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.

Be it enacted by the Senate and House of Representa-

tives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

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

(b) TABLE OF CONTENTS.—The table of contents of 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.

SEC. 2. DEFINITIONS.

In this Act:

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

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

(A) has the meaning given the term in section 1(a) of the Clayton Act (15 U.S.C. 12(a));

(B) includes section 5 of the Federal Trade Commission Act (15 U.S.C. 45) to the extent that section 5 of that Act applies to unfair methods of competition; and

(C) includes any State law that has the same intent and effect as the laws under subparagraphs (A) and (B).

(3) APPROPRIATE FEDERAL ENTITIES.—The term “appropriate Federal entities” means the following:

(A) The Department of Commerce.

(B) The Department of Defense.
(C) The Department of Energy.

(D) The Department of Homeland Security.

(E) The Department of Justice.

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

(4) COUNTERINTELLIGENCE.—The term “counterintelligence” has the meaning given the term in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).

(5) COUNTERMEASURE.—The term “countermeasure” means any action, device, procedure, technique, or other measure that meets or counters a threat, vulnerability, or attack by eliminating or preventing it, or by minimizing the harm it may cause.

(6) CYBERSECURITY PURPOSE.—The term “cybersecurity purpose” means the purpose of protecting an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability.

(7) CYBERSECURITY THREAT.—The term “cybersecurity threat” means any action that may result in an unauthorized effort, not protected by the First Amendment to the Constitution of the United
States, to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system.

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

(A) malicious reconnaissance, including anomalous patterns of communications that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat;

(B) a method of defeating a security control;

(C) a security vulnerability;

(D) a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to unwittingly enable the defeat of a security control;

(E) malicious cyber command and control;

(F) the actual or potential harm caused by an incident, including information exfiltrated when it is necessary in order to describe a cybersecurity threat;
(G) any other attribute of a cybersecurity threat, if disclosure of such attribute is not otherwise prohibited by law; or

(H) any combination thereof.

(9) ENTITY.—

(A) IN GENERAL.—The term “entity” means any private entity, non-Federal government agency or department, or State, tribal, or local government agency or department (including an officer, employee, or agent thereof).

(B) INCLUSIONS.—The term “entity” includes a government agency or department (including an officer, employee, or agent thereof) of the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Northern Mariana Islands, and any other territory or possession of the United States.

(C) EXCLUSION.—The term “entity” does not include a foreign power as defined in section 101(a) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

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

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

(12) INFORMATION SYSTEM.—The term “information system” has the meaning given the term in section 3502 of title 44, United States Code.

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

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

(15) MALICIOUS RECONNAISSANCE.—The term “malicious reconnaissance” means a method for actively probing or passively monitoring an information system for the purpose of discerning security vulnerabilities of the information system, if such
method is associated with a known or suspected cybersecurity threat.

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

(17) PRIVATE ENTITY.—

(A) IN GENERAL.—The term “private entity” means any individual or private group, organization, proprietorship, partnership, trust, cooperative, utility, corporation, or other commercial entity, including an officer, employee, or agent thereof.

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

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

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

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

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

(22) Utility.—The term “utility” means a provider of essential services (other than law enforcement or regulatory services), including electricity, natural gas, propane, telecommunications, transportation, rail, water, or wastewater services.

SEC. 3. SHARING OF INFORMATION BY THE FEDERAL GOVERNMENT.

(a) In General.—Consistent with the protection of intelligence sources and methods and the protection of privacy and civil liberties, the Director of National Intelligence, the Secretary of Homeland Security, and the Attorney General, in consultation with the heads of the appropriate Federal agencies, shall develop and promulgate procedures to facilitate and promote—
(1) the timely sharing of classified cyber threat indicators in the possession of the Federal Government with cleared representatives of appropriate entities;

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

(3) the sharing with appropriate entities, or, if appropriate, public availability, of unclassified, including controlled unclassified, cyber threat indicators in the possession of the Federal Government.

(b) Development of Procedures.—

(1) In General.—The procedures developed and promulgated under subsection (a) shall—

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

(B) incorporate, to the greatest extent possible, existing processes and existing roles and responsibilities of Federal and non-Federal entities for information sharing by the Federal Government, including sector specific information sharing and analysis centers.
(2) COORDINATION.—In developing the procedures required under this section, the Director of National Intelligence, the Secretary of Homeland Security, and the Attorney General shall coordinate with appropriate entities to ensure that effective protocols are implemented that will facilitate and promote the sharing of cyber threat indicators by the Federal Government in a timely manner.

(e) SUBMITTAL TO CONGRESS.—Not later than 60 days after the date of the enactment of this Act, the Director of National Intelligence, in consultation with the heads of the appropriate Federal entities, shall submit to Congress the procedures required by subsection (a).

SEC. 4. AUTHORIZATIONS FOR PREVENTING, INVESTIGATING, OR MITIGATING CYBERSECURITY THREATS.

(a) AUTHORIZATION FOR MONITORING.—

(1) IN GENERAL.—Notwithstanding any other provision of law, a private entity may, [only] for cybersecurity purposes and in order to obtain, identify, or otherwise possess cyber threat indicators, monitor—

(A) the information systems of such private entity;
(B) the information systems of another entity, upon written consent of such other entity;

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

(D) information that is stored on, processed by, or transiting the information systems monitored by the private entity under this paragraph.

(2) CONSTRUCTION.—Nothing in this subsection shall be construed to authorize the monitoring of information systems to identify or obtain cyber threat indicators, other than as provided in this subsection.

(b) AUTHORIZATION FOR OPERATION OF COUNTERMEASURES.—Notwithstanding any other provision of law, a private entity may, [only] for cybersecurity purposes, operate countermeasures—

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

(2) on the information systems of another entity upon written consent of such entity to protect the rights or property of such entity; and
(3) on the information systems of a Federal entity upon written consent of an authorized representative of such Federal entity to protect the rights or property of the Federal Government.

(c) Authorization for Sharing or Receiving Cyber Threat Indicators.—Notwithstanding any other provision of law, and [OPTION A: “only for the purpose of preventing, investigating, or otherwise mitigating cybersecurity threats to information systems or information that is stored on, processed by, or transiting an information system,”] OR [OPTION B: “for the purposes permitted under this Act”] an entity may, consistent with the protection of classified information, share with, or receive from, any other entity or the Federal Government cyber threat indicators and countermeasures.

(d) Use and Protection of Information.—

(1) Security of Information.—Anyone monitoring information systems, operating countermeasures, or providing or receiving cyber threat indicators under this section shall implement and utilize security controls to prevent unauthorized access or acquisition of communications, records, system traffic, or other information, consistent with the need to protect information systems or information that is stored on, processed by, or transiting an in-
formation system from cybersecurity threats or to mitigate such threats.

(2) **Removal of Certain Personal Information.**—An entity sharing cyber threat indicators pursuant to this Act shall, prior to such sharing, remove any information contained within such indicators that is known to be personal information of or identifying a United States person, not directly related to a cybersecurity threat in order to ensure that such information is protected from unauthorized disclosure to any other entity or the Federal Government.

(3) **Use of Cyber Threat Indicators by Entities.**—Consistent with this Act and except as provided in paragraph (5), cyber threat indicators or countermeasures shared or received under this section may, for cybersecurity purposes—

(A) be used by a private entity to monitor or operate countermeasures on its information systems, or the information systems of another entity or a Federal entity upon the written consent of that other entity or that Federal entity; and

(B) be otherwise used, retained, and further shared by an entity.
(4) LIMITATION ON USE OF CYBER THREAT INDICATORS.—Cyber threat indicators shared or received under this section shall not be used—

(A) for any purpose, unless otherwise authorized by this Act, other than to protect information systems or information that is stored on, processed by, or transiting an information system from cybersecurity threats or to mitigate such threats; or

(B) to gain an unfair competitive advantage to the detriment of the entity authorizing such monitoring or countermeasures, and the conduct described in subsection (e) shall not constitute unfair competitive conduct.

(5) USE OF CYBER THREAT INDICATORS BY STATE, TRIBAL, OR LOCAL DEPARTMENTS OR AGENCIES.—

(A) LAW ENFORCEMENT USE.—

(i) PRIOR WRITTEN CONSENT.—Except as provided in clause (ii), cyber threat indicators shared with a State, tribal, or local department or agency under this section may, with the prior written consent of the entity sharing such indicators, be used by a State, tribal, or local department or
agency for the purpose of preventing, investigating, or prosecute a criminal act.

(ii) Oral consent.—If the need for immediate use prevents obtaining written consent, such consent may be provided orally with subsequent documentation of the consent.

(B) Exemption from disclosure.—Cyber threat indicators shared with a State, tribal, or local department or agency under this section shall be—

(i) deemed voluntarily shared information; and

(ii) exempt from disclosure under any State, tribal, or local law requiring disclosure of information or records.

(C) State, tribal, and local regulatory authority.—

(i) Authorization.—Cyber threat indicators shared with a State, tribal, or local department or agency under this section may, consistent with State regulatory authority specifically relating to the prevention or mitigation of cybersecurity threats to information systems, inform the
development or implementation of regulations relating to such information systems.

(ii) LIMITATION.—Such cyber threat indicators shall not otherwise be directly used by any State, tribal, or local department or agency to regulate the lawful activities of an entity.

(iii) EXCEPTION.—Any procedures required to be developed and implemented under this Act shall not be considered regulations within the meaning of this subparagraph.

(e) ANTITRUST EXEMPTION.—

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

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

(A) facilitating the prevention, investigation, or mitigation of cybersecurity threats to information systems or information that is
stored on, processed by, or transiting an information system; or

(B) communicating or disclosing cyber threat indicators to help prevent, investigate, or mitigate the effects of cybersecurity threats to information systems or information that is stored on, processed by, or transiting an information system.

(f) No Right or Benefit.—The sharing of cyber threat indicators with an entity under this Act shall not create a right or benefit to similar information by such entity or any other entity.

SEC. 5. SHARING OF CYBER THREAT INDICATORS AND COUNTERMEASURES WITH THE FEDERAL GOVERNMENT.

(a) Requirement for Policies and Procedures.—

(1) Interim policies and procedures.—Not later than 30 days after the date of the enactment of this Act, the Attorney General, in coordination with the heads of the appropriate Federal entities, shall develop, and submit to Congress, interim policies and procedures relating to the receipt of cyber threat indicators and countermeasures by the Federal Government.
(2) Final policies and procedures.—Not later than 60 days after the date of the enactment of this Act, the Attorney General, in coordination with the heads of the appropriate Federal entities, shall promulgate final policies and procedures relating to the receipt of cyber threat indicators and countermeasures by the Federal Government.

(3) Requirements concerning policies and procedures.—The policies and procedures developed and promulgated under this subsection shall—

(A) ensure that cyber threat indicators shared with the Federal Government by any entity pursuant to section 3, and that are received through the process described in subsection (c)—

(i) are shared in real time and simultaneous with such receipt with all of the appropriate Federal entities;

(ii) are not subject to any delay, interference, or any other action that could impede real-time receipt by all of the appropriate Federal entities; and

(iii) may be provided to other Federal entities;
(B) ensure that cyber threat indicators shared with the Federal Government by any entity pursuant to section 3 in a manner other than the process described in subsection (c)—

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

(ii) may be provided to other Federal entities;

(C) govern, consistent with this Act and any other applicable laws, the retention, use, and dissemination by the Federal Government of cyber threat indicators shared with the Federal Government under this Act, including the extent, if any, to which such cyber threat indicators may be used by the Federal Government for authorized [OPTION B: “cybersecurity, foreign intelligence, counterintelligence, or law enforcement”] OR [OPTION A: “cybersecurity”] purposes; and

(D) ensure there is an audit capability and appropriate sanctions in place for officers, employees, or agents of a Federal entity who knowingly and willfully conduct activities under this Act in an unauthorized manner.

(b) PRIVACY AND CIVIL LIBERTIES.—
(1) GUIDELINES OF ATTORNEY GENERAL.—The Attorney General shall, in coordination with the heads of the appropriate Federal agencies and in consultation with Federal privacy and civil liberties officials, develop and periodically review guidelines relating to privacy and civil liberties which shall govern the receipt, retention, use, and dissemination of cyber threat indicators by a Federal entity obtained in connection with activities authorized in this Act.

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

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

(B) limit the receipt, retention, use and dissemination of cyber threat indicators associated with specific persons, including establishing a process for the timely destruction of information that is known not to be directly related to [OPTION A: “a cybersecurity threat”] OR [OPTION B: “uses authorized under this Act”];
(C) include requirements to safeguard cyber threat indicators that may be used to identify specific persons from unauthorized access or acquisition, including appropriate sanctions for activities by officers, employees, or agents of the Federal Government in contravention of such guidelines;

(D) include procedures for notifying entities if information received pursuant to this section is not a cyber threat indicator; and

(E) protect the confidentiality of cyber threat indicators associated with specific persons to the greatest extent practicable and require recipients to be informed that such indicators may only be used for purposes authorized under this Act.

(c) CAPABILITY AND PROCESS WITHIN THE DEPARTMENT OF HOMELAND SECURITY.—

(1) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act, the Secretary of Homeland Security, in coordination with the heads of the appropriate Federal entities, shall develop and implement a capability and process within the Department of Homeland Security that—
(A) shall accept from any entity in real
time cyber threat indicators and counter-
measures in an electronic format, pursuant to
this section;

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

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

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

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

(iv) communications with a Federal
regulatory authority by regulated entities;
and
(v) cyber threat indicators shared with
a Federal entity as part of a contractual or
statutory requirement;”
(C) ensures that all of the appropriate
Federal entities receive such cyber threat indi-
cators in real time and simultaneous with re-
ceipt through the process within the Depart-
ment of Homeland Security; and
(D) is in compliance with the policies, pro-
cedures, and guidelines required by this section.

(2) CERTIFICATION.—Not later than 10 days
prior to the implementation of the capability and
process required by paragraph (1), the Secretary of
Homeland Security shall, in consultation with the
heads of the appropriate Federal entities, certify to
Congress [OPTION C: “that such capability and
process within the Department of Homeland Secu-
rit y does fully and effectively operate as a real time,
automated process by which the Federal Government
may receive from any entity cyber threat indicators
and countermeasures in an electronic format in ac-
cordance with the policies, procedures, and guide-
lines developed under this section.”] OR [OPTION
D: “whether such capability and process fully and
effectively operates—
(A) as the process by which the Federal Government receives from any entity cyber threat indicators and countermeasures in an electronic format; and

(B) in accordance with the policies, procedures, and guidelines developed under this section.”]

(3) PUBLIC NOTICE AND ACCESS.—The Secretary of Homeland Security shall ensure there is public notice of, and access to, the capability and process developed and implemented under paragraph (1) so that any entity may share cyber threat indicators and countermeasures through such process with the Federal Government and that all of the appropriate Federal entities receive such cyber threat indicators and countermeasures in real time and simultaneous with receipt through the process within the Department of Homeland Security.

(4) OTHER FEDERAL ENTITIES.—The process developed and implemented under paragraph (1) shall ensure that other Federal entities receive in a timely manner any cyber threat indicators and countermeasures shared with the Federal Government through the process created in this subsection.

(5) REPORT.—
(A) IN GENERAL.—Not later than 60 days after the date of the enactment of this Act, the Secretary of Homeland Security shall submit to Congress a report on the development and implementation of the capability and process required by paragraph (1), including a description of such capability and process and the public notice of, and access to, such process.

(B) CLASSIFIED ANNEX.—The report required by subparagraph (A) shall be submitted in unclassified form, but may include a classified annex.

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

(1) NO WAIVER OF PRIVILEGE OR PROTECTION.—The provision of cyber threat indicators and countermeasures to the Federal Government under this Act shall not constitute a waiver of any applicable privilege or protection provided by law, including trade secret protection.

(2) PROPRIETARY INFORMATION.—Cyber threat indicators and countermeasures provided to the Federal Government under this Act shall be considered the commercial, financial, and proprietary informa-
tion of the entity providing such information to the Federal Government.

(3) **Exemption from Disclosure.**—Cyber threat indicators and countermeasures provided to the Federal Government under this Act shall be—

(A) deemed voluntarily shared information and exempt from disclosure under section 552 of title 5, United States Code, and any State, tribal, or local law requiring disclosure of information or records; and

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

(4) **Ex Parte Communications.**—The provision of cyber threat indicators and countermeasures to the Federal Government under this Act shall not be subject to the rules of any Federal agency or department or any judicial doctrine regarding ex parte communications with a decisionmaking official.

(5) **Disclosure, Retention, and Use.**—

(A) **Authorized Activities.**—Cyber threat indicators and countermeasures provided to the Federal Government under this Act may
be disclosed to, retained by, and used by, consistent with otherwise applicable Federal law, any Federal agency or department, component, officer, employee, or agent of the Federal Government solely for—

(i) a cybersecurity purpose;

(ii) the purpose of responding to, or otherwise preventing or mitigating, an imminent threat of death or serious bodily harm;

(iii) [OPTION B: “the purpose of preventing, investigating, or prosecuting a cyber crime; or

(iv) a foreign intelligence or counterintelligence purpose.”]

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

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

(i) in accordance with the policies, procedures, and guidelines required by subsections (a) and (b);

(ii) in a manner that protects from unauthorized use or disclosure any cyber threat indicators that may be used to identify specific persons; and

(iii) in a manner that protects the confidentiality of cyber threat indicators containing information of, or that identifies, a United States person.

(D) FEDERAL REGULATORY AUTHORITY.—

(i) IN GENERAL.—Cyber threat indicators and countermeasures provided to the Federal Government under this Act may, consistent with existing Federal or State regulatory authority specifically relating to the prevention or mitigation of cybersecurity threats to information systems, inform the development or implementation of regulations relating to such information systems.
(ii) LIMITATION.—Cyber threat indicators and countermeasures provided to the Federal Government under this Act shall not be directly used by any Federal, State, tribal, or local government department or agency to regulate the lawful activities of an entity, including activities relating to monitoring, operation of countermeasures, or sharing of cyber threat indicators.

(iii) EXCEPTION.—Any procedures required to be developed and implemented under this Act shall not be considered regulations within the meaning of this subparagraph.

SEC. 6. PROTECTION FROM LIABILITY.

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

(b) SHARING OR RECEIPT OF CYBER THREAT INDICATORS.—No cause of action shall lie or be maintained in any court against any entity, and such action shall be
promptly dismissed, for the sharing or receipt of cyber
threat indicators or countermeasures under subsection (e)
of section 4 that is conducted in accordance with this Act.

(c) Good Faith Defense in Certain Causes of
Action.—If a cause of action is not otherwise dismissed
or precluded under subsection (a) or (b), a good faith reli-
ance by an entity that the conduct complained of was per-
mitted under this Act shall be a complete defense against
any action brought in any court against such entity.

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

(1) gross negligence or willful misconduct in the
course of conducting activities authorized by this
Act; or

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

SEC. 7. OVERSIGHT OF GOVERNMENT ACTIVITIES.

(a) Biennial Report on Implementation.—

(1) In General.—Not later than 2 years after
the date of the enactment of this Act, and not less
frequently than once every 2 years thereafter, the
heads of the appropriate Federal entities shall joint-
ly submit to Congress a detailed report concerning
the implementation of this Act.
(2) CONTENTS.—Each report submitted under paragraph (1) shall include the following:

(A) An assessment of the sufficiency of the policies, procedures, and guidelines required by section 5 in ensuring that cyber threat indicators are shared effectively and responsibly within the Federal Government.

(B) An evaluation of the effectiveness of real-time information sharing through the capability and process developed under section 5(c), including any impediments to such real-time sharing.

(C) An assessment of the sufficiency of the procedures developed under section 3 in ensuring that cyber threat indicators in the possession of the Federal Government are shared in a timely and adequate manner with appropriate entities, or, if appropriate, are made publicly available.

(D) An assessment of whether cyber threat indicators have been properly classified and an accounting of the number of security clearances authorized by the Federal Government for the purposes of this Act.
(E) A review of the type of cyber threat indicators shared with the Federal Government under this Act, including—

(i) the degree to which such information may impact the privacy and civil liberties of United States persons;

(ii) a quantitative and qualitative assessment of the impact of the sharing of such cyber threat indicators with the Federal Government on privacy and civil liberties of United States persons; and

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

(F) A review of actions taken by the Federal Government based on cyber threat indicators shared with the Federal Government under this Act, including the appropriateness of any subsequent use or dissemination of such cyber threat indicators by a Federal entity under section 5.

(G) A description of any violations of the requirements of this Act by the Federal Government.
(H) A classified list of entities that received classified cyber threat indicators from the Federal Government under this Act and an evaluation of the risks and benefits of sharing such cyber threat indicators.

(3) Recommendations.—Each report submitted under paragraph (1) may include such recommendations as the heads of the appropriate Federal entities may have for improvements or modifications to the authorities and processes under this Act.

(4) Form of report.—Each report required by paragraph (1) shall be submitted in unclassified form, but shall include a classified annex.

(b) Reports on Privacy and Civil Liberties.—

(1) Biennial report from privacy and civil liberties oversight board.—Not later than 1 year after the date of the enactment of this Act and not less frequently than once every 2 years thereafter, the Privacy and Civil Liberties Oversight Board shall submit to Congress and the President a report providing—

(A) an assessment of the privacy and civil liberties impact of the type of activities carried out under this Act; and
(B) an assessment of the sufficiency of the policies, procedures, and guidelines established pursuant to section 5 in addressing privacy and civil liberties concerns.

(2) Biennial report of inspectors general.—

(A) in general.—Not later than 2 years after the date of the enactment of this Act and not less frequently than once every 2 years thereafter, the Inspector General of the Department of Homeland Security, the Inspector General of the Intelligence Community, the Inspector General of the Department of Justice, and the Inspector General of the Department of Defense shall jointly submit to Congress a report on the receipt, use, and dissemination of cyber threat indicators and countermeasures that have been shared with Federal entities under this Act.

(B) Contents.—Each report submitted under subparagraph (A) shall include the following:

(i) A review of the types of cyber threat indicators shared with Federal entities.
(ii) A review of the actions taken by Federal entities as a result of the receipt of such cyber threat indicators.

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

(iv) A review of the sharing of such cyber threat indicators among Federal entities to identify inappropriate barriers to sharing information.

(3) **Recommendations.**—Each report submitted under this subsection may include such recommendations as the Privacy and Civil Liberties Oversight Board, with respect to a report submitted under paragraph (1), or the Inspectors General referred to in paragraph (2)(A), with respect to a report submitted under paragraph (2), may have for improvements or modifications to the authorities under this Act.

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

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

(a) **Otherwise Lawful Disclosures.**—Nothing in this Act shall be construed to limit or prohibit otherwise lawful disclosures of communications, records, or other in-
formation by an entity to any other entity or the Federal Government under this Act.

(b) WHISTLEBLOWER PROTECTIONS.—Nothing in this Act shall be construed to preempt any employee from exercising rights currently provided under any whistleblower law, rule, or regulation.

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

(1) as creating any immunity against, or otherwise affecting, any action brought by the Federal Government, or any agency or department thereof, to enforce any law, executive order, or procedure governing the appropriate handling, disclosure, or use of classified information;

(2) to impact the conduct of authorized law enforcement or intelligence activities; or

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

(d) RELATIONSHIP TO OTHER LAWS.—Nothing in this Act shall be construed to affect any requirement under any other provision of law for an entity to provide information to the Federal Government.
(e) **Prohibited Conduct.**—Nothing in this Act shall be construed to permit price-fixing, allocating a market between competitors, monopolizing or attempting to monopolize a market, boycotting, or exchanges of price or cost information, customer lists, or information regarding future competitive planning.

(f) **Information Sharing Relationships.**—Nothing in this Act shall be construed—

1. to limit or modify an existing information sharing relationship;

2. to prohibit a new information sharing relationship;

3. to require a new information sharing relationship between any entity and the Federal Government;

4. to require the use of the capability and process within the Department of Homeland Security developed under section 5(c); or

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

(g) **Anti-Tasking Restriction.**—Nothing in this Act shall be construed to permit the Federal Government—
(1) to require an entity to provide information
to the Federal Government; or

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

(h) No Liability for Non-Participation.—Nothing
in this Act shall be construed to subject any entity
to liability for choosing not to engage in the voluntary ac-
tivities authorized in this Act.

(i) Use and Retention of Information.—Nothing
in this Act shall be construed to authorize, or to mod-
ify any existing authority of, a department or agency of
the Federal Government to retain or use any information
shared under this Act for any use other than permitted
in this Act.

(j) Federal Preemption.—

(1) In General.—This Act supersedes any
statute or other law of a State or political subdivi-
sion of a State that restricts or otherwise expressly
regulates an activity authorized under this Act.

(2) State Law Enforcement.—Nothing in
this Act shall be construed to supersedes any statute
or other law of a State or political subdivision of a
State concerning the use of authorized law enforce-
ment practices and procedures.
SEC. 9. CONFORMING AMENDMENTS.

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

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

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

(3) by adding at the end the following:

“(10) information shared with or provided to the Federal Government pursuant to the Cybersecurity Information Sharing Act of 2014.”.