

113TH CONGRESS
2D SESSION

S. _____

To authorize private entities to prevent, investigate, and mitigate cybersecurity threats, to authorize the sharing of cyber threat indicators and countermeasures, and for other purposes.

IN THE SENATE OF THE UNITED STATES

_____ introduced the following bill; which was read twice
and referred to the Committee on _____

A BILL

To authorize private entities to prevent, investigate, and mitigate cybersecurity threats, to authorize the sharing of cyber threat indicators and countermeasures, 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; TABLE OF CONTENTS.**

4 (a) SHORT TITLE.—This Act may be cited as the
5 “Cybersecurity Information Sharing Act of 2014”.

6 (b) TABLE OF CONTENTS.—The table of contents of
7 this Act is as follows:

Sec. 1. Short title; table of contents.

Sec. 2. Definitions.

Sec. 3. Sharing of information by the Federal Government.

- Sec. 4. Authorizations for preventing, investigating, or mitigating cybersecurity threats.
- Sec. 5. Sharing of cyber threat indicators and countermeasures with the Federal Government.
- Sec. 6. Protection from liability.
- Sec. 7. Oversight of Government activities.
- Sec. 8. Construction and preemption.
- Sec. 9. Conforming amendments.

1 **SEC. 2. DEFINITIONS.**

2 In this Act:

3 (1) AGENCY.—The term “agency” has the
4 meaning given the term in section 3502 of title 44,
5 United States Code.

6 (2) ANTITRUST LAWS.—The term “antitrust
7 laws”—

8 (A) has the meaning given the term in sec-
9 tion 1(a) of the Clayton Act (15 U.S.C. 12(a));

10 (B) includes section 5 of the Federal
11 Trade Commission Act (15 U.S.C. 45) to the
12 extent that section 5 of that Act applies to un-
13 fair methods of competition; and

14 (C) includes any State law that has the
15 same intent and effect as the laws under sub-
16 paragraphs (A) and (B).

17 (3) APPROPRIATE FEDERAL ENTITIES.—The
18 term “appropriate Federal entities” means the fol-
19 lowing:

20 (A) The Department of Commerce.

21 (B) The Department of Defense.

1 (C) The Department of Energy.

2 (D) The Department of Homeland Secu-
3 rity.

4 (E) The Department of Justice.

5 (F) The Office of the Director of National
6 Intelligence.

7 (4) COUNTERINTELLIGENCE.—The term “coun-
8 terintelligence” has the meaning given the term in
9 section 3 of the National Security Act of 1947 (50
10 U.S.C. 3003).

11 (5) COUNTERMEASURE.—The term “counter-
12 measure” means any action, device, procedure, tech-
13 nique, or other measure that meets or counters a
14 threat, vulnerability, or attack by eliminating or pre-
15 venting it, or by minimizing the harm it may cause.

16 (6) CYBERSECURITY PURPOSE.—The term “cy-
17 bersecurity purpose” means the purpose of pro-
18 tecting an information system or information that is
19 stored on, processed by, or transiting an information
20 system from a cybersecurity threat or security vul-
21 nerability.

22 (7) CYBERSECURITY THREAT.—The term “cy-
23 bersecurity threat” means any action that may re-
24 sult in an unauthorized effort, not protected by the
25 First Amendment to the Constitution of the United

1 States, to adversely impact the security, availability,
2 confidentiality, or integrity of an information system
3 or information that is stored on, processed by, or
4 transiting an information system.

5 (8) CYBER THREAT INDICATOR.—The term
6 “cyber threat indicator” means information that in-
7 dicates, describes, or is necessary to identify—

8 (A) malicious reconnaissance, including
9 anomalous patterns of communications that ap-
10 pear to be transmitted for the purpose of gath-
11 ering technical information related to a cyberse-
12 curity threat;

13 (B) a method of defeating a security con-
14 trol;

15 (C) a security vulnerability;

16 (D) a method of causing a user with legiti-
17 mate access to an information system or infor-
18 mation that is stored on, processed by, or
19 transiting an information system to unwittingly
20 enable the defeat of a security control;

21 (E) malicious cyber command and control;

22 (F) the actual or potential harm caused by
23 an incident, including information exfiltrated
24 when it is necessary in order to describe a cy-
25 bersecurity threat;

1 (G) any other attribute of a cybersecurity
2 threat, if disclosure of such attribute is not oth-
3 erwise prohibited by law; or

4 (H) any combination thereof.

5 (9) ENTITY.—

6 (A) IN GENERAL.—The term “entity”
7 means any private entity, non-Federal govern-
8 ment agency or department, or State, tribal, or
9 local government agency or department (includ-
10 ing an officer, employee, or agent thereof).

11 (B) INCLUSIONS.—The term “entity” in-
12 cludes a government agency or department (in-
13 cluding an officer, employee, or agent thereof)
14 of the District of Columbia, the Commonwealth
15 of Puerto Rico, the Virgin Islands, Guam,
16 American Samoa, the Northern Mariana Is-
17 lands, and any other territory or possession of
18 the United States.

19 (C) EXCLUSION.—The term “entity” does
20 not include a foreign power as defined in sec-
21 tion 101(a) of the Foreign Intelligence Surveil-
22 lance Act of 1978 (50 U.S.C. 1801).

23 (10) FEDERAL ENTITY.—The term “Federal
24 entity” means a department or agency of the United

1 States, or any component, officer, employee, or
2 agent of such a department or agency.

3 (11) FOREIGN INTELLIGENCE.—The term “for-
4 eign intelligence” has the meaning given the term in
5 section (3) of the National Security Act of 1947 (50
6 U.S.C. 3003).

7 (12) INFORMATION SYSTEM.—The term “infor-
8 mation system” has the meaning given the term in
9 section 3502 of title 44, United States Code.

10 (13) LOCAL GOVERNMENT.—The term “local
11 government” means any borough, city, county, par-
12 ish, town, township, village, or other general purpose
13 political subdivision of a State.

14 (14) MALICIOUS CYBER COMMAND AND CON-
15 TROL.—The term “malicious cyber command and
16 control” means a method for unauthorized remote
17 identification of, access to, or use of, an information
18 system or information that is stored on, processed
19 by, or transiting an information system.

20 (15) MALICIOUS RECONNAISSANCE.—The term
21 “malicious reconnaissance” means a method for ac-
22 tively probing or passively monitoring an information
23 system for the purpose of discerning security
24 vulnerabilities of the information system, if such

1 method is associated with a known or suspected cy-
2 bersecurity threat.

3 (16) MONITOR.—The term “monitor” means
4 the interception, acquisition, or collection of informa-
5 tion that is stored on, processed by, or transiting an
6 information system.

7 (17) PRIVATE ENTITY.—

8 (A) IN GENERAL.—The term “private enti-
9 ty” means any individual or private group, or-
10 ganization, proprietorship, partnership, trust,
11 cooperative, utility, corporation, or other com-
12 mercial entity, including an officer, employee, or
13 agent thereof.

14 (B) EXCLUSION.—The term “private enti-
15 ty” does not include a foreign power as defined
16 in section 101(a) of the Foreign Intelligence
17 Surveillance Act of 1978 (50 U.S.C. 1801).

18 (18) SECURITY CONTROL.—The term “security
19 control” means the management, operational, and
20 technical controls prescribed for an information sys-
21 tem to protect the confidentiality, integrity, and
22 availability of the system and its information.

23 (19) SECURITY VULNERABILITY.—The term
24 “security vulnerability” means any attribute of hard-

1 ware, software, process, or procedure that could en-
2 able or facilitate the defeat of a security control.

3 (20) TRIBAL.—The term “tribal” has the
4 meaning given the term “Indian tribe” in section 4
5 of the Indian Self-Determination and Education As-
6 sistance Act (25 U.S.C. 450b).

7 (21) UNITED STATES PERSON.—The term
8 “United States person” has the meaning given the
9 term in section 101(i) of the Foreign Intelligence
10 Surveillance Act of 1978 (50 U.S.C. 1801).

11 (22) UTILITY.—The term “utility” means a
12 provider of essential services (other than law en-
13 forcement or regulatory services), including elec-
14 tricity, natural gas, propane, telecommunications,
15 transportation, rail, water, or wastewater services.

16 **SEC. 3. SHARING OF INFORMATION BY THE FEDERAL GOV-**
17 **ERNMENT.**

18 (a) IN GENERAL.—Consistent with the protection of
19 intelligence sources and methods and the protection of pri-
20 vacy and civil liberties, the Director of National Intel-
21 ligence, the Secretary of Homeland Security, and the At-
22 torney General, in consultation with the heads of the ap-
23 propriate Federal agencies, shall develop and promulgate
24 procedures to facilitate and promote—

1 (1) the timely sharing of classified cyber threat
2 indicators in the possession of the Federal Govern-
3 ment with cleared representatives of appropriate en-
4 tities;

5 (2) the timely sharing with appropriate entities
6 of cyber threat indicators in the possession of the
7 Federal Government that may be declassified and
8 shared at an unclassified level; and

9 (3) the sharing with appropriate entities, or, if
10 appropriate, public availability, of unclassified, in-
11 cluding controlled unclassified, cyber threat indica-
12 tors in the possession of the Federal Government.

13 (b) DEVELOPMENT OF PROCEDURES.—

14 (1) IN GENERAL.—The procedures developed
15 and promulgated under subsection (a) shall—

16 (A) ensure the Federal Government has
17 and maintains the capability to share cyber
18 threat indicators in real time consistent with
19 the protection of classified information; and

20 (B) incorporate, to the greatest extent pos-
21 sible, existing processes and existing roles and
22 responsibilities of Federal and non-Federal enti-
23 ties for information sharing by the Federal
24 Government, including sector specific informa-
25 tion sharing and analysis centers.

1 (2) COORDINATION.—In developing the proce-
2 dures required under this section, the Director of
3 National Intelligence, the Secretary of Homeland Se-
4 curity, and the Attorney General shall coordinate
5 with appropriate entities to ensure that effective pro-
6 tocols are implemented that will facilitate and pro-
7 mote the sharing of cyber threat indicators by the
8 Federal Government in a timely manner.

9 (c) SUBMITTAL TO CONGRESS.—Not later than 60
10 days after the date of the enactment of this Act, the Direc-
11 tor of National Intelligence, in consultation with the heads
12 of the appropriate Federal entities, shall submit to Con-
13 gress the procedures required by subsection (a).

14 **SEC. 4. AUTHORIZATIONS FOR PREVENTING, INVES-**
15 **TIGATING, OR MITIGATING CYBERSECURITY**
16 **THREATS.**

17 (a) AUTHORIZATION FOR MONITORING.—

18 (1) IN GENERAL.—Notwithstanding any other
19 provision of law, a private entity may, **[only]** for cy-
20 bersecurity purposes and in order to obtain, identify,
21 or otherwise possess cyber threat indicators, mon-
22 itor—

23 (A) the information systems of such pri-
24 vate entity;

1 (B) the information systems of another en-
2 tity, upon written consent of such other entity;

3 (C) the information systems of a Federal
4 entity, upon written consent of an authorized
5 representative of the Federal entity; and

6 (D) information that is stored on, proc-
7 essed by, or transiting the information systems
8 monitored by the private entity under this para-
9 graph.

10 (2) CONSTRUCTION.—Nothing in this sub-
11 section shall be construed to authorize the moni-
12 toring of information systems to identify or obtain
13 cyber threat indicators, other than as provided in
14 this subsection.

15 (b) AUTHORIZATION FOR OPERATION OF COUNTER-
16 MEASURES.—Notwithstanding any other provision of law,
17 a private entity may, **【only】** for cybersecurity purposes,
18 operate countermeasures—

19 (1) on the information systems of such private
20 entity in order to protect the rights or property of
21 the private entity;

22 (2) on the information systems of another enti-
23 ty upon written consent of such entity to protect the
24 rights or property of such entity; and

1 (3) on the information systems of a Federal en-
2 tity upon written consent of an authorized represent-
3 ative of such Federal entity to protect the rights or
4 property of the Federal Government.

5 (c) AUTHORIZATION FOR SHARING OR RECEIVING
6 CYBER THREAT INDICATORS.—Notwithstanding any
7 other provision of law, and [*OPTION A*: “only for the pur-
8 pose of preventing, investigating, or otherwise mitigating
9 cybersecurity threats to information systems or informa-
10 tion that is stored on, processed by, or transiting an infor-
11 mation system,”] *OR* [*OPTION B*: “for the purposes per-
12 mitted under this Act”] an entity may, consistent with the
13 protection of classified information, share with, or receive
14 from, any other entity or the Federal Government cyber
15 threat indicators and countermeasures.

16 (d) USE AND PROTECTION OF INFORMATION.—

17 (1) SECURITY OF INFORMATION.—Anyone mon-
18 itoring information systems, operating counter-
19 measures, or providing or receiving cyber threat in-
20 dicators under this section shall implement and uti-
21 lize security controls to prevent unauthorized access
22 or acquisition of communications, records, system
23 traffic, or other information, consistent with the
24 need to protect information systems or information
25 that is stored on, processed by, or transiting an in-

1 formation system from cybersecurity threats or to
2 mitigate such threats.

3 (2) REMOVAL OF CERTAIN PERSONAL INFORMA-
4 TION.—An entity sharing cyber threat indicators
5 pursuant to this Act shall, prior to such sharing, re-
6 move any information contained within such indica-
7 tors that is known to be personal information of or
8 identifying a United States person, not directly re-
9 lated to a cybersecurity threat in order to ensure
10 that such information is protected from unauthor-
11 ized disclosure to any other entity or the Federal
12 Government.

13 (3) USE OF CYBER THREAT INDICATORS BY EN-
14 TITIES.—Consistent with this Act and except as pro-
15 vided in paragraph (5), cyber threat indicators or
16 countermeasures shared or received under this sec-
17 tion may, for cybersecurity purposes—

18 (A) be used by a private entity to monitor
19 or operate countermeasures on its information
20 systems, or the information systems of another
21 entity or a Federal entity upon the written con-
22 sent of that other entity or that Federal entity;
23 and

24 (B) be otherwise used, retained, and fur-
25 ther shared by an entity.

1 (4) LIMITATION ON USE OF CYBER THREAT IN-
2 DICATORS.—Cyber threat indicators shared or re-
3 ceived under this section shall not be used—

4 (A) for any purpose, unless otherwise au-
5 thorized by this Act, other than to protect in-
6 formation systems or information that is stored
7 on, processed by, or transiting an information
8 system from cybersecurity threats or to miti-
9 gate such threats; or

10 (B) to gain an unfair competitive advan-
11 tage to the detriment of the entity authorizing
12 such monitoring or countermeasures, and the
13 conduct described in subsection (e) shall not
14 constitute unfair competitive conduct.

15 (5) USE OF CYBER THREAT INDICATORS BY
16 STATE, TRIBAL, OR LOCAL DEPARTMENTS OR AGEN-
17 CIES.—

18 (A) LAW ENFORCEMENT USE.—

19 (i) PRIOR WRITTEN CONSENT.—Ex-
20 cept as provided in clause (ii), cyber threat
21 indicators shared with a State, tribal, or
22 local department or agency under this sec-
23 tion may, with the prior written consent of
24 the entity sharing such indicators, be used
25 by a State, tribal, or local department or

1 agency for the purpose of preventing, in-
2 vestigating, or prosecuting a criminal act.

3 (ii) ORAL CONSENT.—If the need for
4 immediate use prevents obtaining written
5 consent, such consent may be provided
6 orally with subsequent documentation of
7 the consent.

8 (B) EXEMPTION FROM DISCLOSURE.—
9 Cyber threat indicators shared with a State,
10 tribal, or local department or agency under this
11 section shall be—

12 (i) deemed voluntarily shared informa-
13 tion; and

14 (ii) exempt from disclosure under any
15 State, tribal, or local law requiring disclo-
16 sure of information or records.

17 (C) STATE, TRIBAL, AND LOCAL REGU-
18 LATORY AUTHORITY.—

19 (i) AUTHORIZATION.—Cyber threat
20 indicators shared with a State, tribal, or
21 local department or agency under this sec-
22 tion may, consistent with State regulatory
23 authority specifically relating to the pre-
24 vention or mitigation of cybersecurity
25 threats to information systems, inform the

1 development or implementation of regula-
2 tions relating to such information systems.

3 (ii) LIMITATION.—Such cyber threat
4 indicators shall not otherwise be directly
5 used by any State, tribal, or local depart-
6 ment or agency to regulate the lawful ac-
7 tivities of an entity.

8 (iii) EXCEPTION.—Any procedures re-
9 quired to be developed and implemented
10 under this Act shall not be considered reg-
11 ulations within the meaning of this sub-
12 paragraph.

13 (e) ANTITRUST EXEMPTION.—

14 (1) IN GENERAL.—It shall not be considered a
15 violation of any provision of antitrust laws for two
16 or more private entities to exchange or provide cyber
17 threat indicators, or assistance relating to the pre-
18 vention, investigation, or mitigation of cybersecurity
19 threats, for cybersecurity purposes under this Act.

20 (2) APPLICABILITY.—Paragraph (1) shall apply
21 only to information that is exchanged or assistance
22 provided in order to assist with—

23 (A) facilitating the prevention, investiga-
24 tion, or mitigation of cybersecurity threats to
25 information systems or information that is

1 stored on, processed by, or transiting an infor-
2 mation system; or

3 (B) communicating or disclosing cyber
4 threat indicators to help prevent, investigate, or
5 mitigate the effects of cybersecurity threats to
6 information systems or information that is
7 stored on, processed by, or transiting an infor-
8 mation system.

9 (f) NO RIGHT OR BENEFIT.—The sharing of cyber
10 threat indicators with an entity under this Act shall not
11 create a right or benefit to similar information by such
12 entity or any other entity.

13 **SEC. 5. SHARING OF CYBER THREAT INDICATORS AND**
14 **COUNTERMEASURES WITH THE FEDERAL**
15 **GOVERNMENT.**

16 (a) REQUIREMENT FOR POLICIES AND PROCE-
17 DURES.—

18 (1) INTERIM POLICIES AND PROCEDURES.—Not
19 later than 30 days after the date of the enactment
20 of this Act, the Attorney General, in coordination
21 with the heads of the appropriate Federal entities,
22 shall develop, and submit to Congress, interim poli-
23 cies and procedures relating to the receipt of cyber
24 threat indicators and countermeasures by the Fed-
25 eral Government.

1 (2) FINAL POLICIES AND PROCEDURES.—Not
2 later than 60 days after the date of the enactment
3 of this Act, the Attorney General, in coordination
4 with the heads of the appropriate Federal entities,
5 shall promulgate final policies and procedures relat-
6 ing to the receipt of cyber threat indicators and
7 countermeasures by the Federal Government.

8 (3) REQUIREMENTS CONCERNING POLICIES AND
9 PROCEDURES.—The policies and procedures devel-
10 oped and promulgated under this subsection shall—

11 (A) ensure that cyber threat indicators
12 shared with the Federal Government by any en-
13 tity pursuant to section 3, and that are received
14 through the process described in subsection
15 (c)—

16 (i) are shared in real time and simul-
17 taneous with such receipt with all of the
18 appropriate Federal entities;

19 (ii) are not subject to any delay, inter-
20 ference, or any other action that could im-
21 pede real-time receipt by all of the appro-
22 priate Federal entities; and

23 (iii) may be provided to other Federal
24 entities;

1 (B) ensure that cyber threat indicators
2 shared with the Federal Government by any en-
3 tity pursuant to section 3 in a manner other
4 than the process described in subsection (c)—

5 (i) are shared immediately with all of
6 the appropriate Federal entities; and

7 (ii) may be provided to other Federal
8 entities;

9 (C) govern, consistent with this Act and
10 any other applicable laws, the retention, use,
11 and dissemination by the Federal Government
12 of cyber threat indicators shared with the Fed-
13 eral Government under this Act, including the
14 extent, if any, to which such cyber threat indi-
15 cators may be used by the Federal Government
16 for authorized [*OPTION B*: “cybersecurity, for-
17 eign intelligence, counterintelligence, or law en-
18 forcement”] *OR* [*OPTION A*: “cybersecurity”]
19 purposes; and

20 (D) ensure there is an audit capability and
21 appropriate sanctions in place for officers, em-
22 ployees, or agents of a Federal entity who
23 knowingly and willfully conduct activities under
24 this Act in an unauthorized manner.

25 (b) PRIVACY AND CIVIL LIBERTIES.—

1 (1) GUIDELINES OF ATTORNEY GENERAL.—The
2 Attorney General shall, in coordination with the
3 heads of the appropriate Federal agencies and in
4 consultation with Federal privacy and civil liberties
5 officials, develop and periodically review guidelines
6 relating to privacy and civil liberties which shall gov-
7 ern the receipt, retention, use, and dissemination of
8 cyber threat indicators by a Federal entity obtained
9 in connection with activities authorized in this Act.

10 (2) CONTENT.—The guidelines developed and
11 reviewed under paragraph (1) shall, consistent with
12 the need to protect information systems from cyber-
13 security threats and mitigate cybersecurity threats—

14 (A) limit the impact on privacy and civil
15 liberties of activities by the Federal Government
16 under this Act;

17 (B) limit the receipt, retention, use and
18 dissemination of cyber threat indicators associ-
19 ated with specific persons, including estab-
20 lishing a process for the timely destruction of
21 information that is known not to be directly re-
22 lated to [*OPTION A*: “a cybersecurity threat”]
23 *OR* [*OPTION B*: “uses authorized under this
24 Act”];

1 (C) include requirements to safeguard
2 cyber threat indicators that may be used to
3 identify specific persons from unauthorized ac-
4 cess or acquisition, including appropriate sanc-
5 tions for activities by officers, employees, or
6 agents of the Federal Government in contraven-
7 tion of such guidelines;

8 (D) include procedures for notifying enti-
9 ties if information received pursuant to this sec-
10 tion is not a cyber threat indicator; and

11 (E) protect the confidentiality of cyber
12 threat indicators associated with specific per-
13 sons to the greatest extent practicable and re-
14 quire recipients to be informed that such indica-
15 tors may only be used for purposes authorized
16 under this Act.

17 (c) CAPABILITY AND PROCESS WITHIN THE DEPART-
18 MENT OF HOMELAND SECURITY.—

19 (1) IN GENERAL.—Not later than 90 days after
20 the date of the enactment of this Act, the Secretary
21 of Homeland Security, in coordination with the
22 heads of the appropriate Federal entities, shall de-
23 velop and implement a capability and process within
24 the Department of Homeland Security that—

1 (A) shall accept from any entity in real
2 time cyber threat indicators and counter-
3 measures in an electronic format, pursuant to
4 this section;

5 (B) shall, upon submittal of the certifi-
6 cation under paragraph (2) that such capability
7 and process fully and effectively operates as de-
8 scribed in such paragraph, be the process by
9 which the Federal Government receives cyber
10 threat indicators and countermeasures in an
11 electronic format that are shared by an entity
12 with the Federal Government [*OPTION C*:
13 “through a real time, automated process;”] *OR*
14 [*OPTION D*: “except—

15 (i) communications between a Federal
16 entity and a private entity regarding a pre-
17 viously shared cyber threat indicator;

18 (ii) communications regarding an
19 open Federal law enforcement **[**or national
20 security**]** investigation;

21 (iii) voluntary participation in a foren-
22 sic investigation by a Federal entity;

23 (iv) communications with a Federal
24 regulatory authority by regulated entities;
25 and

1 (v) cyber threat indicators shared with
2 a Federal entity as part of a contractual or
3 statutory requirement;”]

4 (C) ensures that all of the appropriate
5 Federal entities receive such cyber threat indi-
6 cators in real time and simultaneous with re-
7 ceipt through the process within the Depart-
8 ment of Homeland Security; and

9 (D) is in compliance with the policies, pro-
10 cedures, and guidelines required by this section.

11 (2) CERTIFICATION.—Not later than 10 days
12 prior to the implementation of the capability and
13 process required by paragraph (1), the Secretary of
14 Homeland Security shall, in consultation with the
15 heads of the appropriate Federal entities, certify to
16 Congress [*OPTION C*: “that such capability and
17 process within the Department of Homeland Secu-
18 rity does fully and effectively operate as a real time,
19 automated process by which the Federal Government
20 may receive from any entity cyber threat indicators
21 and countermeasures in an electronic format in ac-
22 cordance with the policies, procedures, and guide-
23 lines developed under this section.”] *OR* [*OPTION*
24 *D*: “whether such capability and process fully and
25 effectively operates—

1 (A) as the process by which the Federal
2 Government receives from any entity cyber
3 threat indicators and countermeasures in an
4 electronic format; and

5 (B) in accordance with the policies, proce-
6 dures, and guidelines developed under this sec-
7 tion.”]

8 (3) PUBLIC NOTICE AND ACCESS.—The Sec-
9 retary of Homeland Security shall ensure there is
10 public notice of, and access to, the capability and
11 process developed and implemented under paragraph
12 (1) so that any entity may share cyber threat indica-
13 tors and countermeasures through such process with
14 the Federal Government and that all of the appro-
15 priate Federal entities receive such cyber threat indi-
16 cators and countermeasures in real time and simul-
17 taneous with receipt through the process within the
18 Department of Homeland Security.

19 (4) OTHER FEDERAL ENTITIES.—The process
20 developed and implemented under paragraph (1)
21 shall ensure that other Federal entities receive in a
22 timely manner any cyber threat indicators and coun-
23 termeasures shared with the Federal Government
24 through the process created in this subsection.

25 (5) REPORT.—

1 (A) IN GENERAL.—Not later than 60 days
2 after the date of the enactment of this Act, the
3 Secretary of Homeland Security shall submit to
4 Congress a report on the development and im-
5 plementation of the capability and process re-
6 quired by paragraph (1), including a description
7 of such capability and process and the public
8 notice of, and access to, such process.

9 (B) CLASSIFIED ANNEX.—The report re-
10 quired by subparagraph (A) shall be submitted
11 in unclassified form, but may include a classi-
12 fied annex.

13 (d) INFORMATION SHARED WITH OR PROVIDED TO
14 THE FEDERAL GOVERNMENT.—

15 (1) NO WAIVER OF PRIVILEGE OR PROTEC-
16 TION.—The provision of cyber threat indicators and
17 countermeasures to the Federal Government under
18 this Act shall not constitute a waiver of any applica-
19 ble privilege or protection provided by law, including
20 trade secret protection.

21 (2) PROPRIETARY INFORMATION.—Cyber threat
22 indicators and countermeasures provided to the Fed-
23 eral Government under this Act shall be considered
24 the commercial, financial, and proprietary informa-

1 tion of the entity providing such information to the
2 Federal Government.

3 (3) EXEMPTION FROM DISCLOSURE.—Cyber
4 threat indicators and countermeasures provided to
5 the Federal Government under this Act shall be—

6 (A) deemed voluntarily shared information
7 and exempt from disclosure under section 552
8 of title 5, United States Code, and any State,
9 tribal, or local law requiring disclosure of infor-
10 mation or records; and

11 (B) withheld, without discretion, from the
12 public under section 552(b)(3)(B) of title 5,
13 United States Code, and any State, tribal, or
14 local provision of law requiring disclosure of in-
15 formation or records.

16 (4) EX PARTE COMMUNICATIONS.—The provi-
17 sion of cyber threat indicators and countermeasures
18 to the Federal Government under this Act shall not
19 be subject to the rules of any Federal agency or de-
20 partment or any judicial doctrine regarding ex parte
21 communications with a decisionmaking official.

22 (5) DISCLOSURE, RETENTION, AND USE.—

23 (A) AUTHORIZED ACTIVITIES.—Cyber
24 threat indicators and countermeasures provided
25 to the Federal Government under this Act may

1 be disclosed to, retained by, and used by, con-
2 sistent with otherwise applicable Federal law,
3 any Federal agency or department, component,
4 officer, employee, or agent of the Federal Gov-
5 ernment solely for—

6 (i) a cybersecurity purpose;

7 (ii) the purpose of responding to, or
8 otherwise preventing or mitigating, an im-
9 minent threat of death or serious bodily
10 harm;

11 (iii) [*OPTION B*: “the purpose of pre-
12 venting, investigating, or prosecuting a
13 cyber crime; or

14 (iv) a foreign intelligence or counter-
15 intelligence purpose.”]

16 (B) PROHIBITED ACTIVITIES.—Cyber
17 threat indicators and countermeasures provided
18 to the Federal Government under this Act shall
19 not be disclosed to, retained by, or used by any
20 Federal agency or department for any use not
21 permitted under subparagraph (A).

22 (C) PRIVACY AND CIVIL LIBERTIES.—
23 Cyber threat indicators and countermeasures
24 provided to the Federal Government under this

1 Act shall be retained, used, and disseminated by
2 the Federal Government—

3 (i) in accordance with the policies,
4 procedures, and guidelines required by sub-
5 sections (a) and (b);

6 (ii) in a manner that protects from
7 unauthorized use or disclosure any cyber
8 threat indicators that may be used to iden-
9 tify specific persons; and

10 (iii) in a manner that protects the
11 confidentiality of cyber threat indicators
12 containing information of, or that identi-
13 fies, a United States person.

14 (D) FEDERAL REGULATORY AUTHORITY.—

15 (i) IN GENERAL.—Cyber threat indi-
16 cators and countermeasures provided to
17 the Federal Government under this Act
18 may, consistent with existing Federal or
19 State regulatory authority specifically re-
20 lating to the prevention or mitigation of
21 cybersecurity threats to information sys-
22 tems, inform the development or implemen-
23 tation of regulations relating to such infor-
24 mation systems.

1 (ii) LIMITATION.—Cyber threat indi-
2 cators and countermeasures provided to
3 the Federal Government under this Act
4 shall not be directly used by any Federal,
5 State, tribal, or local government depart-
6 ment or agency to regulate the lawful ac-
7 tivities of an entity, including activities re-
8 lating to monitoring, operation of counter-
9 measures, or sharing of cyber threat indi-
10 cators.

11 (iii) EXCEPTION.—Any procedures re-
12 quired to be developed and implemented
13 under this Act shall not be considered reg-
14 ulations within the meaning of this sub-
15 paragraph.

16 **SEC. 6. PROTECTION FROM LIABILITY.**

17 (a) MONITORING OF INFORMATION SYSTEMS.—No
18 cause of action shall lie or be maintained in any court
19 against any private entity, and such action shall be
20 promptly dismissed, for the monitoring of information sys-
21 tems and information under subsection (a) of section 4
22 that is conducted in accordance with this Act.

23 (b) SHARING OR RECEIPT OF CYBER THREAT INDI-
24 CATORS.—No cause of action shall lie or be maintained
25 in any court against any entity, and such action shall be

1 promptly dismissed, for the sharing or receipt of cyber
2 threat indicators or countermeasures under subsection (c)
3 of section 4 that is conducted in accordance with this Act.

4 (c) GOOD FAITH DEFENSE IN CERTAIN CAUSES OF
5 ACTION.—If a cause of action is not otherwise dismissed
6 or precluded under subsection (a) or (b), a good faith reli-
7 ance by an entity that the conduct complained of was per-
8 mitted under this Act shall be a complete defense against
9 any action brought in any court against such entity.

10 (d) CONSTRUCTION.—Nothing in this section shall be
11 construed to require dismissal of a cause of action against
12 an entity that has engaged in—

13 (1) gross negligence or wilful misconduct in the
14 course of conducting activities authorized by this
15 Act; or

16 (2) conduct that is otherwise not in compliance
17 with the requirements of this Act.

18 **SEC. 7. OVERSIGHT OF GOVERNMENT ACTIVITIES.**

19 (a) BIENNIAL REPORT ON IMPLEMENTATION.—

20 (1) IN GENERAL.—Not later than 2 years after
21 the date of the enactment of this Act, and not less
22 frequently than once every 2 years thereafter, the
23 heads of the appropriate Federal entities shall joint-
24 ly submit to Congress a detailed report concerning
25 the implementation of this Act.

1 (2) CONTENTS.—Each report submitted under
2 paragraph (1) shall include the following:

3 (A) An assessment of the sufficiency of the
4 policies, procedures, and guidelines required by
5 section 5 in ensuring that cyber threat indica-
6 tors are shared effectively and responsibly with-
7 in the Federal Government.

8 (B) An evaluation of the effectiveness of
9 real-time information sharing through the capa-
10 bility and process developed under section 5(c),
11 including any impediments to such real-time
12 sharing.

13 (C) An assessment of the sufficiency of the
14 procedures developed under section 3 in ensur-
15 ing that cyber threat indicators in the posses-
16 sion of the Federal Government are shared in
17 a timely and adequate manner with appropriate
18 entities, or, if appropriate, are made publicly
19 available.

20 (D) An assessment of whether cyber threat
21 indicators have been properly classified and an
22 accounting of the number of security clearances
23 authorized by the Federal Government for the
24 purposes of this Act.

1 (E) A review of the type of cyber threat in-
2 dicators shared with the Federal Government
3 under this Act, including—

4 (i) the degree to which such informa-
5 tion may impact the privacy and civil lib-
6 erties of United States persons;

7 (ii) a quantitative and qualitative as-
8 sessment of the impact of the sharing of
9 such cyber threat indicators with the Fed-
10 eral Government on privacy and civil lib-
11 erties of United States persons; and

12 (iii) the adequacy of any steps taken
13 by the Federal Government to reduce such
14 impact.

15 (F) A review of actions taken by the Fed-
16 eral Government based on cyber threat indica-
17 tors shared with the Federal Government under
18 this Act, including the appropriateness of any
19 subsequent use or dissemination of such cyber
20 threat indicators by a Federal entity under sec-
21 tion 5.

22 (G) A description of any violations of the
23 requirements of this Act by the Federal Govern-
24 ment.

1 (H) A classified list of entities that re-
2 ceived classified cyber threat indicators from
3 the Federal Government under this Act and an
4 evaluation of the risks and benefits of sharing
5 such cyber threat indicators.

6 (3) RECOMMENDATIONS.—Each report sub-
7 mitted under paragraph (1) may include such rec-
8 ommendations as the heads of the appropriate Fed-
9 eral entities may have for improvements or modifica-
10 tions to the authorities and processes under this Act.

11 (4) FORM OF REPORT.—Each report required
12 by paragraph (1) shall be submitted in unclassified
13 form, but shall include a classified annex.

14 (b) REPORTS ON PRIVACY AND CIVIL LIBERTIES.—

15 (1) BIENNIAL REPORT FROM PRIVACY AND
16 CIVIL LIBERTIES OVERSIGHT BOARD.—Not later
17 than 1 year after the date of the enactment of this
18 Act and not less frequently than once every 2 years
19 thereafter, the Privacy and Civil Liberties Oversight
20 Board shall submit to Congress and the President a
21 report providing—

22 (A) an assessment of the privacy and civil
23 liberties impact of the type of activities carried
24 out under this Act; and

1 (B) an assessment of the sufficiency of the
2 policies, procedures, and guidelines established
3 pursuant to section 5 in addressing privacy and
4 civil liberties concerns.

5 (2) BIENNIAL REPORT OF INSPECTORS GEN-
6 ERAL.—

7 (A) IN GENERAL.—Not later than 2 years
8 after the date of the enactment of this Act and
9 not less frequently than once every 2 years
10 thereafter, the Inspector General of the Depart-
11 ment of Homeland Security, the Inspector Gen-
12 eral of the Intelligence Community, the Inspec-
13 tor General of the Department of Justice, and
14 the Inspector General of the Department of De-
15 fense shall jointly submit to Congress a report
16 on the receipt, use, and dissemination of cyber
17 threat indicators and countermeasures that
18 have been shared with Federal entities under
19 this Act.

20 (B) CONTENTS.—Each report submitted
21 under subparagraph (A) shall include the fol-
22 lowing:

23 (i) A review of the types of cyber
24 threat indicators shared with Federal enti-
25 ties.

1 (ii) A review of the actions taken by
2 Federal entities as a result of the receipt
3 of such cyber threat indicators.

4 (iii) A list of Federal entities receiving
5 such cyber threat indicators.

6 (iv) A review of the sharing of such
7 cyber threat indicators among Federal en-
8 tities to identify inappropriate barriers to
9 sharing information.

10 (3) RECOMMENDATIONS.—Each report sub-
11 mitted under this subsection may include such rec-
12 ommendations as the Privacy and Civil Liberties
13 Oversight Board, with respect to a report submitted
14 under paragraph (1), or the Inspectors General re-
15 ferred to in paragraph (2)(A), with respect to a re-
16 port submitted under paragraph (2), may have for
17 improvements or modifications to the authorities
18 under this Act.

19 (4) FORM.—Each report required under this
20 subsection shall be submitted in unclassified form,
21 but may include a classified annex.

22 **SEC. 8. CONSTRUCTION AND PREEMPTION.**

23 (a) OTHERWISE LAWFUL DISCLOSURES.—Nothing in
24 this Act shall be construed to limit or prohibit otherwise
25 lawful disclosures of communications, records, or other in-

1 formation by an entity to any other entity or the Federal
2 Government under this Act.

3 (b) WHISTLEBLOWER PROTECTIONS.—Nothing in
4 this Act shall be construed to preempt any employee from
5 exercising rights currently provided under any whistle-
6 blower law, rule, or regulation.

7 (c) PROTECTION OF SOURCES AND METHODS.—
8 Nothing in this Act shall be construed—

9 (1) as creating any immunity against, or other-
10 wise affecting, any action brought by the Federal
11 Government, or any agency or department thereof,
12 to enforce any law, executive order, or procedure
13 governing the appropriate handling, disclosure, or
14 use of classified information;

15 (2) to impact the conduct of authorized law en-
16 forcement or intelligence activities; or

17 (3) to modify the authority of a department or
18 agency of the Federal Government to protect sources
19 and methods and the national security of the United
20 States.

21 (d) RELATIONSHIP TO OTHER LAWS.—Nothing in
22 this Act shall be construed to affect any requirement
23 under any other provision of law for an entity to provide
24 information to the Federal Government.

1 (e) PROHIBITED CONDUCT.—Nothing in this Act
2 shall be construed to permit price-fixing, allocating a mar-
3 ket between competitors, monopolizing or attempting to
4 monopolize a market, boycotting, or exchanges of price or
5 cost information, customer lists, or information regarding
6 future competitive planning.

7 (f) INFORMATION SHARING RELATIONSHIPS.—Noth-
8 ing in this Act shall be construed—

9 (1) to limit or modify an existing information
10 sharing relationship;

11 (2) to prohibit a new information sharing rela-
12 tionship;

13 (3) to require a new information sharing rela-
14 tionship between any entity and the Federal Govern-
15 ment;

16 (4) to require the use of the capability and
17 process within the Department of Homeland Secu-
18 rity developed under section 5(c); or

19 (5) to amend, repeal, or supersede a contractual
20 agreement or relationship between any entities, or
21 between any entity and the Federal Government.

22 (g) ANTI-TASKING RESTRICTION.—Nothing in this
23 Act shall be construed to permit the Federal Govern-
24 ment—

1 (1) to require an entity to provide information
2 to the Federal Government; or

3 (2) to condition the sharing of cyber threat in-
4 dicators with an entity on such entity's provision of
5 cyber threat indicators to the Federal Government.

6 (h) NO LIABILITY FOR NON-PARTICIPATION.—Noth-
7 ing in this Act shall be construed to subject any entity
8 to liability for choosing not to engage in the voluntary ac-
9 tivities authorized in this Act.

10 (i) USE AND RETENTION OF INFORMATION.—Noth-
11 ing in this Act shall be construed to authorize, or to mod-
12 ify any existing authority of, a department or agency of
13 the Federal Government to retain or use any information
14 shared under this Act for any use other than permitted
15 in this Act.

16 (j) FEDERAL PREEMPTION.—

17 (1) IN GENERAL.—This Act supersedes any
18 statute or other law of a State or political subdivi-
19 sion of a State that restricts or otherwise expressly
20 regulates an activity authorized under this Act.

21 (2) STATE LAW ENFORCEMENT.—Nothing in
22 this Act shall be construed to supersede any statute
23 or other law of a State or political subdivision of a
24 State concerning the use of authorized law enforce-
25 ment practices and procedures.

1 **SEC. 9. CONFORMING AMENDMENTS.**

2 Section 552(b) of title 5, United States Code, is
3 amended—

4 (1) in paragraph (8), by striking “or” at the
5 end;

6 (2) in paragraph (9), by striking “wells.” and
7 inserting “wells; or”; and

8 (3) by adding at the end the following:

9 “(10) information shared with or provided to
10 the Federal Government pursuant to the Cybersecu-
11 rity Information Sharing Act of 2014.”.