2) FORM.—Each report required under para-
23 graph (1) shall be submitted in unclassified form,
24 but may include a classified annex.

1 “(f) FEDERAL PREEMPTION.—This section super-
2 sedes any statute of a State or political subdivision of a
3 State that restricts or otherwise expressly regulates an ac-
4 tivity authorized under subsection (b).

5 “(g) SAVINGS CLAUSES.—

6 “(1) EXISTING AUTHORITIES.—Nothing in this
7 section shall be construed to limit any other author-
8 ity to use a cybersecurity system or to identify, ob-
9 tain, or share cyber threat intelligence or cyber
10 threat information.

11 “(2) LIMITATION ON MILITARY AND INTEL-
12 LIGENCE COMMUNITY INVOLVEMENT IN PRIVATE
13 AND PUBLIC SECTOR CYBERSECURITY EFFORTS.—
14 Nothing in this section shall be construed to provide
15 additional authority to, or modify an existing au-
16 thority of, the Department of Defense or the Na-
17 tional Security Agency or any other element of the
18 intelligence community to control, modify, require,
19 or otherwise direct the cybersecurity efforts of a pri-
20 vate-sector entity or a component of the Federal
21 Government or a State, local, or tribal government.

22 “(3) INFORMATION SHARING RELATIONSHIPS.—
23 Nothing in this section shall be construed to—

24 “(A) limit or modify an existing informa-
25 tion sharing relationship;

1 “(B) prohibit a new information sharing
2 relationship;

3 “(C) require a new information sharing re-
4 lationship between the Federal Government and
5 a private-sector entity; or

6 “(D) modify the authority of a department
7 or agency of the Federal Government to protect
8 sources and methods and the national security
9 of the United States.

10 “(4) LIMITATION ON FEDERAL GOVERNMENT
11 USE OF CYBERSECURITY SYSTEMS.—Nothing in this
12 section shall be construed to provide additional au-
13 thority to, or modify an existing authority of, any
14 entity to use a cybersecurity system owned or con-
15 trolled by the Federal Government on a private-sec-
16 tor system or network to protect such private-sector
17 system or network.

18 “(5) NO LIABILITY FOR NON-PARTICIPATION.—
19 Nothing in this section shall be construed to subject
20 a protected entity, self-protected entity, cyber secu-
21 rity provider, or an officer, employee, or agent of a
22 protected entity, self-protected entity, or cybersecu-
23 rity provider, to liability for choosing not to engage
24 in the voluntary activities authorized under this sec-
25 tion.

1 “(6) USE AND RETENTION OF INFORMATION.—
2 Nothing in this section shall be construed to author-
3 ize, or to modify any existing authority of, a depart-
4 ment or agency of the Federal Government to retain
5 or use information shared pursuant to subsection
6 (b)(1) for any use other than a use permitted under
7 subsection (c)(1).

8 “(h) DEFINITIONS.—In this section:

9 “(1) AVAILABILITY.—The term ‘availability’
10 means ensuring timely and reliable access to and use
11 of information.

12 “(2) CERTIFIED ENTITY.—The term ‘certified
13 entity’ means a protected entity, self-protected enti-
14 ty, or cybersecurity provider that—

15 “(A) possesses or is eligible to obtain a se-
16 curity clearance, as determined by the Director
17 of National Intelligence; and

18 “(B) is able to demonstrate to the Director
19 of National Intelligence that such provider or
20 such entity can appropriately protect classified
21 cyber threat intelligence.

22 “(3) CONFIDENTIALITY.—The term ‘confiden-
23 tiality’ means preserving authorized restrictions on
24 access and disclosure, including means for protecting
25 personal privacy and proprietary information.

1 “(4) CYBER THREAT INFORMATION.—

2 “(A) IN GENERAL.—The term ‘cyber
3 threat information’ means information directly
4 pertaining to—

5 “(i) a vulnerability of a system or net-
6 work of a government or private entity;

7 “(ii) a threat to the integrity, con-
8 fidentiality, or availability of a system or
9 network of a government or private entity
10 or any information stored on, processed on,
11 or transiting such a system or network;

12 “(iii) efforts to deny access to or de-
13 grade, disrupt, or destroy a system or net-
14 work of a government or private entity; or

15 “(iv) efforts to gain unauthorized ac-
16 cess to a system or network of a govern-
17 ment or private entity, including to gain
18 such unauthorized access for the purpose
19 of exfiltrating information stored on, proc-
20 essed on, or transiting a system or network
21 of a government or private entity.

22 “(B) EXCLUSION.— Such term does not
23 include information pertaining to efforts to gain
24 unauthorized access to a system or network of
25 a government or private entity that solely in-

1 involve violations of consumer terms of service or
2 consumer licensing agreements and do not oth-
3 erwise constitute unauthorized access.

4 “(5) CYBER THREAT INTELLIGENCE.—

5 “(A) IN GENERAL.—The term ‘cyber
6 threat intelligence’ means intelligence in the
7 possession of an element of the intelligence
8 community directly pertaining to—

9 “(i) a vulnerability of a system or net-
10 work of a government or private entity;

11 “(ii) a threat to the integrity, con-
12 fidentiality, or availability of a system or
13 network of a government or private entity
14 or any information stored on, processed on,
15 or transiting such a system or network;

16 “(iii) efforts to deny access to or de-
17 grade, disrupt, or destroy a system or net-
18 work of a government or private entity; or

19 “(iv) efforts to gain unauthorized ac-
20 cess to a system or network of a govern-
21 ment or private entity, including to gain
22 such unauthorized access for the purpose
23 of exfiltrating information stored on, proc-
24 essed on, or transiting a system or network
25 of a government or private entity.

1 “(B) EXCLUSION.— Such term does not
2 include intelligence pertaining to efforts to gain
3 unauthorized access to a system or network of
4 a government or private entity that solely in-
5 volve violations of consumer terms of service or
6 consumer licensing agreements and do not oth-
7 erwise constitute unauthorized access.

8 “(6) CYBERSECURITY CRIME.—The term ‘cy-
9 bersecurity crime’ means—

10 “(A) a crime under a Federal or State law
11 that involves—

12 “(i) efforts to deny access to or de-
13 grade, disrupt, or destroy a system or net-
14 work;

15 “(ii) efforts to gain unauthorized ac-
16 cess to a system or network; or

17 “(iii) efforts to exfiltrate information
18 from a system or network without author-
19 ization; or

20 “(B) the violation of a provision of Federal
21 law relating to computer crimes, including a
22 violation of any provision of title 18, United
23 States Code, created or amended by the Com-
24 puter Fraud and Abuse Act of 1986 (Public
25 Law 99–474).

1 “(7) CYBERSECURITY PROVIDER.—The term
2 ‘cybersecurity provider’ means a non-governmental
3 entity that provides goods or services intended to be
4 used for cybersecurity purposes.

5 “(8) CYBERSECURITY PURPOSE.—

6 “(A) IN GENERAL.—The term ‘cybersecu-
7 rity purpose’ means the purpose of ensuring the
8 integrity, confidentiality, or availability of, or
9 safeguarding, a system or network, including
10 protecting a system or network from—

11 “(i) a vulnerability of a system or net-
12 work;

13 “(ii) a threat to the integrity, con-
14 fidentiality, or availability of a system or
15 network or any information stored on,
16 processed on, or transiting such a system
17 or network;

18 “(iii) efforts to deny access to or de-
19 grade, disrupt, or destroy a system or net-
20 work; or

21 “(iv) efforts to gain unauthorized ac-
22 cess to a system or network, including to
23 gain such unauthorized access for the pur-
24 pose of exfiltrating information stored on,

1 processed on, or transiting a system or
2 network.

3 “(B) EXCLUSION.— Such term does not
4 include the purpose of protecting a system or
5 network from efforts to gain unauthorized ac-
6 cess to such system or network that solely in-
7 volve violations of consumer terms of service or
8 consumer licensing agreements and do not oth-
9 erwise constitute unauthorized access.

10 “(9) CYBERSECURITY SYSTEM.—

11 “(A) IN GENERAL.—The term ‘cybersecu-
12 rity system’ means a system designed or em-
13 ployed to ensure the integrity, confidentiality,
14 or availability of, or safeguard, a system or net-
15 work, including protecting a system or network
16 from—

17 “(i) a vulnerability of a system or net-
18 work;

19 “(ii) a threat to the integrity, con-
20 fidentiality, or availability of a system or
21 network or any information stored on,
22 processed on, or transiting such a system
23 or network;

1 “(iii) efforts to deny access to or de-
2 grade, disrupt, or destroy a system or net-
3 work; or

4 “(iv) efforts to gain unauthorized ac-
5 cess to a system or network, including to
6 gain such unauthorized access for the pur-
7 pose of exfiltrating information stored on,
8 processed on, or transiting a system or
9 network.

10 “(B) EXCLUSION.— Such term does not
11 include a system designed or employed to pro-
12 tect a system or network from efforts to gain
13 unauthorized access to such system or network
14 that solely involve violations of consumer terms
15 of service or consumer licensing agreements and
16 do not otherwise constitute unauthorized access.

17 “(10) INTEGRITY.—The term ‘integrity’ means
18 guarding against improper information modification
19 or destruction, including ensuring information non-
20 repudiation and authenticity.

21 “(11) PROTECTED ENTITY.—The term ‘pro-
22 tected entity’ means an entity, other than an indi-
23 vidual, that contracts with a cybersecurity provider
24 for goods or services to be used for cybersecurity
25 purposes.

1 “(12) SELF-PROTECTED ENTITY.—The term
2 ‘self-protected entity’ means an entity, other than an
3 individual, that provides goods or services for cyber-
4 security purposes to itself.

5 “(13) UTILITY.—The term ‘utility’ means an
6 entity providing essential services (other than law
7 enforcement or regulatory services), including elec-
8 tricity, natural gas, propane, telecommunications,
9 transportation, water, or wastewater services.”.

10 (b) PROCEDURES AND GUIDELINES.—The Director
11 of National Intelligence shall—

12 (1) not later than 60 days after the date of the
13 enactment of this Act, establish procedures under
14 paragraph (1) of section 1104(a) of the National Se-
15 curity Act of 1947, as added by subsection (a) of
16 this section, and issue guidelines under paragraph
17 (3) of such section 1104(a);

18 (2) in establishing such procedures and issuing
19 such guidelines, consult with the Secretary of Home-
20 land Security to ensure that such procedures and
21 such guidelines permit the owners and operators of
22 critical infrastructure to receive all appropriate cyber
23 threat intelligence (as defined in section 1104(h)(3)
24 of such Act, as added by subsection (a)) in the pos-
25 session of the Federal Government; and

1 (3) following the establishment of such proce-
2 dures and the issuance of such guidelines, expedi-
3 tiously distribute such procedures and such guide-
4 lines to appropriate departments and agencies of the
5 Federal Government, private-sector entities, and
6 utilities (as defined in section 1104(h)(9) of such
7 Act, as added by subsection (a)).

8 (c) INITIAL REPORT.—The first report required to be
9 submitted under subsection (e) of section 1104 of the Na-
10 tional Security Act of 1947, as added by subsection (a)
11 of this section, shall be submitted not later than 1 year
12 after the date of the enactment of this Act.

13 (d) TABLE OF CONTENTS AMENDMENT.—The table
14 of contents in the first section of the National Security
15 Act of 1947 is amended by adding at the end the following
16 new item:

“Sec. 1104. Cyber threat intelligence and information sharing.”.

17 **SEC. 3. SUNSET.**

18 Effective on the date that is 5 years after the date
19 of the enactment of this Act—

20 (1) section 1104 of the National Security Act of
21 1947, as added by section 2(a) of this Act, is re-
22 pealed; and

23 (2) the table of contents in the first section of
24 the National Security Act of 1947, as amended by
25 section 2(d) of this Act, is amended by striking the

- 1 item relating to section 1104, as added by such sec-
- 2 tion 2(d).

○