

APRIL 11, 2013

RULES COMMITTEE PRINT 113-7
TEXT OF H.R. 624, CYBER INTELLIGENCE
SHARING AND PROTECTION ACT

[Showing the text of H.R. 624 as ordered reported by the Permanent Select Committee on Intelligence with a modification.]

1   **SECTION 1. SHORT TITLE.**

2   This Act may be cited as the “Cyber Intelligence
3   Sharing and Protection Act”.

4 SEC. 2. CYBER THREAT INTELLIGENCE AND INFORMATION
5 SHARING.

(a) IN GENERAL.—Title XI of the National Security Act of 1947 (50 U.S.C. 442 et seq.) is amended by adding 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.—

“(1) IN GENERAL.—The Director of National Intelligence shall establish procedures to allow elements of the intelligence community to share cyber threat intelligence with private-sector entities and

1 utilities and to encourage the sharing of such intel-
2 ligence.

3 “(2) SHARING AND USE OF CLASSIFIED INTEL-
4 LIGENCE.—The procedures established under para-
5 graph (1) shall provide that classified cyber threat
6 intelligence may only be—

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

9 “(i) a certified entity; or

10 “(ii) a person with an appropriate se-
11 curity clearance to receive such cyber
12 threat intelligence;

13 “(B) shared consistent with the need to
14 protect the national security of the United
15 States; and

16 “(C) used by a certified entity in a manner
17 which protects such cyber threat intelligence
18 from unauthorized disclosure.

19 “(3) SECURITY CLEARANCE APPROVALS.—The
20 Director of National Intelligence shall issue guide-
21 lines providing that the head of an element of the
22 intelligence community may, as the head of such ele-
23 ment considers necessary to carry out this sub-
24 section—

1   “(A) grant a security clearance on a tem-
2   porary or permanent basis to an employee or
3   officer of a certified entity;

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

7   “(C) expedite the security clearance proc-
8   ess for a person or entity as the head of such
9   element considers necessary, consistent with the
10   need to protect the national security of the
11   United States.

12   “(4) NO RIGHT OR BENEFIT.—The provision of
13   information to a private-sector entity or a utility
14   under this subsection shall not create a right or ben-
15   efit to similar information by such entity or such
16   utility or any other private-sector entity or utility.

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

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

3   “(1) IN GENERAL.—

4   “(A) CYBERSECURITY PROVIDERS.—Not-
5   withstanding any other provision of law, a cy-
6   bersecurity provider, with the express consent
7   of a protected entity for which such cybersecu-
8   rity provider is providing goods or services for
9   cybersecurity purposes, may, for cybersecurity
10   purposes—

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

15   “(ii) share such cyber threat informa-
16   tion with any other entity designated by
17   such protected entity, including, if specifi-
18   cally designated, the Federal Government.

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

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

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

3 “(ii) share such cyber threat informa-
4 tion with any other entity, including the
5 Federal Government.

6 “(2) SHARING WITH THE FEDERAL GOVERN-
7 MENT.—

8 “(A) INFORMATION SHARED WITH THE
9 NATIONAL CYBERSECURITY AND COMMUNICA-
10 TIONS INTEGRATION CENTER OF THE DEPART-
11 MENT OF HOMELAND SECURITY.—Subject to
12 the use and protection of information require-
13 ments under paragraph (3), the head of a de-
14 partment or agency of the Federal Government
15 receiving cyber threat information in accordance
16 with paragraph (1) shall provide such cyber
17 threat information in as close to real time as
18 possible to the National Cybersecurity and
19 Communications Integration Center of the De-
20 partment of Homeland Security.

21 “(B) REQUEST TO SHARE WITH ANOTHER
22 DEPARTMENT OR AGENCY OF THE FEDERAL
23 GOVERNMENT.—An entity sharing cyber threat
24 information that is provided to the National Cy-
25 bersecurity and Communications Integration

1 Center of the Department of Homeland Secu-
2 rity under subparagraph (A) or paragraph (1)
3 may request the head of such Center to, and
4 the head of such Center may, provide such in-
5 formation in as close to real time as possible to
6 another department or agency of the Federal
7 Government.

8 “(3) 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 by the de-
18   partment or agency of the Federal Govern-
19   ment receiving such cyber threat informa-
20   tion to another department or agency of
21   the Federal Government under paragraph
22   (2)(A) if—

23   “(I) the entity providing such in-
24   formation determines that the provi-
25   sion of such information will under-

1 mine the purpose for which such in-
2 formation is shared; or

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

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

15 “(E) shall be exempt from disclosure under
16 a State, local, or tribal law or regulation that
17 requires public disclosure of information by a
18 public or quasi-public entity.

19 “(4) EXEMPTION FROM LIABILITY.—

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

1   entity, self-protected entity, or cybersecurity
2   provider, acting in good faith—

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

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

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

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

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

24   “(B) the applicability of other provisions of
25   law, including section 552 of title 5, United

1 States Code (commonly known as the ‘Freedom
2 of Information Act’), with respect to informa-
3 tion required to be provided to the Federal Gov-
4 ernment under such other provision of law.

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

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

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

20 “(c) FEDERAL GOVERNMENT USE OF INFORMA-
21 TION.—

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

1 “(A) for cybersecurity purposes;

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

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

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

20 “(2) AFFIRMATIVE SEARCH RESTRICTION.—

21 The Federal Government may not affirmatively
22 search cyber threat information shared with the
23 Federal Government under subsection (b) for a pur-
24 pose other than a purpose referred to in paragraph
25 (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) unless
16   such information is used in accordance with the poli-
17   cies and procedures established under paragraph (7):

18   “(A) Library circulation records.

19   “(B) Library patron lists.

20   “(C) Book sales records.

21   “(D) Book customer lists.

22   “(E) Firearms sales records.

23   “(F) Tax return records.

24   “(G) Educational records.

25   “(H) Medical records.

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

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

13   “(7) PRIVACY AND CIVIL LIBERTIES.—

14   “(A) POLICIES AND PROCEDURES.—The
15   Director of National Intelligence, in consulta-
16   tion with the Secretary of Homeland Security
17   and the Attorney General, shall establish and
18   periodically review policies and procedures gov-
19   erning the receipt, retention, use, and disclosure
20   of non-publicly available cyber threat informa-
21   tion shared with the Federal Government in ac-
22   cordance with subsection (b)(1). Such policies
23   and procedures shall, consistent with the need
24   to protect systems and networks from cyber

1 threats and mitigate cyber threats in a timely
2 manner—

3 “(i) minimize the impact on privacy
4 and civil liberties;

5 “(ii) reasonably limit the receipt, re-
6 tention, use, and disclosure of cyber threat
7 information associated with specific per-
8 sons that is not necessary to protect sys-
9 tems or networks from cyber threats or
10 mitigate cyber threats in a timely manner;

11 “(iii) include requirements to safe-
12 guard non-publicly available cyber threat
13 information that may be used to identify
14 specific persons from unauthorized access
15 or acquisition;

16 “(iv) protect the confidentiality of
17 cyber threat information associated with
18 specific persons to the greatest extent
19 practicable; and

20 “(v) not delay or impede the flow of
21 cyber threat information necessary to de-
22 fend against or mitigate a cyber threat.

23 “(B) SUBMISSION TO CONGRESS.—The Di-
24 rector of National Intelligence shall, consistent
25 with the need to protect sources and methods,

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

4 “(C) IMPLEMENTATION.—The head of
5 each department or agency of the Federal Gov-
6 ernment receiving cyber threat information
7 shared with the Federal Government under sub-
8 section (b)(1) shall—

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

12 “(ii) promptly notify the Director of
13 National Intelligence, the Attorney Gen-
14 eral, and the congressional intelligence
15 committees of any significant violations of
16 such policies and procedures.

17 “(D) OVERSIGHT.—The Director of Na-
18 tional Intelligence, in consultation with the At-
19 torney General, the Secretary of Homeland Se-
20 curity, and the Secretary of Defense, shall es-
21 tablish a program to monitor and oversee com-
22 pliance with the policies and procedures estab-
23 lished under subparagraph (A).

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

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

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

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

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

21   “(A) the district in which the complainant
22 resides;

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

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

4   “(D) the District of Columbia.

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

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

15   “(e) REPORTS ON INFORMATION SHARING.—

16   “(1) INSPECTOR GENERAL REPORT.—The In-
17   spector General of the Intelligence Community, in
18   consultation with the Inspector General of the De-
19   partment of Justice, the Inspector General of the
20   Department of Defense, and the Privacy and Civil
21   Liberties Oversight Board, shall annually submit to
22   the congressional intelligence committees a report
23   containing a review of the use of information shared
24   with the Federal Government under this section, in-
25   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) PRIVACY AND CIVIL LIBERTIES OFFICERS
23   REPORT.—The Civil Liberties Protection Officer of
24   the Office of the Director of National Intelligence
25   and the Chief Privacy and Civil Liberties Officer of

1 the Department of Justice, in consultation with the
2 Privacy and Civil Liberties Oversight Board, the In-
3 spector General of the Intelligence Community, and
4 the senior privacy and civil liberties officer of each
5 department or agency of the Federal Government
6 that receives cyber threat information shared with
7 the Federal Government under this section, shall an-
8 nually and jointly submit to Congress a report as-
9 sessing the privacy and civil liberties impact of the
10 activities conducted by the Federal Government
11 under this section. Such report shall include any rec-
12 ommendations the Civil Liberties Protection Officer
13 and Chief Privacy and Civil Liberties Officer con-
14 sider appropriate to minimize or mitigate the privacy
15 and civil liberties impact of the sharing of cyber
16 threat information under this section.

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

24 “(g) SAVINGS CLAUSES.—

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

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

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

19   “(A) limit or modify an existing informa-
20   tion sharing relationship;

21   “(B) prohibit a new information sharing
22   relationship;

23   “(C) require a new information sharing re-
24   lationship between the Federal Government and
25   a private-sector entity or utility;

1   “(D) modify the authority of a department
2   or agency of the Federal Government to protect
3   sources and methods and the national security
4   of the United States; or

5   “(E) preclude the Federal Government
6   from requiring an entity to report significant
7   cyber incidents if authorized or required to do
8   so under another provision of law.

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

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

8 “(ii) a threat to the integrity, con-
9 fidentiality, or availability of a system or
10 network of a government or private entity
11 or utility 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 of a government or private entity or
17 utility; or

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

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

8   “(5) CYBER THREAT INTELLIGENCE.—

9   “(A) IN GENERAL.—The term ‘cyber
10   threat intelligence’ means intelligence in the
11   possession of an element of the intelligence
12   community directly pertaining to—

13   “(i) a vulnerability of a system or net-
14   work of a government or private entity or
15   utility;

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

22   “(iii) efforts to deny access to or de-
23   grade, disrupt, or destroy a system or net-
24   work of a government or private entity or
25   utility; or

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

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

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

18   “(A) a crime under a Federal or State law
19   that involves—

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

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

1 “(iii) efforts to exfiltrate information
2 from a system or network without author-
3 ization; or

4 “(B) the violation of a provision of Federal
5 law relating to computer crimes, including a
6 violation of any provision of title 18, United
7 States Code, created or amended by the Com-
8 puter Fraud and Abuse Act of 1986 (Public
9 Law 99–474).

10 “(7) CYBERSECURITY PROVIDER.—The term
11 ‘cybersecurity provider’ means a non-Federal entity
12 that provides goods or services intended to be used
13 for cybersecurity purposes.

14 “(8) CYBERSECURITY PURPOSE.—

15 “(A) IN GENERAL.—The term ‘cybersecu-
16 rity purpose’ means the purpose of ensuring the
17 integrity, confidentiality, or availability of, or
18 safeguarding, a system or network, including
19 protecting a system or network from—

20 “(i) a vulnerability of a system or net-
21 work;

22 “(ii) a threat to the integrity, con-
23 fidentiality, or availability of a system or
24 network or any information stored on,

1 processed on, or transiting such a system
2 or network;

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

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

12 “(B) EXCLUSION.—Such term does not in-
13 clude the purpose of protecting a system or net-
14 work from efforts to gain unauthorized access
15 to such system or network that solely involve
16 violations of consumer terms of service or con-
17 sumer licensing agreements and do not other-
18 wise constitute unauthorized access.

19 “(9) CYBERSECURITY SYSTEM.—

20 “(A) IN GENERAL.—The term ‘cybersecu-
21 rity system’ means a system designed or em-
22 ployed to ensure the integrity, confidentiality,
23 or availability of, or safeguard, a system or net-
24 work, including protecting a system or network
25 from—

1 “(i) a vulnerability of a system or net-
2 work;

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

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

11 “(iv) efforts to gain unauthorized ac-
12 cess to a system or network, including to
13 gain such unauthorized access for the pur-
14 pose of exfiltrating information stored on,
15 processed on, or transiting a system or
16 network.

17 “(B) EXCLUSION.—Such term does not in-
18 clude a system designed or employed to protect
19 a system or network from efforts to gain unau-
20 thorized access to such system or network that
21 solely involve violations of consumer terms of
22 service or consumer licensing agreements and
23 do not otherwise constitute unauthorized access.

24 “(10) INTEGRITY.—The term ‘integrity’ means
25 guarding against improper information modification

1 or destruction, including ensuring information non-
2 repudiation and authenticity.

3 “(11) PROTECTED ENTITY.—The term ‘pro-
4 tected entity’ means an entity, other than an indi-
5 vidual, that contracts with a cybersecurity provider
6 for goods or services to be used for cybersecurity
7 purposes.

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

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

17 (b) PROCEDURES AND GUIDELINES.—The Director
18 of National Intelligence shall—

19 (1) not later than 60 days after the date of the
20 enactment of this Act, establish procedures under
21 paragraph (1) of section 1104(a) of the National Se-
22 curity Act of 1947, as added by subsection (a) of
23 this section, and issue guidelines under paragraph
24 (3) of such section 1104(a);

1   (2) in establishing such procedures and issuing
2   such guidelines, consult with the Secretary of Home-
3   land Security to ensure that such procedures and
4   such guidelines permit the owners and operators of
5   critical infrastructure to receive all appropriate cyber
6   threat intelligence (as defined in section 1104(h)(5)
7   of such Act, as added by subsection (a)) in the pos-
8   session of the Federal Government; and

9   (3) following the establishment of such proce-
10   dures and the issuance of such guidelines, expedi-
11   tiously distribute such procedures and such guide-
12   lines to appropriate departments and agencies of the
13   Federal Government, private-sector entities, and
14   utilities (as defined in section 1104(h)(13) of such
15   Act, as added by subsection (a)).

16   (c) PRIVACY AND CIVIL LIBERTIES POLICIES AND
17   PROCEDURES.—Not later than 60 days after the date of
18   the enactment of this Act, the Director of National Intel-
19   ligence, in consultation with the Secretary of Homeland
20   Security and the Attorney General, shall establish the poli-
21   cies and procedures required under section 1104(c)(7)(A)
22   of the National Security Act of 1947, as added by sub-
23   section (a) of this section.

24   (d) INITIAL REPORTS.—The first reports required to
25   be submitted under paragraphs (1) and (2) of subsection

1 (e) of section 1104 of the National Security Act of 1947,
2 as added by subsection (a) of this section, shall be sub-
3 mitted not later than 1 year after the date of the enact-
4 ment of this Act.

5 (e) TABLE OF CONTENTS AMENDMENT.—The table
6 of contents in the first section of the National Security
7 Act of 1947 is amended by adding at the end the following
8 new item:

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

9 **SEC. 3. SUNSET.**

10 Effective on the date that is 5 years after the date
11 of the enactment of this Act—

12 (1) section 1104 of the National Security Act of
13 1947, as added by section 2(a) of this Act, is re-
14 pealed; and

15 (2) the table of contents in the first section of
16 the National Security Act of 1947, as amended by
17 section 2(d) of this Act, is amended by striking the
18 item relating to section 1104, as added by such sec-
19 tion 2(d).

