

Calendar No. 462

113TH CONGRESS
2D SESSION**S. 2588**

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

JULY 10, 2014

Mrs. FEINSTEIN, from the Select Committee on Intelligence, reported the following original bill; which was read twice and placed on the calendar

A BILL

To improve cybersecurity in the United States through enhanced 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 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. Report on cybersecurity threats.
 Sec. 10. 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.

1 (B) The Department of Defense.

2 (C) The Department of Energy.

3 (D) The Department of Homeland Security.
4

5 (E) The Department of Justice.

6 (F) The Department of the Treasury.

7 (G) The Office of the Director of National
8 Intelligence.

9 (4) COUNTERMEASURE.—The term “counter-
10 measure” means an action, device, procedure, tech-
11 nique, or other measure applied to an information
12 system or information that is stored on, processed
13 by, or transiting an information system that pre-
14 vents or mitigates a known or suspected cybersecu-
15 rity threat or security vulnerability.

16 (5) 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 (6) CYBERSECURITY THREAT.—The term “cy-
23 bersecurity threat” means an action, not protected
24 by the First Amendment to the Constitution of the
25 United States, on or through an information system

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

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

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

14 (B) a method of defeating a security con-
15 trol or exploitation of a security vulnerability;

16 (C) a security vulnerability;

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

23 (E) malicious cyber command and control;

24 (F) the actual or potential harm caused by
25 an incident, including information exfiltrated

1 when it is necessary in order to describe a cy-
2 bersecurity threat;

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

6 (H) any combination thereof.

7 (8) ELECTRONIC FORMAT.—

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

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

17 (9) ENTITY.—

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

24 (B) INCLUSIONS.—The term “entity” in-
25 cludes a government agency or department (in-

1 including an officer, employee, or agent thereof)
2 of the District of Columbia, the Commonwealth
3 of Puerto Rico, the Virgin Islands, Guam,
4 American Samoa, the Northern Mariana Is-
5 lands, and any other territory or possession of
6 the United States.

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

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

15 (11) INFORMATION SYSTEM.—The term “infor-
16 mation system”—

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

19 (B) includes industrial control systems,
20 such as supervisory control and data acquisition
21 systems, distributed control systems, and pro-
22 grammable logic controllers.

23 (12) LOCAL GOVERNMENT.—The term “local
24 government” means any borough, city, county, par-

1 ish, town, township, village, or other political sub-
2 division of a State.

3 (13) MALICIOUS CYBER COMMAND AND CON-
4 TROL.—The term “malicious cyber command and
5 control” means a method for unauthorized remote
6 identification of, access to, or use of, an information
7 system or information that is stored on, processed
8 by, or transiting an information system.

9 (14) MALICIOUS RECONNAISSANCE.—The term
10 “malicious reconnaissance” means a method for ac-
11 tively probing or passively monitoring an information
12 system for the purpose of discerning security
13 vulnerabilities of the information system, if such
14 method is associated with a known or suspected cy-
15 bersecurity threat.

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

20 (16) PRIVATE ENTITY.—

21 (A) IN GENERAL.—The term “private enti-
22 ty” means any individual or private group, or-
23 ganization, proprietorship, partnership, trust,
24 cooperative, corporation, or other commercial or

1 nonprofit entity, including an officer, employee,
2 or agent thereof.

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

7 (17) SECURITY CONTROL.—The term “security
8 control” means the management, operational, and
9 technical controls used to protect the confidentiality,
10 integrity, and availability of an information system
11 or its information.

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

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

20 **SEC. 3. SHARING OF INFORMATION BY THE FEDERAL GOV-**
21 **ERNMENT.**

22 (a) IN GENERAL.—Consistent with the protection of
23 intelligence sources and methods and the protection of pri-
24 vacy and civil liberties, the Director of National Intel-
25 ligence, the Secretary of Homeland Security, the Secretary

1 of Defense, and the Attorney General, in consultation with
2 the heads of the appropriate Federal entities, shall develop
3 and promulgate procedures to facilitate and promote—

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

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

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

16 (b) DEVELOPMENT OF PROCEDURES.—

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

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

23 (B) incorporate, to the greatest extent pos-
24 sible, existing processes and existing roles and
25 responsibilities of Federal and non-Federal enti-

1 ties for information sharing by the Federal
2 Government, including sector specific informa-
3 tion sharing and analysis centers.

4 (2) COORDINATION.—In developing the proce-
5 dures required under this section, the Director of
6 National Intelligence, the Secretary of Homeland Se-
7 curity, and the Attorney General shall coordinate
8 with appropriate Federal entities, including the Na-
9 tional Laboratories (as defined in section 2 of the
10 Energy Policy Act of 2005 (42 U.S.C. 15801)), to
11 ensure that effective protocols are implemented that
12 will facilitate and promote the sharing of cyber
13 threat indicators by the Federal Government in a
14 timely manner.

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

20 **SEC. 4. AUTHORIZATIONS FOR PREVENTING, DETECTING,**
21 **ANALYZING, AND MITIGATING CYBERSECU-**
22 **RITY THREATS.**

23 (a) AUTHORIZATION FOR MONITORING.—

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

4 (A) the information systems of such pri-
5 vate entity;

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

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

11 (D) information that is stored on, proc-
12 essed by, or transiting the information systems
13 monitored by the private entity under this para-
14 graph.

15 (2) CONSTRUCTION.—Nothing in this sub-
16 section shall be construed to authorize the moni-
17 toring of information systems other than as provided
18 in this subsection or to limit otherwise lawful activ-
19 ity.

20 (b) AUTHORIZATION FOR OPERATION OF COUNTER-
21 MEASURES.—

22 (1) IN GENERAL.—Notwithstanding any other
23 provision of law, a private entity may, for cybersecu-
24 rity purposes, operate countermeasures that are ap-
25 plied to—

1 (A) the information systems of such pri-
2 vate entity in order to protect the rights or
3 property of the private entity;

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

7 (C) the information systems of a Federal
8 entity upon written consent of an authorized
9 representative of such Federal entity to protect
10 the rights or property of the Federal Govern-
11 ment.

12 (2) CONSTRUCTION.—Nothing in this sub-
13 section shall be construed to authorize the use of
14 countermeasures other than as provided in this sub-
15 section or to limit otherwise lawful activity.

16 (c) AUTHORIZATION FOR SHARING OR RECEIVING
17 CYBER THREAT INDICATORS OR COUNTERMEASURES.—

18 (1) IN GENERAL.—Notwithstanding any other
19 provision of law, and for the purposes permitted
20 under this Act, an entity may, consistent with the
21 protection of classified information, share with, or
22 receive from, any other entity or the Federal Gov-
23 ernment cyber threat indicators and counter-
24 measures.

1 (2) CONSTRUCTION.—Nothing in this sub-
2 section shall be construed to authorize the sharing
3 or receiving of cyber threat indicators or counter-
4 measures other than as provided in this subsection
5 or to limit otherwise lawful activity.

6 (d) PROTECTION AND USE OF INFORMATION.—

7 (1) SECURITY OF INFORMATION.—An entity or
8 Federal entity monitoring information systems, oper-
9 ating countermeasures, or providing or receiving
10 cyber threat indicators or countermeasures under
11 this section shall implement and utilize security con-
12 trols to protect against unauthorized access to or ac-
13 quisition of such cyber threat indicators or counter-
14 measures.

15 (2) REMOVAL OF CERTAIN PERSONAL INFORMA-
16 TION.—An entity or Federal entity sharing cyber
17 threat indicators pursuant to this Act shall, prior to
18 such sharing, remove any information contained
19 within such indicators that the entity or Federal en-
20 tity knows at the time of sharing to be personal in-
21 formation of or identifying a specific person not di-
22 rectly related to a cybersecurity threat.

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

1 (A) IN GENERAL.—Consistent with this
2 Act, cyber threat indicators or countermeasures
3 shared or received under this section may, for
4 cybersecurity purposes—

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

11 (ii) be otherwise used, retained, and
12 further shared by an entity.

13 (B) CONSTRUCTION.—Nothing in this
14 paragraph shall be construed to authorize the
15 use of cyber threat indicators or counter-
16 measures other than as provided in this section.

17 (4) USE OF CYBER THREAT INDICATORS BY
18 STATE, TRIBAL, OR LOCAL DEPARTMENTS OR AGEN-
19 CIES.—

20 (A) LAW ENFORCEMENT USE.—

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

1 the entity sharing such indicators, be used
2 by a State, tribal, or local department or
3 agency for the purpose of preventing, in-
4 vestigating, or prosecuting a computer
5 crime.

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

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

15 (i) deemed voluntarily shared informa-
16 tion; and

17 (ii) exempt from disclosure under any
18 State, tribal, or local law requiring disclo-
19 sure of information or records.

20 (C) STATE, TRIBAL, AND LOCAL REGU-
21 LATORY AUTHORITY.—

22 (i) AUTHORIZATION.—Cyber threat
23 indicators shared with a State, tribal, or
24 local department or agency under this sec-
25 tion may, consistent with State regulatory

1 authority specifically relating to the pre-
2 vention or mitigation of cybersecurity
3 threats to information systems, inform the
4 development or implementation of regula-
5 tions relating to such information systems.

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

11 (e) ANTITRUST EXEMPTION.—

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

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

22 (A) facilitating the prevention, investiga-
23 tion, or mitigation of cybersecurity threats to
24 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 60 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 180 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 4, 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 4 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;

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

11 (iii) may be provided to other Federal
12 entities;

13 (C) govern, consistent with this Act, any
14 other applicable laws, and the fair information
15 practice principles set forth in appendix A of
16 the document entitled “National Strategy for
17 Trusted Identities in Cyberspace” and pub-
18 lished by the President in April, 2011, the re-
19 tention, use, and dissemination by the Federal
20 Government of cyber threat indicators shared
21 with the Federal Government under this Act,
22 including the extent, if any, to which such cyber
23 threat indicators may be used by the Federal
24 Government; and

1 (D) ensure there is an audit capability and
2 appropriate sanctions in place for officers, em-
3 ployees, or agents of a Federal entity who
4 knowingly and willfully conduct activities under
5 this Act in an unauthorized manner.

6 (b) PRIVACY AND CIVIL LIBERTIES.—

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

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

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

1 (B) limit the receipt, retention, use, and
2 dissemination of cyber threat indicators con-
3 taining personal information of or identifying
4 specific persons, including establishing—

5 (i) a process for the timely destruction
6 of information that is known not to be di-
7 rectly related to uses authorized under this
8 Act; and

9 (ii) specific limitations on the length
10 of any period in which a cyber threat indi-
11 cator may be retained;

12 (C) include requirements to safeguard
13 cyber threat indicators containing personal in-
14 formation of or identifying specific persons
15 from unauthorized access or acquisition, includ-
16 ing appropriate sanctions for activities by offi-
17 cers, employees, or agents of the Federal Gov-
18 ernment in contravention of such guidelines;

19 (D) include procedures for notifying enti-
20 ties if information received pursuant to this sec-
21 tion is known by a Federal entity receiving the
22 information not to constitute a cyber threat in-
23 dicator; and

24 (E) protect the confidentiality of cyber
25 threat indicators containing personal informa-

1 tion of or identifying specific persons to the
2 greatest extent practicable and require recipi-
3 ents to be informed that such indicators may
4 only be used for purposes authorized under this
5 Act.

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

8 (1) IN GENERAL.—Not later than 90 days after
9 the date of the enactment of this Act, the Secretary
10 of Homeland Security, in coordination with the
11 heads of the appropriate Federal entities, shall de-
12 velop and implement a capability and process within
13 the Department of Homeland Security that—

14 (A) shall accept from any entity in real
15 time cyber threat indicators and counter-
16 measures in an electronic format, pursuant to
17 this section;

18 (B) shall, upon submittal of the certifi-
19 cation under paragraph (2) that such capability
20 and process fully and effectively operates as de-
21 scribed in such paragraph, be the process by
22 which the Federal Government receives cyber
23 threat indicators and countermeasures under
24 this Act in an electronic format that are shared

1 by a private entity with the Federal Govern-
2 ment except—

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

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

8 (iii) information received through an
9 automated malware analysis capability op-
10 erated by the Federal Bureau of Investiga-
11 tion that is designed to ensure that infor-
12 mation received through and analysis pro-
13 duced by such capability is also imme-
14 diately shared through the capability and
15 process developed by the Secretary of
16 Homeland Security under this paragraph;

17 (iv) communications with a Federal
18 regulatory authority by regulated entities
19 regarding a cybersecurity threat; and

20 (v) cyber threat indicators or counter-
21 measures shared with a Federal entity as
22 part of a contractual or statutory require-
23 ment;

24 (C) ensures that all of the appropriate
25 Federal entities receive such cyber threat indi-

1 cators in real time and simultaneous with re-
2 ceipt through the process within the Depart-
3 ment of Homeland Security; and

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

6 (2) CERTIFICATION.—Not later than 10 days
7 prior to the implementation of the capability and
8 process required by paragraph (1), the Secretary of
9 Homeland Security shall, in consultation with the
10 heads of the appropriate Federal entities, certify to
11 Congress whether such capability and process fully
12 and effectively operates—

13 (A) as the process by which the Federal
14 Government receives from any entity cyber
15 threat indicators and countermeasures in an
16 electronic format under this Act; and

17 (B) in accordance with the policies, proce-
18 dures, and guidelines developed under this sec-
19 tion.

20 (3) PUBLIC NOTICE AND ACCESS.—The Sec-
21 retary of Homeland Security shall ensure there is
22 public notice of, and access to, the capability and
23 process developed and implemented under paragraph
24 (1) so that any entity may share cyber threat indica-
25 tors and countermeasures through such process with

1 the Federal Government and that all of the appro-
2 priate Federal entities receive such cyber threat indi-
3 cators and countermeasures in real time and simul-
4 taneous with receipt through the process within the
5 Department of Homeland Security.

6 (4) OTHER FEDERAL ENTITIES.—The process
7 developed and implemented under paragraph (1)
8 shall ensure that other Federal entities receive in a
9 timely manner any cyber threat indicators and coun-
10 termeasures shared with the Federal Government
11 through the process created in this subsection.

12 (5) REPORTS.—

13 (A) REPORT ON DEVELOPMENT AND IM-
14 PLEMENTATION.—

15 (i) IN GENERAL.—Not later than 60
16 days after the date of the enactment of
17 this Act, the Secretary of Homeland Secu-
18 rity shall submit to Congress a report on
19 the development and implementation of the
20 capability and process required by para-
21 graph (1), including a description of such
22 capability and process and the public no-
23 tice of, and access to, such process.

24 (ii) CLASSIFIED ANNEX.—The report
25 required by clause (i) shall be submitted in

1 unclassified form, but may include a classi-
2 fied annex.

3 (B) REPORT ON AUTOMATED MALWARE
4 ANALYSIS CAPABILITY.—Not later than 1 year
5 after the date of the enactment of this Act, the
6 Director of the Federal Bureau of Investigation
7 and the Secretary of Homeland Security shall
8 submit to Congress a report on the implementa-
9 tion of the automated malware analysis capa-
10 bility described in paragraph (1)(B)(iii), includ-
11 ing an assessment of the feasibility and advis-
12 ability of transferring the administration and
13 operation of such capability to the Department
14 of Homeland Security.

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

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

23 (2) PROPRIETARY INFORMATION.—A cyber
24 threat indicator or countermeasure provided by an
25 entity to the Federal Government under this Act

1 shall be considered the commercial, financial, and
2 proprietary information of such entity when so des-
3 ignated by such entity.

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

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

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

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

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

24 (A) AUTHORIZED ACTIVITIES.—Cyber
25 threat indicators and countermeasures provided

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

7 (i) a cybersecurity purpose;

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

12 (iii) the purpose of responding to, or
13 otherwise preventing or mitigating, a seri-
14 ous threat to a minor, including sexual ex-
15 ploitation and threats to physical safety; or

16 (iv) the purpose of preventing, inves-
17 tigating, or prosecuting an offense arising
18 out of a threat described in clause (ii) or
19 any of the offenses listed in—

20 (I) sections 1028 through 1030
21 of title 18, United States Code (relat-
22 ing to fraud and identity theft);

23 (II) chapter 37 of such title (re-
24 lating to espionage and censorship);
25 and

1 (III) chapter 90 of such title (re-
2 lating to protection of trade secrets).

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

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

14 (i) in accordance with the policies,
15 procedures, and guidelines required by sub-
16 sections (a) and (b);

17 (ii) in a manner that protects from
18 unauthorized use or disclosure any cyber
19 threat indicators that may contain personal
20 information of or identifying specific per-
21 sons; and

22 (iii) in a manner that protects the
23 confidentiality of cyber threat indicators
24 containing information of, or that identi-
25 fies, a specific person.

1 (D) FEDERAL REGULATORY AUTHORITY.—

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

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

22 (iii) EXCEPTION.—Procedures devel-
23 oped and implemented under this Act shall
24 not be considered regulations within the
25 meaning of this subparagraph.

1 **SEC. 6. PROTECTION FROM LIABILITY.**

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

8 (b) SHARING OR RECEIPT OF CYBER THREAT INDI-
9 CATORS.—No cause of action shall lie or be maintained
10 in any court against any entity, and such action shall be
11 promptly dismissed, for the sharing or receipt of cyber
12 threat indicators or countermeasures under subsection (c)
13 of section 4 if—

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

16 (2) in a case in which a cyber threat indicator
17 or countermeasure is shared with the Federal Gov-
18 ernment in an electronic format, the cyber threat in-
19 dicator or countermeasure is shared in a manner
20 that is consistent with section 5(c).

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

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

4 (1) gross negligence or wilful misconduct in the
5 course of conducting activities authorized by this
6 Act; or

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

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

10 (a) BIENNIAL REPORT ON IMPLEMENTATION.—

11 (1) IN GENERAL.—Not later than 1 year after
12 the date of the enactment of this Act, and not less
13 frequently than once every 2 years thereafter, the
14 heads of the appropriate Federal entities shall joint-
15 ly submit to Congress a detailed report concerning
16 the implementation of this Act.

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

19 (A) An assessment of the sufficiency of the
20 policies, procedures, and guidelines required by
21 section 5 in ensuring that cyber threat indica-
22 tors are shared effectively and responsibly with-
23 in the Federal Government.

24 (B) An evaluation of the effectiveness of
25 real-time information sharing through the capa-

1 bility and process developed under section 5(c),
2 including any impediments to such real-time
3 sharing.

4 (C) An assessment of the sufficiency of the
5 procedures developed under section 3 in ensur-
6 ing that cyber threat indicators in the posses-
7 sion of the Federal Government are shared in
8 a timely and adequate manner with appropriate
9 entities, or, if appropriate, are made publicly
10 available.

11 (D) An assessment of whether cyber threat
12 indicators have been properly classified and an
13 accounting of the number of security clearances
14 authorized by the Federal Government for the
15 purposes of this Act.

16 (E) A review of the type of cyber threat in-
17 dicators shared with the Federal Government
18 under this Act, including—

19 (i) the degree to which such informa-
20 tion may impact the privacy and civil lib-
21 erties of specific persons;

22 (ii) a quantitative and qualitative as-
23 sessment of the impact of the sharing of
24 such cyber threat indicators with the Fed-

1 eral Government on privacy and civil lib-
2 erties of specific persons; and

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

6 (F) A review of actions taken by the Fed-
7 eral Government based on cyber threat indica-
8 tors shared with the Federal Government under
9 this Act, including the appropriateness of any
10 subsequent use or dissemination of such cyber
11 threat indicators by a Federal entity under sec-
12 tion 5.

13 (G) A description of any significant viola-
14 tions of the requirements of this Act by the
15 Federal Government.

16 (H) A classified summary of the number
17 and type of entities that received classified
18 cyber threat indicators from the Federal Gov-
19 ernment under this Act and an evaluation of
20 the risks and benefits of sharing such cyber
21 threat indicators.

22 (3) RECOMMENDATIONS.—Each report sub-
23 mitted under paragraph (1) may include such rec-
24 ommendations as the heads of the appropriate Fed-

1 eral entities may have for improvements or modifica-
2 tions to the authorities and processes under this Act.

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

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

7 (1) BIENNIAL REPORT FROM PRIVACY AND
8 CIVIL LIBERTIES OVERSIGHT BOARD.—Not later
9 than 2 years after the date of the enactment of this
10 Act and not less frequently than once every 2 years
11 thereafter, the Privacy and Civil Liberties Oversight
12 Board shall submit to Congress and the President a
13 report providing—

14 (A) an assessment of the privacy and civil
15 liberties impact of the type of activities carried
16 out under this Act; and

17 (B) an assessment of the sufficiency of the
18 policies, procedures, and guidelines established
19 pursuant to section 5 in addressing privacy and
20 civil liberties concerns.

21 (2) BIENNIAL REPORT OF INSPECTORS GEN-
22 ERAL.—

23 (A) IN GENERAL.—Not later than 2 years
24 after the date of the enactment of this Act and
25 not less frequently than once every 2 years

1 thereafter, the Inspector General of the Depart-
2 ment of Homeland Security, the Inspector Gen-
3 eral of the Intelligence Community, the Inspec-
4 tor General of the Department of Justice, and
5 the Inspector General of the Department of De-
6 fense shall jointly submit to Congress a report
7 on the receipt, use, and dissemination of cyber
8 threat indicators and countermeasures that
9 have been shared with Federal entities under
10 this Act.

11 (B) CONTENTS.—Each report submitted
12 under subparagraph (A) shall include the fol-
13 lowing:

14 (i) A review of the types of cyber
15 threat indicators shared with Federal enti-
16 ties.

17 (ii) A review of the actions taken by
18 Federal entities as a result of the receipt
19 of such cyber threat indicators.

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

22 (iv) A review of the sharing of such
23 cyber threat indicators among Federal en-
24 tities to identify inappropriate barriers to
25 sharing information.

1 (3) RECOMMENDATIONS.—Each report sub-
2 mitted under this subsection may include such rec-
3 ommendations as the Privacy and Civil Liberties
4 Oversight Board, with respect to a report submitted
5 under paragraph (1), or the Inspectors General re-
6 ferred to in paragraph (2)(A), with respect to a re-
7 port submitted under paragraph (2), may have for
8 improvements or modifications to the authorities
9 under this Act.

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

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

14 (a) OTHERWISE LAWFUL DISCLOSURES.—Nothing in
15 this Act shall be construed to limit or prohibit otherwise
16 lawful disclosures of communications, records, or other in-
17 formation, including reporting of known or suspected
18 criminal activity, by an entity to any other entity or the
19 Federal Government under this Act.

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

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

1 (1) as creating any immunity against, or other-
2 wise affecting, any action brought by the Federal
3 Government, or any agency or department thereof,
4 to enforce any law, executive order, or procedure
5 governing the appropriate handling, disclosure, or
6 use of classified information;

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

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

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

17 (e) PROHIBITED CONDUCT.—Nothing in this Act
18 shall be construed to permit price-fixing, allocating a mar-
19 ket between competitors, monopolizing or attempting to
20 monopolize a market, boycotting, or exchanges of price or
21 cost information, customer lists, or information regarding
22 future competitive planning.

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

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

3 (2) to prohibit a new information sharing rela-
4 tionship;

5 (3) to require a new information sharing rela-
6 tionship between any entity and the Federal Govern-
7 ment;

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

11 (5) to amend, repeal, or supersede any current
12 or future contractual agreement, terms of service
13 agreement, or other contractual relationship between
14 any entities, or between any entity and the Federal
15 Government.

16 (g) ANTI-TASKING RESTRICTION.—Nothing in this
17 Act shall be construed to permit the Federal Govern-
18 ment—

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

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

24 (h) NO LIABILITY FOR NON-PARTICIPATION.—Noth-
25 ing in this Act shall be construed to subject any entity

1 to liability for choosing not to engage in the voluntary ac-
2 tivities authorized in this Act.

3 (i) USE AND RETENTION OF INFORMATION.—Noth-
4 ing in this Act shall be construed to authorize, or to mod-
5 ify any existing authority of, a department or agency of
6 the Federal Government to retain or use any information
7 shared under this Act for any use other than permitted
8 in this Act.

9 (j) FEDERAL PREEMPTION.—

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

14 (2) STATE LAW ENFORCEMENT.—Nothing in
15 this Act shall be construed to supersede any statute
16 or other law of a State or political subdivision of a
17 State concerning the use of authorized law enforce-
18 ment practices and procedures.

19 (k) REGULATORY AUTHORITY.—Nothing in this Act
20 shall be construed—

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

23 (2) to establish any regulatory authority not
24 specifically established under Act; or

1 (3) to authorize regulatory actions that would
2 duplicate or conflict with regulatory requirements,
3 mandatory standards, or related processes under
4 Federal law.

5 **SEC. 9. REPORT ON CYBERSECURITY THREATS.**

6 (a) REQUIREMENT FOR REPORT.—Not later than
7 180 days after the date of the enactment of this Act, the
8 Director of National Intelligence, in coordination with the
9 heads of other appropriate elements of the intelligence
10 community, shall submit to the Select Committee on Intel-
11 ligence of the Senate and the Permanent Select Committee
12 on Intelligence of the House of Representatives a report
13 on cybersecurity threats, including cyber attacks, theft,
14 and data breaches. Such report shall include the following:

15 (1) An assessment of the current intelligence
16 sharing and cooperation relationships of the United
17 States with other countries regarding cybersecurity
18 threats, including cyber attacks, theft, and data
19 breaches, directed against the United States and
20 which threaten the United States national security
21 interests and economy and intellectual property, spe-
22 cifically identifying the relative utility of such rela-
23 tionships, which elements of the intelligence commu-
24 nity participate in such relationships, and whether
25 and how such relationships could be improved.

1 (2) A list and an assessment of the countries
2 and non-state actors that are the primary threats of
3 carrying out a cybersecurity threat, including a
4 cyber attack, theft, or data breach, against the
5 United States and which threaten the United States
6 national security, economy, and intellectual property.

7 (3) A description of the extent to which the ca-
8 pabilities of the United States Government to re-
9 spond to or prevent cybersecurity threats, including
10 cyber attacks, theft, or data breaches, directed
11 against the United States private sector are de-
12 graded by a delay in the prompt notification by pri-
13 vate entities of such threats or cyber attacks, theft,
14 and breaches.

15 (4) An assessment of additional technologies or
16 capabilities that would enhance the ability of the
17 United States to prevent and to respond to cyberse-
18 curity threats, including cyber attacks, theft, and
19 data breaches.

20 (5) An assessment of any technologies or prac-
21 tices utilized by the private sector that could be rap-
22 idly fielded to assist the intelligence community in
23 preventing and responding to cybersecurity threats.

24 (b) INTELLIGENCE COMMUNITY DEFINED.—In this
25 section, the term “intelligence community” has the mean-

1 ing given that term in section 3(4) of the National Secu-
2 rity Act of 1947 (50 U.S.C. 3003(4)).

3 (c) FORM OF REPORT.—The report required by sub-
4 section (a) shall be made available in classified and unclas-
5 sified forms.

6 **SEC. 10. CONFORMING AMENDMENTS.**

7 (a) PUBLIC INFORMATION.—Section 552(b) of title
8 5, United States Code, is amended—

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

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

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

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

17 (b) MODIFICATION OF LIMITATION ON DISSEMINA-
18 TION OF CERTAIN INFORMATION CONCERNING PENETRA-
19 TIONS OF DEFENSE CONTRACTOR NETWORKS.—Section
20 941(c)(3) of the National Defense Authorization Act for
21 Fiscal Year 2013 (Public Law 112–239) is amended by
22 inserting at the end the following: “The Secretary may
23 share such information with other Federal entities if such
24 information consists of cyber threat indicators and coun-
25 termeasures and such information is shared consistent

1 with the policies and procedures promulgated by the At-
2 torney General under section 5 of the Cybersecurity Infor-
3 mation Sharing Act of 2014.”.

Calendar No. 462

113TH CONGRESS
2^D SESSION

S. 2588

A BILL

To improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes.

JULY 10, 2014

Read twice and placed on the calendar