

113TH CONGRESS
2D SESSION

S. _____

To improve cybersecurity in the United States through enhanced sharing
of information about cybersecurity threats, 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 improve cybersecurity in the United States through en-
hanced sharing of information about cybersecurity
threats, 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, detecting, analyzing, and mitigating cy-
bersecurity 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.

22 (C) The Department of Energy.

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

3 (E) The Department of Justice.

4 (F) The Department of the Treasury.

5 (G) 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 an action, device, procedure, tech-
13 nique, or other measure applied to an information
14 system or information that is stored on, processed
15 by, or transiting an information system that pre-
16 vents or mitigates a cybersecurity threat or security
17 vulnerability.

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

24 (7) CYBERSECURITY THREAT.—The term “cy-
25 bersecurity threat” means an action, not protected

1 by the First Amendment to the Constitution of the
2 United States, on or through an information system
3 that may result in an unauthorized effort to ad-
4 versely impact the security, availability, confiden-
5 tiality, or integrity of an information system or in-
6 formation that is stored on, processed by, or
7 transiting an information system.

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

11 (A) malicious reconnaissance, including
12 anomalous patterns of communications that ap-
13 pear to be transmitted for the purpose of gath-
14 ering technical information related to a cyberse-
15 curity threat or security vulnerability;

16 (B) a method of defeating a security con-
17 trol or exploitation of a security vulnerability;

18 (C) a security vulnerability;

19 (D) a method of causing a user with legiti-
20 mate access to an information system or infor-
21 mation that is stored on, processed by, or
22 transiting an information system to unwittingly
23 enable the defeat of a security control or exploi-
24 tation of a security vulnerability;

25 (E) malicious cyber command and control;

1 (F) the actual or potential harm caused by
2 an incident, including information exfiltrated
3 when it is necessary in order to describe a cy-
4 bersecurity threat;

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

8 (H) any combination thereof.

9 (9) ELECTRONIC FORMAT.—

10 (A) IN GENERAL.—Except as provided in
11 subparagraph (B), the term “electronic format”
12 means information that is shared through elec-
13 tronic mail, an interactive form on an Internet
14 website, or a real time, automated process be-
15 tween information systems.

16 (B) EXCLUSION.—The term “electronic
17 format” does not include voice or video commu-
18 nication.

19 (10) ENTITY.—

20 (A) IN GENERAL.—The term “entity”
21 means any private entity, non-Federal govern-
22 ment agency or department, or State, tribal, or
23 local government agency or department (includ-
24 ing a political subdivision, officer, employee, or
25 agent thereof).

1 (B) INCLUSIONS.—The term “entity” in-
2 cludes a government agency or department (in-
3 cluding an officer, employee, or agent thereof)
4 of the District of Columbia, the Commonwealth
5 of Puerto Rico, the Virgin Islands, Guam,
6 American Samoa, the Northern Mariana Is-
7 lands, and any other territory or possession of
8 the United States.

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

13 (11) FEDERAL ENTITY.—The term “Federal
14 entity” means a department or agency of the United
15 States, or any component, officer, employee, or
16 agent of such a department or agency.

17 (12) FOREIGN INTELLIGENCE.—The term “for-
18 eign intelligence” has the meaning given the term in
19 section (3) of the National Security Act of 1947 (50
20 U.S.C. 3003).

21 (13) INFORMATION SYSTEM.—The term “infor-
22 mation system”—

23 (A) has the meaning given the term in sec-
24 tion 3502 of title 44, United States Code; and

1 (B) includes industrial control systems,
2 such as supervisory control and data acquisition
3 systems, distributed control systems, and pro-
4 grammable logic controllers.

5 (14) LOCAL GOVERNMENT.—The term “local
6 government” means any borough, city, county, par-
7 ish, town, township, village, or other political sub-
8 division of a State.

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

15 (16) MALICIOUS RECONNAISSANCE.—The term
16 “malicious reconnaissance” means a method for ac-
17 tively probing or passively monitoring an information
18 system for the purpose of discerning security
19 vulnerabilities of the information system, if such
20 method is associated with a known or suspected cy-
21 bersecurity threat.

22 (17) MONITOR.—The term “monitor” means to
23 obtain, identify, or otherwise possess information
24 that is stored on, processed by, or transiting an in-
25 formation system.

1 (18) PRIVATE ENTITY.—

2 (A) IN GENERAL.—The term “private enti-
3 ty” means any individual or private group, or-
4 ganization, proprietorship, partnership, trust,
5 cooperative, corporation, or other commercial or
6 nonprofit entity, including an officer, employee,
7 or agent thereof.

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

12 (19) SECURITY CONTROL.—The term “security
13 control” means the management, operational, and
14 technical controls used to protect the confidentiality,
15 integrity, and availability of an information system
16 or its information.

17 (20) SECURITY VULNERABILITY.—The term
18 “security vulnerability” means any attribute of hard-
19 ware, software, process, or procedure that could en-
20 able or facilitate the defeat of a security control.

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

1 (22) UNITED STATES PERSON.—The term
2 “United States person” has the meaning given the
3 term in section 101(i) of the Foreign Intelligence
4 Surveillance Act of 1978 (50 U.S.C. 1801).

5 **SEC. 3. SHARING OF INFORMATION BY THE FEDERAL GOV-**
6 **ERNMENT.**

7 (a) IN GENERAL.—Consistent with the protection of
8 intelligence sources and methods and the protection of pri-
9 vacy and civil liberties, the Director of National Intel-
10 ligence, the Secretary of Homeland Security, the Secretary
11 of Defense, and the Attorney General, in consultation with
12 the heads of the appropriate Federal agencies, shall de-
13 velop and promulgate procedures to facilitate and pro-
14 mote—

15 (1) the timely sharing of classified cyber threat
16 indicators in the possession of the Federal Govern-
17 ment with cleared representatives of appropriate en-
18 tities;

19 (2) the timely sharing with appropriate entities
20 of cyber threat indicators or information in the pos-
21 session of the Federal Government that may be de-
22 classified and shared at an unclassified level; and

23 (3) the sharing with appropriate entities, or, if
24 appropriate, public availability, of unclassified, in-

1 including controlled unclassified, cyber threat indica-
2 tors in the possession of the Federal Government.

3 (b) DEVELOPMENT OF PROCEDURES.—

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

6 (A) ensure the Federal Government has
7 and maintains the capability to share cyber
8 threat indicators in real time consistent with
9 the protection of classified information; and

10 (B) incorporate, to the greatest extent pos-
11 sible, existing processes and existing roles and
12 responsibilities of Federal and non-Federal enti-
13 ties for information sharing by the Federal
14 Government, including sector specific informa-
15 tion sharing and analysis centers.

16 (2) COORDINATION.—In developing the proce-
17 dures required under this section, the Director of
18 National Intelligence, the Secretary of Homeland Se-
19 curity, and the Attorney General shall coordinate
20 with appropriate Federal entities to ensure that ef-
21 fective protocols are implemented that will facilitate
22 and promote the sharing of cyber threat indicators
23 by the Federal Government in a timely manner.

24 (c) SUBMITTAL TO CONGRESS.—Not later than 60
25 days after the date of the enactment of this Act, the Direc-

1 tor of National Intelligence, in consultation with the heads
2 of the appropriate Federal entities, shall submit to Con-
3 gress the procedures required by subsection (a).

4 **SEC. 4. AUTHORIZATIONS FOR PREVENTING, DETECTING,**
5 **ANALYZING, AND MITIGATING CYBERSECU-**
6 **RITY THREATS.**

7 (a) AUTHORIZATION FOR MONITORING.—

8 (1) IN GENERAL.—Notwithstanding any other
9 provision of law, a private entity may, for cybersecu-
10 rity purposes, monitor—

11 (A) the information systems of such pri-
12 vate entity;

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

15 (C) the information systems of a Federal
16 entity, upon written consent of an authorized
17 representative of the Federal entity; and

18 (D) information that is stored on, proc-
19 essed by, or transiting the information systems
20 monitored by the private entity under this para-
21 graph.

22 (2) CONSTRUCTION.—Nothing in this sub-
23 section shall be construed to authorize the moni-
24 toring of information systems other than as provided
25 in this subsection.

1 (b) AUTHORIZATION FOR OPERATION OF COUNTER-
2 MEASURES.—

3 (1) IN GENERAL.—Notwithstanding any other
4 provision of law, a private entity may, for cybersecu-
5 rity purposes, operate countermeasures that are ap-
6 plied to—

7 (A) the information systems of such pri-
8 vate entity in order to protect the rights or
9 property of the private entity;

10 (B) the information systems of another en-
11 tity upon written consent of such entity to pro-
12 tect the rights or property of such entity; and

13 (C) the information systems of a Federal
14 entity upon written consent of an authorized
15 representative of such Federal entity to protect
16 the rights or property of the Federal Govern-
17 ment.

18 (2) CONSTRUCTION.—Nothing in this sub-
19 section shall be construed to authorize the use of
20 countermeasures other than as provided in this sub-
21 section.

22 (c) AUTHORIZATION FOR SHARING OR RECEIVING
23 CYBER THREAT INDICATORS OR COUNTERMEASURES.—

24 (1) IN GENERAL.—Notwithstanding any other
25 provision of law, and for the purposes permitted

1 under this Act, an entity may, consistent with the
2 protection of classified information, share with, or
3 receive from, any other entity or the Federal Gov-
4 ernment cyber threat indicators and counter-
5 measures.

6 (2) CONSTRUCTION.—Nothing in this sub-
7 section shall be construed to authorize the sharing
8 or receiving of cyber threat indicators or counter-
9 measures, other than as provided in this subsection.

10 (d) PROTECTION AND USE OF INFORMATION.—

11 (1) SECURITY OF INFORMATION.—An entity
12 monitoring information systems, operating counter-
13 measures, or providing or receiving cyber threat in-
14 dicators or countermeasures under this section shall
15 implement and utilize security controls to protect
16 against unauthorized access to or acquisition of such
17 cyber threat indicators or countermeasures.

18 (2) REMOVAL OF CERTAIN PERSONAL INFORMA-
19 TION.—An entity sharing cyber threat indicators
20 pursuant to this Act shall, prior to such sharing, re-
21 move any information contained within such indica-
22 tors that is known to be personal information of or
23 identifying a United States person, not directly re-
24 lated to a cybersecurity threat in order to ensure
25 that such information is protected from unauthor-

1 ized disclosure to any other entity or the Federal
2 Government.

3 (3) USE OF CYBER THREAT INDICATORS AND
4 COUNTERMEASURES BY ENTITIES.—

5 (A) IN GENERAL.—Consistent with this
6 Act, cyber threat indicators or countermeasures
7 shared or received under this section may, for
8 cybersecurity purposes—

9 (i) be used by an entity to monitor or
10 operate countermeasures on its information
11 systems, or the information systems of an-
12 other entity or a Federal entity upon the
13 written consent of that other entity or that
14 Federal entity; and

15 (ii) be otherwise used, retained, and
16 further shared by an entity.

17 (B) CONSTRUCTION.—Nothing in this
18 paragraph shall be construed to authorize the
19 use of cyber threat indicators or counter-
20 measures other than as provided in this section.

21 (4) USE OF CYBER THREAT INDICATORS BY
22 STATE, TRIBAL, OR LOCAL DEPARTMENTS OR AGEN-
23 CIES.—

24 (A) LAW ENFORCEMENT USE.—

1 (i) PRIOR WRITTEN CONSENT.—Ex-
2 cept as provided in clause (ii), cyber threat
3 indicators shared with a State, tribal, or
4 local department or agency under this sec-
5 tion may, with the prior written consent of
6 the entity sharing such indicators, be used
7 by a State, tribal, or local department or
8 agency for the purpose of preventing, in-
9 vestigating, or prosecuting a criminal act.

10 (ii) ORAL CONSENT.—If the need for
11 immediate use prevents obtaining written
12 consent, such consent may be provided
13 orally with subsequent documentation of
14 the consent.

15 (B) EXEMPTION FROM DISCLOSURE.—
16 Cyber threat indicators shared with a State,
17 tribal, or local department or agency under this
18 section shall be—

19 (i) deemed voluntarily shared informa-
20 tion; and

21 (ii) exempt from disclosure under any
22 State, tribal, or local law requiring disclo-
23 sure of information or records.

24 (C) STATE, TRIBAL, AND LOCAL REGU-
25 LATORY AUTHORITY.—

1 (i) AUTHORIZATION.—Cyber threat
2 indicators shared with a State, tribal, or
3 local department or agency under this sec-
4 tion may, consistent with State regulatory
5 authority specifically relating to the pre-
6 vention or mitigation of cybersecurity
7 threats to information systems, inform the
8 development or implementation of regula-
9 tions relating to such information systems.

10 (ii) LIMITATION.—Such cyber threat
11 indicators shall not otherwise be directly
12 used by any State, tribal, or local depart-
13 ment or agency to regulate the lawful ac-
14 tivities of an entity.

15 (e) ANTITRUST EXEMPTION.—

16 (1) IN GENERAL.—Except as provided in sec-
17 tion 8(e), it shall not be considered a violation of
18 any provision of antitrust laws for two or more pri-
19 vate entities to exchange or provide cyber threat in-
20 dicators, or assistance relating to the prevention, in-
21 vestigation, or mitigation of cybersecurity threats,
22 for cybersecurity purposes under this Act.

23 (2) APPLICABILITY.—Paragraph (1) shall apply
24 only to information that is exchanged or assistance
25 provided in order to assist with—

1 (A) facilitating the prevention, investiga-
2 tion, or mitigation of cybersecurity threats to
3 information systems or information that is
4 stored on, processed by, or transiting an infor-
5 mation system; or

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

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

16 **SEC. 5. SHARING OF CYBER THREAT INDICATORS AND**
17 **COUNTERMEASURES WITH THE FEDERAL**
18 **GOVERNMENT.**

19 (a) REQUIREMENT FOR POLICIES AND PROCE-
20 DURES.—

21 (1) INTERIM POLICIES AND PROCEDURES.—Not
22 later than 60 days after the date of the enactment
23 of this Act, the Attorney General, in coordination
24 with the heads of the appropriate Federal entities,
25 shall develop, and submit to Congress, interim poli-

1 cies and procedures relating to the receipt of cyber
2 threat indicators and countermeasures by the Fed-
3 eral Government.

4 (2) FINAL POLICIES AND PROCEDURES.—Not
5 later than 180 days after the date of the enactment
6 of this Act, the Attorney General, in coordination
7 with the heads of the appropriate Federal entities,
8 shall promulgate final policies and procedures relat-
9 ing to the receipt of cyber threat indicators and
10 countermeasures by the Federal Government.

11 (3) REQUIREMENTS CONCERNING POLICIES AND
12 PROCEDURES.—The policies and procedures devel-
13 oped and promulgated under this subsection shall—

14 (A) ensure that cyber threat indicators
15 shared with the Federal Government by any en-
16 tity pursuant to section 4, and that are received
17 through the process described in subsection
18 (c)—

19 (i) are shared in real time and simul-
20 taneous with such receipt with all of the
21 appropriate Federal entities;

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

1 (iii) may be provided to other Federal
2 entities;

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

7 (i) are shared immediately with all of
8 the appropriate Federal entities;

9 (ii) are not subject to any unreason-
10 able delay, interference, or any other ac-
11 tion that could impede receipt by all of the
12 appropriate Federal entities; and

13 (iii) may be provided to other Federal
14 entities;

15 (C) govern, consistent with this Act and
16 any other applicable laws, the retention, use,
17 and dissemination by the Federal Government
18 of cyber threat indicators shared with the Fed-
19 eral Government under this Act, including the
20 extent, if any, to which such cyber threat indi-
21 cators may be used by the Federal Government;
22 and

23 (D) ensure there is an audit capability and
24 appropriate sanctions in place for officers, em-
25 ployees, or agents of a Federal entity who

1 knowingly and willfully conduct activities under
2 this Act in an unauthorized manner.

3 (b) PRIVACY AND CIVIL LIBERTIES.—

4 (1) GUIDELINES OF ATTORNEY GENERAL.—The
5 Attorney General shall, in coordination with the
6 heads of the appropriate Federal agencies and in
7 consultation with officers designated under section
8 1062 of the National Security Intelligence Reform
9 Act of 2004 (42 U.S.C. 2000ee-1), develop and peri-
10 odically review guidelines relating to privacy and
11 civil liberties which shall govern the receipt, reten-
12 tion, use, and dissemination of cyber threat indica-
13 tors by a Federal entity obtained in connection with
14 activities authorized in this Act.

15 (2) CONTENT.—The guidelines developed and
16 reviewed under paragraph (1) shall, consistent with
17 the need to protect information systems from cyber-
18 security threats and mitigate cybersecurity threats—

19 (A) limit the impact on privacy and civil
20 liberties of activities by the Federal Government
21 under this Act;

22 (B) limit the receipt, retention, use and
23 dissemination of cyber threat indicators associ-
24 ated with specific persons, including estab-
25 lishing a process for the timely destruction of

1 information that is known not to be directly re-
2 lated to uses authorized under this Act;

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

10 (D) include procedures for notifying enti-
11 ties if information received pursuant to this sec-
12 tion is known by a Federal entity receiving the
13 information not to constitute a cyber threat in-
14 dicator; and

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

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

23 (1) IN GENERAL.—Not later than 90 days after
24 the date of the enactment of this Act, the Secretary
25 of Homeland Security, in coordination with the

1 heads of the appropriate Federal entities, shall de-
2 velop and implement a capability and process within
3 the Department of Homeland Security that—

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

8 (B) shall, upon submittal of the certifi-
9 cation under paragraph (2) that such capability
10 and process fully and effectively operates as de-
11 scribed in such paragraph, be the process by
12 which the Federal Government receives cyber
13 threat indicators and countermeasures under
14 this Act in an electronic format that are shared
15 by an entity with the Federal Government ex-
16 cept—

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

20 (ii) voluntary or legally compelled par-
21 ticipation in an open Federal investigation;

22 (iii) communications with a Federal
23 regulatory authority by regulated entities
24 regarding a cybersecurity threat; and

1 (iv) cyber threat indicators or counter-
2 measures shared with a Federal entity as
3 part of a contractual or statutory require-
4 ment;

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

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

12 (2) CERTIFICATION.—Not later than 10 days
13 prior to the implementation of the capability and
14 process required by paragraph (1), the Secretary of
15 Homeland Security shall, in consultation with the
16 heads of the appropriate Federal entities, certify to
17 Congress whether such capability and process fully
18 and effectively operates—

19 (A) as the process by which the Federal
20 Government receives from any entity cyber
21 threat indicators and countermeasures in an
22 electronic format under this Act; and

23 (B) in accordance with the policies, proce-
24 dures, and guidelines developed under this sec-
25 tion.

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

12 (4) OTHER FEDERAL ENTITIES.—The process
13 developed and implemented under paragraph (1)
14 shall ensure that other Federal entities receive in a
15 timely manner any cyber threat indicators and coun-
16 termeasures shared with the Federal Government
17 through the process created in this subsection.

18 (5) REPORT.—

19 (A) IN GENERAL.—Not later than 60 days
20 after the date of the enactment of this Act, the
21 Secretary of Homeland Security shall submit to
22 Congress a report on the development and im-
23 plementation of the capability and process re-
24 quired by paragraph (1), including a description

1 of such capability and process and the public
2 notice of, and access to, such process.

3 (B) CLASSIFIED ANNEX.—The report re-
4 quired by subparagraph (A) shall be submitted
5 in unclassified form, but may include a classi-
6 fied annex.

7 (d) INFORMATION SHARED WITH OR PROVIDED TO
8 THE FEDERAL GOVERNMENT.—

9 (1) NO WAIVER OF PRIVILEGE OR PROTEC-
10 TION.—The provision of cyber threat indicators and
11 countermeasures to the Federal Government under
12 this Act shall not constitute a waiver of any applica-
13 ble privilege or protection provided by law, including
14 trade secret protection.

15 (2) PROPRIETARY INFORMATION.—A cyber
16 threat indicator or countermeasure provided by an
17 entity to the Federal Government under this Act
18 shall be considered the commercial, financial, and
19 proprietary information of such entity when so des-
20 ignated by such entity.

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

24 (A) deemed voluntarily shared information
25 and exempt from disclosure under section 552

1 of title 5, United States Code, and any State,
2 tribal, or local law requiring disclosure of infor-
3 mation or records; and

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

9 (4) EX PARTE COMMUNICATIONS.—The provi-
10 sion of cyber threat indicators and countermeasures
11 to the Federal Government under this Act shall not
12 be subject to the rules of any Federal agency or de-
13 partment or any judicial doctrine regarding ex parte
14 communications with a decisionmaking official.

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

16 (A) AUTHORIZED ACTIVITIES.—Cyber
17 threat indicators and countermeasures provided
18 to the Federal Government under this Act may
19 be disclosed to, retained by, and used by, con-
20 sistent with otherwise applicable Federal law,
21 any Federal agency or department, component,
22 officer, employee, or agent of the Federal Gov-
23 ernment solely for—

24 (i) a cybersecurity purpose;

1 (ii) the purpose of responding to, or
2 otherwise preventing or mitigating, an im-
3 minent threat of death or serious bodily
4 harm; or

5 (iii) the purpose of preventing, inves-
6 tigating, or prosecuting any of the offenses
7 listed in sections 1028 through 1030 of
8 title 18, United States Code, and chapters
9 37 and 90 of such title.

10 (B) PROHIBITED ACTIVITIES.—Cyber
11 threat indicators and countermeasures provided
12 to the Federal Government under this Act shall
13 not be disclosed to, retained by, or used by any
14 Federal agency or department for any use not
15 permitted under subparagraph (A).

16 (C) PRIVACY AND CIVIL LIBERTIES.—
17 Cyber threat indicators and countermeasures
18 provided to the Federal Government under this
19 Act shall be retained, used, and disseminated by
20 the Federal Government—

21 (i) in accordance with the policies,
22 procedures, and guidelines required by sub-
23 sections (a) and (b);

24 (ii) in a manner that protects from
25 unauthorized use or disclosure any cyber

1 threat indicators that may be used to iden-
2 tify specific persons; and

3 (iii) in a manner that protects the
4 confidentiality of cyber threat indicators
5 containing information of, or that identi-
6 fies, a United States person.

7 (D) FEDERAL REGULATORY AUTHORITY.—

8 (i) IN GENERAL.—Cyber threat indi-
9 cators and countermeasures provided to
10 the Federal Government under this Act
11 may, consistent with Federal or State reg-
12 ulatory authority specifically relating to
13 the prevention or mitigation of cybersecu-
14 rity threats to information systems, inform
15 the development or implementation of reg-
16 ulations relating to such information sys-
17 tems.

18 (ii) LIMITATION.—Cyber threat indi-
19 cators and countermeasures provided to
20 the Federal Government under this Act
21 shall not be directly used by any Federal,
22 State, tribal, or local government depart-
23 ment or agency to regulate the lawful ac-
24 tivities of an entity, including activities re-
25 lating to monitoring, operation of counter-

1 measures, or sharing of cyber threat indi-
2 cators.

3 (iii) EXCEPTION.—Procedures devel-
4 oped and implemented under this Act shall
5 not be considered regulations within the
6 meaning of this subparagraph.

7 **SEC. 6. PROTECTION FROM LIABILITY.**

8 (a) MONITORING OF INFORMATION SYSTEMS.—No
9 cause of action shall lie or be maintained in any court
10 against any private entity, and such action shall be
11 promptly dismissed, for the monitoring of information sys-
12 tems and information under subsection (a) of section 4
13 that is conducted in accordance with this Act.

14 (b) SHARING OR RECEIPT OF CYBER THREAT INDI-
15 CATORS.—No cause of action shall lie or be maintained
16 in any court against any entity, and such action shall be
17 promptly dismissed, for the sharing or receipt of cyber
18 threat indicators or countermeasures under subsection (c)
19 of section 4 if—

20 (1) such sharing or receipt is conducted in ac-
21 cordance with this Act; and

22 (2) in a case in which a cyber threat indicator
23 or countermeasure is shared with the Federal Gov-
24 ernment in an electronic format, the cyber threat in-

1 dicator or countermeasure is shared in a manner
2 that is consistent with section 5(c).

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

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

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

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

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

18 (a) BIENNIAL REPORT ON IMPLEMENTATION.—

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

1 (H) A classified summary of the number
2 and type of entities that received classified
3 cyber threat indicators from the Federal Gov-
4 ernment under this Act and an evaluation of
5 the risks and benefits of sharing such cyber
6 threat indicators.

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

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

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

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

23 (A) an assessment of the privacy and civil
24 liberties impact of the type of activities carried
25 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 any current
20 or future contractual agreement, terms of service
21 agreement, or other contractual relationship between
22 any entities, or between any entity and the Federal
23 Government.

1 (g) ANTI-TASKING RESTRICTION.—Nothing in this
2 Act shall be construed to permit the Federal Govern-
3 ment—

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

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

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

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

19 (j) FEDERAL PREEMPTION.—

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

24 (2) STATE LAW ENFORCEMENT.—Nothing in
25 this Act shall be construed to supersede any statute

1 or other law of a State or political subdivision of a
2 State concerning the use of authorized law enforce-
3 ment practices and procedures.

4 (k) REGULATORY AUTHORITY.—Nothing in this Act
5 shall be construed—

6 (1) to authorize the promulgation of any regu-
7 lations not specifically authorized by this Act;

8 (2) to establish any regulatory authority not
9 specifically established under Act; or

10 (3) to authorize regulatory actions that would
11 duplicate or conflict with regulatory requirements,
12 mandatory standards, or related processes that were
13 in effect on the day before the date of the enactment
14 of this Act.

15 **SEC. 9. CONFORMING AMENDMENTS.**

16 Section 552(b) of title 5, United States Code, is
17 amended—

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

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

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

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