

114TH CONGRESS
1ST SESSION

H. R. 234

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

JANUARY 8, 2015

Mr. RUPPERSBERGER introduced the following bill; which was referred to the Select Committee on Intelligence (Permanent Select), and in addition to the Committees on the Judiciary, Armed Services, and Homeland Security, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

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. FEDERAL GOVERNMENT COORDINATION WITH RE-**
2 **SPECT TO CYBERSECURITY.**

3 (a) COORDINATED ACTIVITIES.—The Federal Gov-
4 ernment shall conduct cybersecurity activities to provide
5 shared situational awareness that enables integrated oper-
6 ational actions to protect, prevent, mitigate, respond to,
7 and recover from cyber incidents.

8 (b) COORDINATED INFORMATION SHARING.—

9 (1) DESIGNATION OF COORDINATING ENTITY
10 FOR CYBER THREAT INFORMATION.—The President
11 shall designate an entity within the Department of
12 Homeland Security as the civilian Federal entity to
13 receive cyber threat information that is shared by a
14 cybersecurity provider or self-protected entity in ac-
15 cordance with section 1104(b) of the National Secu-
16 rity Act of 1947, as added by section 3(a) of this
17 Act, except as provided in paragraph (2) and subject
18 to the procedures established under paragraph (4).

19 (2) DESIGNATION OF A COORDINATING ENTITY
20 FOR CYBERSECURITY CRIMES.—The President shall
21 designate an entity within the Department of Justice
22 as the civilian Federal entity to receive cyber threat
23 information related to cybersecurity crimes that is
24 shared by a cybersecurity provider or self-protected
25 entity in accordance with section 1104(b) of the Na-
26 tional Security Act of 1947, as added by section 3(a)

1 of this Act, subject to the procedures under para-
2 graph (4).

3 (3) SHARING BY COORDINATING ENTITIES.—

4 The entities designated under paragraphs (1) and
5 (2) shall share cyber threat information shared with
6 such entities in accordance with section 1104(b) of
7 the National Security Act of 1947, as added by sec-
8 tion 3(a) of this Act, consistent with the procedures
9 established under paragraphs (4) and (5).

10 (4) PROCEDURES.—Each department or agency
11 of the Federal Government receiving cyber threat in-
12 formation shared in accordance with section 1104(b)
13 of the National Security Act of 1947, as added by
14 section 3(a) of this Act, shall establish procedures
15 to—

16 (A) ensure that cyber threat information
17 shared with departments or agencies of the
18 Federal Government in accordance with such
19 section 1104(b) is also shared with appropriate
20 departments and agencies of the Federal Gov-
21 ernment with a national security mission in real
22 time;

23 (B) ensure the distribution to other de-
24 partments and agencies of the Federal Govern-

1 ment of cyber threat information in real time;
2 and

3 (C) facilitate information sharing, inter-
4 action, and collaboration among and between
5 the Federal Government; State, local, tribal,
6 and territorial governments; and cybersecurity
7 providers and self-protected entities.

8 (5) PRIVACY AND CIVIL LIBERTIES.—

9 (A) POLICIES AND PROCEDURES.—The
10 Secretary of Homeland Security, the Attorney
11 General, the Director of National Intelligence,
12 and the Secretary of Defense shall jointly estab-
13 lish and periodically review policies and proce-
14 dures governing the receipt, retention, use, and
15 disclosure of non-publicly available cyber threat
16 information shared with the Federal Govern-
17 ment in accordance with section 1104(b) of the
18 National Security Act of 1947, as added by sec-
19 tion 3(a) of this Act. Such policies and proce-
20 dures shall, consistent with the need to protect
21 systems and networks from cyber threats and
22 mitigate cyber threats in a timely manner—

23 (i) minimize the impact on privacy
24 and civil liberties;

1 (ii) reasonably limit the receipt, reten-
2 tion, use, and disclosure of cyber threat in-
3 formation associated with specific persons
4 that is not necessary to protect systems or
5 networks from cyber threats or mitigate
6 cyber threats in a timely manner;

7 (iii) include requirements to safeguard
8 non-publicly available cyber threat infor-
9 mation that may be used to identify spe-
10 cific persons from unauthorized access or
11 acquisition;

12 (iv) protect the confidentiality of cyber
13 threat information associated with specific
14 persons to the greatest extent practicable;
15 and

16 (v) not delay or impede the flow of
17 cyber threat information necessary to de-
18 fend against or mitigate a cyber threat.

19 (B) SUBMISSION TO CONGRESS.—The Sec-
20 retary of Homeland Security, the Attorney Gen-
21 eral, the Director of National Intelligence, and
22 the Secretary of Defense shall, consistent with
23 the need to protect sources and methods, jointly
24 submit to Congress the policies and procedures

1 required under subparagraph (A) and any up-
2 dates to such policies and procedures.

3 (C) IMPLEMENTATION.—The head of each
4 department or agency of the Federal Govern-
5 ment receiving cyber threat information shared
6 with the Federal Government under such sec-
7 tion 1104(b) shall—

8 (i) implement the policies and proce-
9 dures established under subparagraph (A);
10 and

11 (ii) promptly notify the Secretary of
12 Homeland Security, the Attorney General,
13 the Director of National Intelligence, the
14 Secretary of Defense, and the appropriate
15 congressional committees of any significant
16 violations of such policies and procedures.

17 (D) OVERSIGHT.—The Secretary of Home-
18 land Security, the Attorney General, the Direc-
19 tor of National Intelligence, and the Secretary
20 of Defense shall jointly establish a program to
21 monitor and oversee compliance with the poli-
22 cies and procedures established under subpara-
23 graph (A).

24 (6) INFORMATION SHARING RELATIONSHIPS.—
25 Nothing in this section shall be construed to—

1 (A) alter existing agreements or prohibit
2 new agreements with respect to the sharing of
3 cyber threat information between the Depart-
4 ment of Defense and an entity that is part of
5 the defense industrial base;

6 (B) alter existing information-sharing rela-
7 tionships between a cybersecurity provider, pro-
8 tected entity, or self-protected entity and the
9 Federal Government;

10 (C) prohibit the sharing of cyber threat in-
11 formation directly with a department or agency
12 of the Federal Government for criminal inves-
13 tigative purposes related to crimes described in
14 section 1104(c)(1) of the National Security Act
15 of 1947, as added by section 3(a) of this Act;
16 or

17 (D) alter existing agreements or prohibit
18 new agreements with respect to the sharing of
19 cyber threat information between the Depart-
20 ment of Treasury and an entity that is part of
21 the financial services sector.

22 (7) TECHNICAL ASSISTANCE.—

23 (A) DISCUSSIONS AND ASSISTANCE.—
24 Nothing in this section shall be construed to
25 prohibit any department or agency of the Fed-

1 eral Government from engaging in formal or in-
2 formal technical discussion regarding cyber
3 threat information with a cybersecurity provider
4 or self-protected entity or from providing tech-
5 nical assistance to address vulnerabilities or
6 mitigate threats at the request of such a pro-
7 vider or such an entity.

8 (B) COORDINATION.—Any department or
9 agency of the Federal Government engaging in
10 an activity referred to in subparagraph (A)
11 shall coordinate such activity with the entity of
12 the Department of Homeland Security des-
13 ignated under paragraph (1) and share all sig-
14 nificant information resulting from such activity
15 with such entity and all other appropriate de-
16 partments and agencies of the Federal Govern-
17 ment.

18 (C) SHARING BY DESIGNATED ENTITY.—
19 Consistent with the policies and procedures es-
20 tablished under paragraph (5), the entity of the
21 Department of Homeland Security designated
22 under paragraph (1) shall share with all appro-
23 priate departments and agencies of the Federal
24 Government all significant information resulting
25 from—

1 (i) formal or informal technical dis-
2 cussions between such entity of the De-
3 partment of Homeland Security and a cy-
4 bersecurity provider or self-protected entity
5 about cyber threat information; or

6 (ii) any technical assistance such enti-
7 ty of the Department of Homeland Secu-
8 rity provides to such cybersecurity provider
9 or such self-protected entity to address
10 vulnerabilities or mitigate threats.

11 (c) REPORTS ON INFORMATION SHARING.—

12 (1) INSPECTOR GENERAL OF THE DEPARTMENT
13 OF HOMELAND SECURITY REPORT.—The Inspector
14 General of the Department of Homeland Security, in
15 consultation with the Inspector General of the De-
16 partment of Justice, the Inspector General of the In-
17 telligence Community, the Inspector General of the
18 Department of Defense, and the Privacy and Civil
19 Liberties Oversight Board, shall annually submit to
20 the appropriate congressional committees a report
21 containing a review of the use of information shared
22 with the Federal Government under subsection (b)
23 of section 1104 of the National Security Act of
24 1947, as added by section 3(a) of this Act, includ-
25 ing—

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
6 such subsection;

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 Inspector
20 General of the Department of Homeland Secu-
21 rity for improvements or modifications to the
22 authorities under such section.

23 (2) PRIVACY AND CIVIL LIBERTIES OFFICERS
24 REPORT.—The Officer for Civil Rights and Civil
25 Liberties of the Department of Homeland Security,

1 in consultation with the Privacy and Civil Liberties
2 Oversight Board, the Inspector General of the Intel-
3 ligence Community, and the senior privacy and civil
4 liberties officer of each department or agency of the
5 Federal Government that receives cyber threat infor-
6 mation shared with the Federal Government under
7 such subsection (b), shall annually and jointly sub-
8 mit to Congress a report assessing the privacy and
9 civil liberties impact of the activities conducted by
10 the Federal Government under such section 1104.
11 Such report shall include any recommendations the
12 Civil Liberties Protection Officer and Chief Privacy
13 and Civil Liberties Officer consider appropriate to
14 minimize or mitigate the privacy and civil liberties
15 impact of the sharing of cyber threat information
16 under such section 1104.

17 (3) FORM.—Each report required under para-
18 graph (1) or (2) shall be submitted in unclassified
19 form, but may include a classified annex.

20 (d) DEFINITIONS.—In this section:

21 (1) APPROPRIATE CONGRESSIONAL COMMIT-
22 TEES.—The term “appropriate congressional com-
23 mittees” means—

24 (A) the Committee on Homeland Security,
25 the Committee on the Judiciary, the Permanent

1 Select Committee on Intelligence, and the Com-
2 mittee on Armed Services of the House of Rep-
3 resentatives; and

4 (B) the Committee on Homeland Security
5 and Governmental Affairs, the Committee on
6 the Judiciary, the Select Committee on Intel-
7 ligence, and the Committee on Armed Services
8 of the Senate.

9 (2) CYBER THREAT INFORMATION, CYBER
10 THREAT INTELLIGENCE, CYBERSECURITY CRIMES,
11 CYBERSECURITY PROVIDER, CYBERSECURITY PUR-
12 POSE, AND SELF-PROTECTED ENTITY.—The terms
13 “cyber threat information”, “cyber threat intel-
14 ligence”, “cybersecurity crimes”, “cybersecurity pro-
15 vider”, “cybersecurity purpose”, and “self-protected
16 entity” have the meaning given those terms in sec-
17 tion 1104 of the National Security Act of 1947, as
18 added by section 3(a) of this Act.

19 (3) INTELLIGENCE COMMUNITY.—The term
20 “intelligence community” has the meaning given the
21 term in section 3(4) of the National Security Act of
22 1947 (50 U.S.C. 401a(4)).

23 (4) SHARED SITUATIONAL AWARENESS.—The
24 term “shared situational awareness” means an envi-
25 ronment where cyber threat information is shared in

1 real time between all designated Federal cyber oper-
2 ations centers to provide actionable information
3 about all known cyber threats.

4 **SEC. 3. CYBER THREAT INTELLIGENCE AND INFORMATION**
5 **SHARING.**

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

9 “CYBER THREAT INTELLIGENCE AND INFORMATION
10 SHARING

11 “SEC. 1104. (a) INTELLIGENCE COMMUNITY SHAR-
12 ING OF CYBER THREAT INTELLIGENCE WITH PRIVATE
13 SECTOR AND UTILITIES.—

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

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

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

26 “(i) a certified entity; or

1 “(ii) a person with an appropriate se-
2 curity clearance to receive such cyber
3 threat intelligence;

4 “(B) shared consistent with the need to
5 protect the national security of the United
6 States;

7 “(C) used by a certified entity in a manner
8 which protects such cyber threat intelligence
9 from unauthorized disclosure; and

10 “(D) used, retained, or further disclosed by
11 a certified entity for cybersecurity purposes.

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

18 “(A) grant a security clearance on a tem-
19 porary or permanent basis to an employee,
20 independent contractor, or officer of a certified
21 entity;

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

1 “(C) expedite the security clearance proc-
2 ess for a person or entity as the head of such
3 element considers necessary, consistent with the
4 need to protect the national security of the
5 United States.

6 “(4) NO RIGHT OR BENEFIT.—The provision of
7 information to a private-sector entity or a utility
8 under this subsection shall not create a right or ben-
9 efit to similar information by such entity or such
10 utility or any other private-sector entity or utility.

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

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

22 “(1) IN GENERAL.—

23 “(A) CYBERSECURITY PROVIDERS.—Not-
24 withstanding any other provision of law, a cy-
25 bersecurity provider, with the express consent

1 of a protected entity for which such cybersecu-
2 rity provider is providing goods or services for
3 cybersecurity purposes, may, for cybersecurity
4 purposes—

5 “(i) use cybersecurity systems to iden-
6 tify and obtain cyber threat information to
7 protect the rights and property of such
8 protected entity; and

9 “(ii) share such cyber threat informa-
10 tion with any other entity designated by
11 such protected entity, including, if specifi-
12 cally designated, the entities of the Depart-
13 ment of Homeland Security and the De-
14 partment of Justice designated under
15 paragraphs (1) and (2) of section 2(b) of
16 the Cyber Intelligence Sharing and Protec-
17 tion Act.

18 “(B) SELF-PROTECTED ENTITIES.—Not-
19 withstanding any other provision of law, a self-
20 protected entity may, for cybersecurity pur-
21 poses—

22 “(i) use cybersecurity systems to iden-
23 tify and obtain cyber threat information to
24 protect the rights and property of such
25 self-protected entity; and

1 “(ii) share such cyber threat informa-
2 tion with any other entity, including the
3 entities of the Department of Homeland
4 Security and the Department of Justice
5 designated under paragraphs (1) and (2)
6 of section 2(b) of the Cyber Intelligence
7 Sharing and Protection Act.

8 “(2) USE AND PROTECTION OF INFORMA-
9 TION.—Cyber threat information shared in accord-
10 ance with paragraph (1)—

11 “(A) shall only be shared in accordance
12 with any restrictions placed on the sharing of
13 such information by the protected entity or self-
14 protected entity authorizing such sharing, in-
15 cluding appropriate anonymization or minimiza-
16 tion of such information and excluding limiting
17 a department or agency of the Federal Govern-
18 ment from sharing such information with an-
19 other department or agency of the Federal Gov-
20 ernment in accordance with this section;

21 “(B) may not be used by an entity to gain
22 an unfair competitive advantage to the det-
23 riment of the protected entity or the self-pro-
24 tected entity authorizing the sharing of infor-
25 mation;

1 “(C) may only be used by a non-Federal
2 recipient of such information for a cybersecurity
3 purpose;

4 “(D) if shared with the Federal Govern-
5 ment—

6 “(i) shall be exempt from disclosure
7 under section 552 of title 5, United States
8 Code (commonly known as the ‘Freedom of
9 Information Act’);

10 “(ii) shall be considered proprietary
11 information and shall not be disclosed to
12 an entity outside of the Federal Govern-
13 ment except as authorized by the entity
14 sharing such information;

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

17 “(iv) shall not be provided to another
18 department or agency of the Federal Gov-
19 ernment under paragraph (2)(A) if—

20 “(I) the entity providing such in-
21 formation determines that the provi-
22 sion of such information will under-
23 mine the purpose for which such in-
24 formation is shared; or

1 “(II) unless otherwise directed by
2 the President, the head of the depart-
3 ment or agency of the Federal Gov-
4 ernment receiving such cyber threat
5 information determines that the provi-
6 sion of such information will under-
7 mine the purpose for which such in-
8 formation is shared; and

9 “(v) shall be handled by the Federal
10 Government consistent with the need to
11 protect sources and methods and the na-
12 tional security of the United States; and

13 “(E) shall be exempt from disclosure under
14 a law or regulation of a State, political subdivi-
15 sion of a State, or a tribe that requires public
16 disclosure of information by a public or quasi-
17 public entity.

18 “(3) EXEMPTION FROM LIABILITY.—

19 “(A) EXEMPTION.—No civil or criminal
20 cause of action shall lie or be maintained in
21 Federal or State court against a protected enti-
22 ty, self-protected entity, cybersecurity provider,
23 or an officer, employee, or agent of a protected
24 entity, self-protected entity, or cybersecurity
25 provider, acting in good faith—

1 “(i) for using cybersecurity systems to
2 identify or obtain cyber threat information
3 or for sharing such information in accord-
4 ance with this section; or

5 “(ii) for decisions made for cybersecu-
6 rity purposes and based on cyber threat in-
7 formation identified, obtained, or shared
8 under this section.

9 “(B) LACK OF GOOD FAITH.—For pur-
10 poses of the exemption from liability under sub-
11 paragraph (A), a lack of good faith includes
12 any act or omission taken with intent to injure,
13 defraud, or otherwise endanger any individual,
14 government entity, private entity, or utility.

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

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

22 “(B) the applicability of other provisions of
23 law, including section 552 of title 5, United
24 States Code (commonly known as the ‘Freedom
25 of Information Act’), with respect to informa-

1 tion required to be provided to the Federal Gov-
2 ernment under such other provision of law.

3 “(5) RULE OF CONSTRUCTION.—Nothing in
4 this subsection shall be construed to provide new au-
5 thority to—

6 “(A) a cybersecurity provider to use a cy-
7 bersecurity system to identify or obtain cyber
8 threat information from a system or network
9 other than a system or network owned or oper-
10 ated by a protected entity for which such cyber-
11 security provider is providing goods or services
12 for cybersecurity purposes; or

13 “(B) a self-protected entity to use a cyber-
14 security system to identify or obtain cyber
15 threat information from a system or network
16 other than a system or network owned or oper-
17 ated by such self-protected entity.

18 “(c) FEDERAL GOVERNMENT USE OF INFORMA-
19 TION.—

20 “(1) LIMITATION.—The Federal Government
21 may use cyber threat information shared with the
22 Federal Government in accordance with subsection
23 (b)—

24 “(A) for cybersecurity purposes;

1 “(B) for the investigation and prosecution
2 of cybersecurity crimes;

3 “(C) for the protection of individuals from
4 the danger of death or serious bodily harm and
5 the investigation and prosecution of crimes in-
6 volving such danger of death or serious bodily
7 harm; or

8 “(D) for the protection of minors from
9 child pornography, any risk of sexual exploi-
10 tation, and serious threats to the physical safe-
11 ty of minors, including kidnapping and traf-
12 ficking and the investigation and prosecution of
13 crimes involving child pornography, any risk of
14 sexual exploitation, and serious threats to the
15 physical safety of minors, including kidnapping
16 and trafficking, and any crime referred to in
17 section 2258A(a)(2) of title 18, United States
18 Code.

19 “(2) AFFIRMATIVE SEARCH RESTRICTION.—
20 The Federal Government may not affirmatively
21 search cyber threat information shared with the
22 Federal Government under subsection (b) for a pur-
23 pose other than a purpose referred to in paragraph
24 (1).

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

4 “(A) require a private-sector entity or util-
5 ity to share information with the Federal Gov-
6 ernment; or

7 “(B) condition the sharing of cyber threat
8 intelligence with a private-sector entity or util-
9 ity on the provision of cyber threat information
10 to the Federal Government.

11 “(4) PROTECTION OF SENSITIVE PERSONAL
12 DOCUMENTS.—The Federal Government may not
13 use the following information, containing informa-
14 tion that identifies a person, shared with the Federal
15 Government in accordance with subsection (b):

16 “(A) Library circulation records.

17 “(B) Library patron lists.

18 “(C) Book sales records.

19 “(D) Book customer lists.

20 “(E) Firearms sales records.

21 “(F) Tax return records.

22 “(G) Educational records.

23 “(H) Medical records.

24 “(5) NOTIFICATION OF NON-CYBER THREAT IN-
25 FORMATION.—If a department or agency of the Fed-

1 eral Government receiving information pursuant to
2 subsection (b)(1) determines that such information
3 is not cyber threat information, such department or
4 agency shall notify the entity or provider sharing
5 such information pursuant to subsection (b)(1).

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

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

14 “(1) IN GENERAL.—If a department or agency
15 of the Federal Government intentionally or willfully
16 violates subsection (b)(3)(D) or subsection (c) with
17 respect to the disclosure, use, or protection of volun-
18 tarily shared cyber threat information shared under
19 this section, the United States shall be liable to a
20 person adversely affected by such violation in an
21 amount equal to the sum of—

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

1 “(B) the costs of the action together with
2 reasonable attorney fees as determined by the
3 court.

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

7 “(A) the district in which the complainant
8 resides;

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

11 “(C) the district in which the department
12 or agency of the Federal Government that dis-
13 closed the information is located; or

14 “(D) the District of Columbia.

15 “(3) STATUTE OF LIMITATIONS.—No action
16 shall lie under this subsection unless such action is
17 commenced not later than two years after the date
18 of the violation of subsection (b)(3)(D) or subsection
19 (c) that is the basis for the action.

20 “(4) EXCLUSIVE CAUSE OF ACTION.—A cause
21 of action under this subsection shall be the exclusive
22 means available to a complainant seeking a remedy
23 for a violation of subsection (b)(3)(D) or subsection
24 (c).

1 “(e) 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 “(f) 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 utility;

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; or

10 “(E) preclude the Federal Government
11 from requiring an entity to report significant
12 cyber incidents if authorized or required to do
13 so under another provision of law.

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

22 “(5) NO LIABILITY FOR NON-PARTICIPATION.—
23 Nothing in this section shall be construed to subject
24 a protected entity, self-protected entity, cybersecu-
25 rity provider, or an officer, employee, or agent of a

1 protected entity, self-protected entity, or cybersecu-
2 rity provider, to liability for choosing not to engage
3 in the voluntary activities authorized under this sec-
4 tion.

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

12 “(7) LIMITATION ON SURVEILLANCE.—Nothing
13 in this section shall be construed to authorize the
14 Department of Defense or the National Security
15 Agency or any other element of the intelligence com-
16 munity to target a United States person for surveil-
17 lance.

18 “(g) DEFINITIONS.—In this section:

19 “(1) AVAILABILITY.—The term ‘availability’
20 means ensuring timely and reliable access to and use
21 of information.

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

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

4 “(B) is able to demonstrate to the Director
5 of National Intelligence that such provider or
6 such entity can appropriately protect classified
7 cyber threat intelligence.

8 “(3) CONFIDENTIALITY.—The term ‘confiden-
9 tiality’ means preserving authorized restrictions on
10 access and disclosure, including means for protecting
11 personal privacy and proprietary information.

12 “(4) CYBER THREAT INFORMATION.—

13 “(A) IN GENERAL.—The term ‘cyber
14 threat information’ means information directly
15 pertaining to—

16 “(i) a vulnerability of a system or net-
17 work of a government or private entity or
18 utility;

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

1 “(iii) efforts to deny access to or de-
2 grade, disrupt, or destroy a system or net-
3 work of a government or private entity or
4 utility; or

5 “(iv) efforts to gain unauthorized ac-
6 cess to a system or network of a govern-
7 ment or private entity or utility, including
8 to gain such unauthorized access for the
9 purpose of exfiltrating information stored
10 on, processed on, or transiting a system or
11 network of a government or private entity
12 or utility.

13 “(B) EXCLUSION.—Such term does not in-
14 clude information pertaining to efforts to gain
15 unauthorized access to a system or network of
16 a government or private entity or utility that
17 solely involve violations of consumer terms of
18 service or consumer licensing agreements and
19 do not otherwise constitute unauthorized access.

20 “(5) CYBER THREAT INTELLIGENCE.—

21 “(A) IN GENERAL.—The term ‘cyber
22 threat intelligence’ means intelligence in the
23 possession of an element of the intelligence
24 community directly pertaining to—

1 “(i) a vulnerability of a system or net-
2 work of a government or private entity or
3 utility;

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

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

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

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

1 solely involve violations of consumer terms of
2 service or consumer licensing agreements and
3 do not otherwise constitute unauthorized access.

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

6 “(A) a crime under a Federal or State law
7 that involves—

8 “(i) efforts to deny access to or de-
9 grade, disrupt, or destroy a system or net-
10 work;

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

13 “(iii) efforts to exfiltrate information
14 from a system or network without author-
15 ization; or

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

22 “(7) CYBERSECURITY PROVIDER.—The term
23 ‘cybersecurity provider’ means a non-Federal entity
24 that provides goods or services intended to be used
25 for cybersecurity purposes.

1 “(8) CYBERSECURITY PURPOSE.—

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

7 “(i) a vulnerability of a system or net-
8 work;

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

14 “(iii) efforts to deny access to or de-
15 grade, disrupt, or destroy a system or net-
16 work; or

17 “(iv) efforts to gain unauthorized ac-
18 cess to a system or network, including to
19 gain such unauthorized access for the pur-
20 pose of exfiltrating information stored on,
21 processed on, or transiting a system or
22 network.

23 “(B) EXCLUSION.—Such term does not in-
24 clude the purpose of protecting a system or net-
25 work from efforts to gain unauthorized access

1 to such system or network that solely involve
2 violations of consumer terms of service or con-
3 sumer licensing agreements and do not other-
4 wise constitute unauthorized access.

5 “(9) CYBERSECURITY SYSTEM.—

6 “(A) IN GENERAL.—The term ‘cybersecu-
7 rity system’ means a system designed or em-
8 ployed to ensure the integrity, confidentiality,
9 or availability of, or safeguard, a system or net-
10 work, including protecting a system or network
11 from—

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

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

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

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

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

3 “(B) EXCLUSION.—Such term does not in-
4 clude a system designed or employed to protect
5 a system or network from efforts to gain unau-
6 thorized access to such system or network that
7 solely involve violations of consumer terms of
8 service or consumer licensing agreements and
9 do not otherwise constitute unauthorized access.

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

14 “(11) PROTECTED ENTITY.—The term ‘pro-
15 tected entity’ means an entity, other than an indi-
16 vidual, that contracts with a cybersecurity provider
17 for goods or services to be used for cybersecurity
18 purposes.

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

23 “(13) UTILITY.—The term ‘utility’ means an
24 entity providing essential services (other than law
25 enforcement or regulatory services), including elec-

1 tricity, natural gas, propane, telecommunications,
2 transportation, water, or wastewater services.”.

3 (b) PROCEDURES AND GUIDELINES.—The Director
4 of National Intelligence shall—

5 (1) not later than 60 days after the date of the
6 enactment of this Act, establish procedures under
7 paragraph (1) of section 1104(a) of the National Se-
8 curity Act of 1947, as added by subsection (a) of
9 this section, and issue guidelines under paragraph
10 (3) of such section 1104(a);

11 (2) in establishing such procedures and issuing
12 such guidelines, consult with the Secretary of Home-
13 land Security to ensure that such procedures and
14 such guidelines permit the owners and operators of
15 critical infrastructure to receive all appropriate cyber
16 threat intelligence (as defined in section 1104(h)(5)
17 of such Act, as added by subsection (a)) in the pos-
18 session of the Federal Government; and

19 (3) following the establishment of such proce-
20 dures and the issuance of such guidelines, expedi-
21 tiously distribute such procedures and such guide-
22 lines to appropriate departments and agencies of the
23 Federal Government, private-sector entities, and
24 utilities (as defined in section 1104(h)(13) of such
25 Act, as added by subsection (a)).

1 (c) PRIVACY AND CIVIL LIBERTIES POLICIES AND
2 PROCEDURES.—Not later than 60 days after the date of
3 the enactment of this Act, the Director of National Intel-
4 ligence, in consultation with the Secretary of Homeland
5 Security and the Attorney General, shall establish the poli-
6 cies and procedures required under section 1104(c)(7)(A)
7 of the National Security Act of 1947, as added by sub-
8 section (a) of this section.

9 (d) INITIAL REPORTS.—The first reports required to
10 be submitted under paragraphs (1) and (2) of subsection
11 (e) of section 1104 of the National Security Act of 1947,
12 as added by subsection (a) of this section, shall be sub-
13 mitted not later than 1 year after the date of the enact-
14 ment of this Act.

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

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

19 **SEC. 4. SUNSET.**

20 Effective on the date that is 5 years after the date
21 of the enactment of this Act—

22 (1) section 1104 of the National Security Act of
23 1947, as added by section 2(a) of this Act, is re-
24 pealed; and

- 1 eral Government to provide information services to provide
- 2 information about cybersecurity incidents that do not pose
- 3 a threat to the Federal Government's information.

