IB

Union Calendar No. 44

114TH CONGRESS
1ST SESSION

H. R. 1560

[Report No. 114–63]

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

IN THE HOUSE OF REPRESENTATIVES

MARCH 24, 2015

Mr. NUNES (for himself, Mr. SCHIFF, Mr. WESTMORELAND, and Mr. HIMES) introduced the following bill; which was referred to the Select Committee on Intelligence (Permanent Select)

APRIL 13, 2015

Additional sponsors: Mr. KING of New York, Mr. LOBIONDO, Ms. SEWELL of Alabama, Mr. QUIGLEY, and Mr. MURPHY of Florida

APRIL 13, 2015

Reported with an amendment, committed to the Committee of the Whole House on the State of the Union, and ordered to be printed

[Strike out all after the enacting clause and insert the part printed in italic]

[For text of introduced bill, see copy of bill as introduced on March 24, 2015]

A BILL

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

Be it enacted by the Senate and House of Representatives 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 "Protecting Cyber Networks Act".

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

SEC. 2. SHARING OF CYBER THREAT INDICATORS AND DEFENSIVE MEASURES BY THE FEDERAL GOVERNMENT WITH NON-FEDERAL ENTITIES.

(a) IN GENERAL.—Title I of the National Security Act of 1947 (50 U.S.C. 3021 et seq.) is amended by inserting after section 110 (50 U.S.C. 3045) the following new section:

"SEC. 111. SHARING OF CYBER THREAT INDICATORS AND DEFENSIVE MEASURES BY THE FEDERAL GOVERNMENT WITH NON-FEDERAL ENTITIES.

"(a) SHARING BY THE FEDERAL GOVERNMENT.—

"(1) IN GENERAL.—Consistent with the protection of classified information, intelligence sources and methods, and privacy and civil liberties, the Director of National Intelligence, in consultation with the heads of the other appropriate Federal entities, shall develop and promulgate procedures to facilitate and promote—

"(A) the timely sharing of classified cyber threat indicators in the possession of the Federal Government with representatives of relevant non-Federal entities with appropriate security clearances;

"(B) the timely sharing with relevant non-Federal entities of cyber threat indicators in the possession of the Federal Government that may be declassified and shared at an unclassified level; and

"(C) the sharing with non-Federal entities, if appropriate, of information in the possession of the Federal Government about imminent or ongoing cybersecurity threats to such entities to prevent or mitigate adverse impacts from such cybersecurity threats.

"(2) DEVELOPMENT OF PROCEDURES.—The procedures developed and promulgated under paragraph (1) 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;

"(B) incorporate, to the greatest extent practicable, 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;

"(C) include procedures for notifying non-Federal entities that have received a cyber threat indicator from a Federal entity in accordance with this Act that is known or determined to be in error or in contravention of the requirements of this section, the Protecting Cyber Networks Act, or the amendments made by such Act or another provision of Federal law or policy of such error or contravention;

"(D) include requirements for Federal entities receiving a cyber threat indicator or defensive measure to implement appropriate security

controls to protect against unauthorized access to, or acquisition of, such cyber threat indicator or defensive measure;

"(E) include procedures that require Federal entities, prior to the sharing of a cyber threat indicator, to—

"(i) review such cyber threat indicator to assess whether such cyber threat indicator, in contravention of the requirement under section 3(d)(2) of the Protecting Cyber Networks Act, contains any information that such Federal entity knows at the time of sharing to be personal information of or information identifying a specific person not directly related to a cybersecurity threat and remove such information; or

"(ii) implement a technical capability configured to remove or exclude any personal information of or information identifying a specific person not directly related to a cybersecurity threat; and

"(F) include procedures to promote the efficient granting of security clearances to appropriate representatives of non-Federal entities.

"(b) DEFINITIONS.—In this section, the terms 'appropriate Federal entities', 'cyber threat indicator', 'defensive measure', 'Federal entity', and 'non-Federal entity' have the meaning given such terms in section 11 of the Protecting Cyber Networks Act.".

(b) SUBMITTAL TO CONGRESS.—Not later than 90 days after the date of the enactment of this Act, the Director of National Intelligence, in consultation with the heads of the other appropriate Federal entities, shall submit to Congress the procedures required by section 111(a) of the National Security Act of 1947, as inserted by subsection (a) of this section.

(c) TABLE OF CONTENTS AMENDMENT.—The table of contents in the first section of the National Security Act of 1947 is amended by inserting after the item relating to section 110 the following new item:

"Sec. 111. Sharing of cyber threat indicators and defensive measures by the Federal Government with non-Federal entities.".

SEC. 3. AUTHORIZATIONS FOR PREVENTING, DETECTING, ANALYZING, AND MITIGATING CYBERSECURITY THREATS.

(a) AUTHORIZATION FOR PRIVATE-SECTOR DEFENSIVE MONITORING.—

(1) IN GENERAL.—Notwithstanding any other provision of law, a private entity may, for a cybersecurity purpose, monitor—

(A) an information system of such private entity;

(B) an information system of a non-Federal entity or a Federal entity, upon the written authorization of such non-Federal entity or such Federal entity; and

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

(2) CONSTRUCTION.—Nothing in this subsection shall be construed to—

(A) authorize the monitoring of an information system, or the use of any information obtained through such monitoring, other than as provided in this Act;

(B) authorize the Federal Government to conduct surveillance of any person; or

(C) limit otherwise lawful activity.

(b) AUTHORIZATION FOR OPERATION OF DEFENSIVE MEASURES.—

(1) IN GENERAL.—Except as provided in paragraph (2) and notwithstanding any other provision of law, a private entity may, for a cybersecurity pur-

pose, operate a defensive measure that is operated on and is limited to—

(A) an information system of such private entity to protect the rights or property of the private entity; and

(B) an information system of a non-Federal entity or a Federal entity upon written authorization of such non-Federal entity or such Federal entity for operation of such defensive measure to protect the rights or property of such private entity, such non-Federal entity, or such Federal entity.

(2) LIMITATION.—The authority provided in paragraph (1) does not include the intentional or reckless operation of any defensive measure that destroys, renders unusable or inaccessible (in whole or in part), substantially harms, or initiates a new action, process, or procedure on an information system or information stored on, processed by, or transiting such information system not owned by—

(A) the private entity operating such defensive measure; or

(B) a non-Federal entity or a Federal entity that has provided written authorization to that private entity for operation of such defen-

sive measure on the information system or information of the entity in accordance with this subsection.

(3) CONSTRUCTION.—Nothing in this subsection shall be construed—

(A) to authorize the use of a defensive measure other than as provided in this subsection; or

(B) to limit otherwise lawful activity.

(c) AUTHORIZATION FOR SHARING OR RECEIVING CYBER THREAT INDICATORS OR DEFENSIVE MEASURES.—

(1) IN GENERAL.—Except as provided in paragraph (2) and notwithstanding any other provision of law, a non-Federal entity may, for a cybersecurity purpose and consistent with the requirement under subsection (d)(2) to remove personal information of or information identifying a specific person not directly related to a cybersecurity threat and the protection of classified information—

(A) share a lawfully obtained cyber threat indicator or defensive measure with any other non-Federal entity or an appropriate Federal entity (other than the Department of Defense or any component of the Department, including the National Security Agency); and

(B) receive a cyber threat indicator or defensive measure from any other non-Federal entity or an appropriate Federal entity.

(2) LAWFUL RESTRICTION.—A non-Federal entity receiving a cyber threat indicator or defensive measure from another non-Federal entity or a Federal entity shall comply with otherwise lawful restrictions placed on the sharing or use of such cyber threat indicator or defensive measure by the sharing non-Federal entity or Federal entity.

(3) CONSTRUCTION.—Nothing in this subsection shall be construed to—

(A) authorize the sharing or receiving of a cyber threat indicator or defensive measure other than as provided in this subsection;

(B) authorize the sharing or receiving of classified information by or with any person not authorized to access such classified information;

(C) prohibit any Federal entity from engaging in formal or informal technical discussion regarding cyber threat indicators or defensive measures with a non-Federal entity or from providing technical assistance to address vulnerabilities or mitigate threats at the request of such an entity;

(D) limit otherwise lawful activity;

(E) prohibit a non-Federal entity, if authorized by applicable law or regulation other than this Act, from sharing a cyber threat indicator or defensive measure with the Department of Defense or any component of the Department, including the National Security Agency; or

(F) authorize the Federal Government to conduct surveillance of any person.

(d) PROTECTION AND USE OF INFORMATION.—

(1) SECURITY OF INFORMATION.—A non-Federal entity monitoring an information system, operating a defensive measure, or providing or receiving a cyber threat indicator or defensive measure under this section shall implement an appropriate security control to protect against unauthorized access to, or acquisition of, such cyber threat indicator or defensive measure.

(2) REMOVAL OF CERTAIN PERSONAL INFORMATION.—A non-Federal entity sharing a cyber threat indicator pursuant to this Act shall, prior to such sharing, take reasonable efforts to—

(A) review such cyber threat indicator to assess whether such cyber threat indicator contains any information that the non-Federal entity rea-

sonably believes at the time of sharing to be personal information of or information identifying a specific person not directly related to a cybersecurity threat and remove such information; or

(B) implement a technical capability configured to remove any information contained within such indicator that the non-Federal entity reasonably believes at the time of sharing to be personal information of or information identifying a specific person not directly related to a cybersecurity threat.

(3) USE OF CYBER THREAT INDICATORS AND DEFENSIVE MEASURES BY NON-FEDERAL ENTITIES.—A non-Federal entity may, for a cybersecurity purpose—

(A) use a cyber threat indicator or defensive measure shared or received under this section to monitor or operate a defensive measure on—

(i) an information system of such non-Federal entity; or

(ii) an information system of another non-Federal entity or a Federal entity upon the written authorization of that other non-Federal entity or that Federal entity; and

(B) otherwise use, retain, and further share such cyber threat indicator or defensive measure subject to—

(i) an otherwise lawful restriction placed by the sharing non-Federal entity or Federal entity on such cyber threat indicator or defensive measure; or

(ii) an otherwise applicable provision of law.

(4) USE OF CYBER THREAT INDICATORS BY STATE, TRIBAL, OR LOCAL GOVERNMENT.—

(A) LAW ENFORCEMENT USE.—A State, tribal, or local government may use a cyber threat indicator shared with such State, tribal, or local government for the purposes described in clauses (i), (ii), and (iii) of section 4(d)(5)(A).

(B) EXEMPTION FROM DISCLOSURE.—A cyber threat indicator shared with a State, tribal, or local government 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, except as

otherwise required by applicable State, tribal, or local law requiring disclosure in any criminal prosecution.

(e) NO RIGHT OR BENEFIT.—The sharing of a cyber threat indicator with a non-Federal entity under this Act shall not create a right or benefit to similar information by such non-Federal entity or any other non-Federal entity.

SEC. 4. SHARING OF CYBER THREAT INDICATORS AND DEFENSIVE MEASURES WITH APPROPRIATE FEDERAL ENTITIES OTHER THAN THE DEPARTMENT OF DEFENSE OR THE NATIONAL SECURITY AGENCY.

(a) REQUIREMENT FOR POLICIES AND PROCEDURES.—

(1) IN GENERAL.—Section 111 of the National Security Act of 1947, as inserted by section 2 of this Act, is amended—

(A) by redesignating subsection (b) as subsection (c); and

(B) by inserting after subsection (a) the following new subsection:

"(b) POLICIES AND PROCEDURES FOR SHARING WITH THE APPROPRIATE FEDERAL ENTITIES OTHER THAN THE DEPARTMENT OF DEFENSE OR THE NATIONAL SECURITY AGENCY.—

"(1) ESTABLISHMENT.—The President shall develop and submit to Congress policies and procedures relating to the receipt of cyber threat indicators and defensive measures by the Federal Government.

"(2) REQUIREMENTS CONCERNING POLICIES AND PROCEDURES.—The policies and procedures required under paragraph (1) shall—

"(A) be developed in accordance with the privacy and civil liberties guidelines required under section 4(b) of the Protecting Cyber Networks Act;

"(B) ensure that—

"(i) a cyber threat indicator shared by a non-Federal entity with an appropriate Federal entity (other than the Department of Defense or any component of the Department, including the National Security Agency) pursuant to section 3 of such Act is shared in real-time with all of the appropriate Federal entities (including all relevant components thereof);

"(ii) the sharing of such cyber threat indicator with appropriate Federal entities is not subject to any delay, modification, or any other action without good cause that

could impede receipt by all of the appropriate Federal entities; and

"(iii) such cyber threat indicator is provided to each other Federal entity to which such cyber threat indicator is relevant; and

"(C) ensure there—

"(i) is an audit capability; and

"(ii) are appropriate sanctions in place for officers, employees, or agents of a Federal entity who knowingly and willfully use a cyber threat indicator or defense measure shared with the Federal Government by a non-Federal entity under the Protecting Cyber Networks Act other than in accordance with this section and such Act.".

(2) SUBMISSION.—The President shall submit to Congress—

(A) not later than 90 days after the date of the enactment of this Act, interim policies and procedures required under section 111(b)(1) of the National Security Act of 1947, as inserted by paragraph (1) of this section; and

(B) not later than 180 days after such date, final policies and procedures required under such section 111(b)(1).

(b) PRIVACY AND CIVIL LIBERTIES.—

(1) GUIDELINES OF ATTORNEY GENERAL.—The Attorney General, in consultation with the heads of the other appropriate Federal agencies and with officers designated under section 1062 of the Intelligence Reform and Terrorism Prevention Act of 2004 (42 U.S.C. 2000ee–1), shall develop and periodically review guidelines relating to privacy and civil liberties that govern the receipt, retention, use, and dissemination of cyber threat indicators by a Federal entity obtained in accordance with this Act and the amendments made by 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, including guidelines to ensure that personal information of or information identifying specific persons is properly removed from information received, retained, used, or dis-

seminated by a Federal entity in accordance with this Act or the amendments made by this Act;

(B) limit the receipt, retention, use, and dissemination of cyber threat indicators containing personal information of or information identifying specific persons, including by establishing—

(i) a process for the prompt destruction of such information that is known not to be directly related to a use for a cybersecurity purpose;

(ii) specific limitations on the length of any period in which a cyber threat indicator may be retained; and

(iii) a process to inform recipients that such indicators may only be used for a cybersecurity purpose;

(C) include requirements to safeguard cyber threat indicators containing personal information of or identifying 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 non-Federal entities and Federal entities if information received pursuant to this section is known or determined by a Federal entity receiving such information not to constitute a cyber threat indicator;

(E) be consistent with any other applicable provisions of law and the fair information practice principles set forth in appendix A of the document entitled "National Strategy for Trusted Identities in Cyberspace" and published by the President in April, 2011; and

(F) include steps that may be needed so that dissemination of cyber threat indicators is consistent with the protection of classified information and other sensitive national security information.

(3) SUBMISSION.—The Attorney General shall submit to Congress—

(A) not later than 90 days after the date of the enactment of this Act, interim guidelines required under paragraph (1); and

(B) not later than 180 days after such date, final guidelines required under such paragraph.

(c) NATIONAL CYBER THREAT INTELLIGENCE INTEGRATION CENTER.—

(1) ESTABLISHMENT.—Title I of the National Security Act of 1947 (50 U.S.C. 3021 et seq.), as amended by section 2 of this Act, is further amended—

(A) by redesignating section 119B as section 119C; and

(B) by inserting after section 119A the following new section:

"SEC. 119B. CYBER THREAT INTELLIGENCE INTEGRATION CENTER.

"(a) ESTABLISHMENT.—There is within the Office of the Director of National Intelligence a Cyber Threat Intelligence Integration Center.

"(b) DIRECTOR.—There is a Director of the Cyber Threat Intelligence Integration Center, who shall be the head of the Cyber Threat Intelligence Integration Center, and who shall be appointed by the Director of National Intelligence.

"(c) PRIMARY MISSIONS.—The Cyber Threat Intelligence Integration Center shall—

"(1) serve as the primary organization within the Federal Government for analyzing and inte-

grating all intelligence possessed or acquired by the United States pertaining to cyber threats;

"(2) ensure that appropriate departments and agencies have full access to and receive all-source intelligence support needed to execute the cyber threat intelligence activities of such agencies and to perform independent, alternative analyses;

"(3) disseminate cyber threat analysis to the President, the appropriate departments and agencies of the Federal Government, and the appropriate committees of Congress;

"(4) coordinate cyber threat intelligence activities of the departments and agencies of the Federal Government; and

"(5) conduct strategic cyber threat intelligence planning for the Federal Government.

"(d) LIMITATIONS.—The Cyber Threat Intelligence Integration Center shall—

"(1) have not more than 50 permanent positions;

"(2) in carrying out the primary missions of the Center described in subsection (c), may not augment staffing through detailees, assignees, or core contractor personnel or enter into any personal services contracts to exceed the limitation under paragraph (1); and

"(3) be located in a building owned or operated by an element of the intelligence community as of the date of the enactment of this section.".

(2) TABLE OF CONTENTS AMENDMENTS.—The table of contents in the first section of the National Security Act of 1947, as amended by section 2 of this Act, is further amended by striking the item relating to section 119B and inserting the following new items:

"Sec. 119B. Cyber Threat Intelligence Integration Center.
"Sec. 119C. National intelligence centers.".

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

(1) NO WAIVER OF PRIVILEGE OR PROTECTION.—The provision of a cyber threat indicator or defensive measure 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.—Consistent with section 3(c)(2), a cyber threat indicator or defensive measure provided by a non-Federal entity to the Federal Government under this Act shall be considered the commercial, financial, and proprietary information of the non-Federal entity that is the originator of such cyber threat indicator or defensive

measure when so designated by such non-Federal entity or a non-Federal entity acting in accordance with the written authorization of the non-Federal entity that is the originator of such cyber threat indicator or defensive measure.

(3) EXEMPTION FROM DISCLOSURE.—A cyber threat indicator or defensive measure 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, except as otherwise required by applicable Federal, State, tribal, or local law requiring disclosure in any criminal prosecution.

(4) EX PARTE COMMUNICATIONS.—The provision of a cyber threat indicator or defensive measure to the Federal Government under this Act shall not be subject to a rule of any Federal department or agency or

any judicial doctrine regarding ex parte communications with a decision-making official.

(5) DISCLOSURE, RETENTION, AND USE.—

(A) AUTHORIZED ACTIVITIES.—A cyber threat indicator or defensive measure provided to the Federal Government under this Act may be disclosed to, retained by, and used by, consistent with otherwise applicable provisions of Federal law, any department, agency, component, officer, employee, or agent of the Federal Government solely for—

(i) a cybersecurity purpose;

(ii) the purpose of responding to, prosecuting, or otherwise preventing or mitigating a threat of death or serious bodily harm or an offense arising out of such a threat;

(iii) the purpose of responding to, or otherwise preventing or mitigating, a serious threat to a minor, including sexual exploitation and threats to physical safety; or

(iv) the purpose of preventing, investigating, disrupting, or prosecuting any of the offenses listed in sections 1028, 1029,

1030, and 3559(c)(2)(F) and chapters 37 and 90 of title 18, United States Code.

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

(C) PRIVACY AND CIVIL LIBERTIES.—A cyber threat indicator or defensive measure provided to the Federal Government under this Act shall be retained, used, and disseminated by the Federal Government in accordance with—

(i) the policies and procedures relating to the receipt of cyber threat indicators and defensive measures by the Federal Government required by subsection (b) of section 111 of the National Security Act of 1947, as added by subsection (a) of this section; and

(ii) the privacy and civil liberties guidelines required by subsection (b).

SEC. 5. FEDERAL GOVERNMENT LIABILITY FOR VIOLATIONS OF PRIVACY OR CIVIL LIBERTIES.

(a) IN GENERAL.—If a department or agency of the Federal Government intentionally or willfully violates the

privacy and civil liberties guidelines issued by the Attorney General under section 4(b), the United States shall be liable to a person injured by such violation in an amount equal to the sum of—

(1) the actual damages sustained by the person as a result of the violation or $1,000, whichever is greater; and

(2) reasonable attorney fees as determined by the court and other litigation costs reasonably incurred in any case under this subsection in which the complainant has substantially prevailed.

(b) VENUE.—An action to enforce liability created under this section may be brought in the district court of the United States in—

(1) the district in which the complainant resides;

(2) the district in which the principal place of business of the complainant is located;

(3) the district in which the department or agency of the Federal Government that violated such privacy and civil liberties guidelines is located; or

(4) the District of Columbia.

(c) STATUTE OF LIMITATIONS.—No action shall lie under this subsection unless such action is commenced not later than two years after the date of the violation of the

privacy and civil liberties guidelines issued by the Attorney General under section 4(b) that is the basis for the action.

(d) EXCLUSIVE CAUSE OF ACTION.—A cause of action under this subsection shall be the exclusive means available to a complainant seeking a remedy for a violation by a department or agency of the Federal Government under this Act.

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 an information system and information under section 3(a) that is conducted in good faith in accordance with this Act and the amendments made by this Act.

(b) SHARING OR RECEIPT OF CYBER THREAT INDICATORS.—No cause of action shall lie or be maintained in any court against any non-Federal entity, and such action shall be promptly dismissed, for the sharing or receipt of a cyber threat indicator or defensive measure under section 3(c), or a good faith failure to act based on such sharing or receipt, if such sharing or receipt is conducted in good faith in accordance with this Act and the amendments made by this Act.

(c) WILLFUL MISCONDUCT.—

(1) RULE OF CONSTRUCTION.—Nothing in this section shall be construed—

(A) to require dismissal of a cause of action against a non-Federal entity (including a private entity) that has engaged in willful misconduct in the course of conducting activities authorized by this Act or the amendments made by this Act; or

(B) to undermine or limit the availability of otherwise applicable common law or statutory defenses.

(2) PROOF OF WILLFUL MISCONDUCT.—In any action claiming that subsection (a) or (b) does not apply due to willful misconduct described in paragraph (1), the plaintiff shall have the burden of proving by clear and convincing evidence the willful misconduct by each non-Federal entity subject to such claim and that such willful misconduct proximately caused injury to the plaintiff.

(3) WILLFUL MISCONDUCT DEFINED.—In this subsection, the term "willful misconduct" means an act or omission that is taken—

(A) intentionally to achieve a wrongful purpose;

(B) knowingly without legal or factual justification; and

(C) in disregard of a known or obvious risk that is so great as to make it highly probable that the harm will outweigh the benefit.

SEC. 7. OVERSIGHT OF GOVERNMENT ACTIVITIES.

(a) BIENNIAL REPORT ON IMPLEMENTATION.—

(1) IN GENERAL.—Section 111 of the National Security Act of 1947, as added by section 2(a) and amended by section 4(a) of this Act, is further amended—

(A) by redesignating subsection (c) (as redesignated by such section 4(a)) as subsection (d); and

(B) by inserting after subsection (b) (as inserted by such section 4(a)) the following new subsection:

"(c) BIENNIAL REPORT ON IMPLEMENTATION.—

"(1) IN GENERAL.—Not less frequently than once every two years, the Director of National Intelligence, in consultation with the heads of the other appropriate Federal entities, shall submit to Congress a report concerning the implementation of this section and the Protecting Cyber Networks 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 this section and section 4 of the Protecting Cyber Networks Act in ensuring that cyber threat indicators are shared effectively and responsibly within the Federal Government.

"(B) An assessment of whether the procedures developed under section 3 of such Act comply with the goals described in subparagraphs (A), (B), and (C) of subsection (a)(1).

"(C) 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 section and such Act.

"(D) A review of the type of cyber threat indicators shared with the Federal Government under this section and such Act, including the following:

"(i) The degree to which such information may impact the privacy and civil liberties of specific 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 specific persons.

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

"(E) A review of actions taken by the Federal Government based on cyber threat indicators shared with the Federal Government under this section or such Act, including the appropriateness of any subsequent use or dissemination of such cyber threat indicators by a Federal entity under this section or section 4 of such Act.

"(F) A description of any significant violations of the requirements of this section or such Act by the Federal Government—

"(i) an assessment of all reports of officers, employees, and agents of the Federal Government misusing information provided to the Federal Government under the Protecting Cyber Networks Act or this section, without regard to whether the misuse was knowing or wilful; and

"(ii) an assessment of all disciplinary actions taken against such officers, employees, and agents.

"(G) A summary of the number and type of non-Federal entities that received classified cyber threat indicators from the Federal Government under this section or such Act and an evaluation of the risks and benefits of sharing such cyber threat indicators.

"(H) An assessment of any personal information of or information identifying a specific person not directly related to a cybersecurity threat that—

"(i) was shared by a non-Federal entity with the Federal Government under this Act in contravention of section 3(d)(2); or

"(ii) was shared within the Federal Government under this Act in contravention of the guidelines required by section 4(b).

"(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 section or such Act.

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

"(5) PUBLIC AVAILABILITY OF REPORTS.—The Director of National Intelligence shall make publicly available the unclassified portion of each report required by paragraph (1).".

(2) INITIAL REPORT.—The first report required under subsection (c) of section 111 of the National Security Act of 1947, as inserted by paragraph (1) of this subsection, shall be submitted not later than one year after the date of the enactment of this Act.

(b) REPORTS ON PRIVACY AND CIVIL LIBERTIES.—

(1) BIENNIAL REPORT FROM PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD.—

(A) IN GENERAL.—Section 1061(e) of the Intelligence Reform and Terrorism Prevention Act of 2004 (42 U.S.C. 2000ee(e)) is amended by adding at the end the following new paragraph:

"(3) BIENNIAL REPORT ON CERTAIN CYBER ACTIVITIES.—

"(A) REPORT REQUIRED.—The Privacy and Civil Liberties Oversight Board shall biennially submit to Congress and the President a report containing—

"(i) an assessment of the privacy and civil liberties impact of the activities carried out under the Protecting Cyber Networks Act and the amendments made by such Act; and

"(ii) an assessment of the sufficiency of the policies, procedures, and guidelines established pursuant to section 4 of the Protecting Cyber Networks Act and the amendments made by such section 4 in addressing privacy and civil liberties concerns.

"(B) RECOMMENDATIONS.—Each report submitted under this paragraph may include such recommendations as the Privacy and Civil Liberties Oversight Board may have for improvements or modifications to the authorities under the Protecting Cyber Networks Act or the amendments made by such Act.

"(C) FORM.—Each report required under this paragraph shall be submitted in unclassified form, but may include a classified annex.

"(D) PUBLIC AVAILABILITY OF REPORTS.—The Privacy and Civil Liberties Oversight Board shall make publicly available the unclassified

portion of each report required by subparagraph (A).".

(B) INITIAL REPORT.—The first report required under paragraph (3) of section 1061(e) of the Intelligence Reform and Terrorism Prevention Act of 2004 (42 U.S.C. 2000ee(e)), as added by subparagraph (A) of this paragraph, shall be submitted not later than 2 years after the date of the enactment of this Act.

(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, in consultation with the Council of Inspectors General on Financial Oversight, shall jointly submit to Congress a report on the receipt, use, and dissemination of cyber threat indicators and defensive measures that have been shared with Federal

entities under this Act and the amendments made by 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.

(C) RECOMMENDATIONS.—Each report submitted under this paragraph may include such recommendations as the Inspectors General referred to in subparagraph (A) may have for improvements or modifications to the authorities under this Act or the amendments made by this Act.

(D) FORM.—Each report required under this paragraph shall be submitted in unclassified form, but may include a classified annex.

(E) PUBLIC AVAILABILITY OF REPORTS.—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 make publicly available the unclassified portion of each report required under subparagraph (A).

SEC. 8. REPORT ON CYBERSECURITY THREATS.

(a) REPORT REQUIRED.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence, in consultation with the heads of other appropriate elements of the intelligence community, shall submit to the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representatives a report on cybersecurity threats, including cyber attacks, theft, and data breaches.

(b) CONTENTS.—The report required by subsection (a) shall include the following:

(1) An assessment of—

(A) the current intelligence sharing and cooperation relationships of the United States with

other countries regarding cybersecurity threats (including cyber attacks, theft, and data breaches) directed against the United States that threaten the United States national security interests, economy, and intellectual property; and

(B) the relative utility of such relationships, which elements of the intelligence community participate in such relationships, and whether and how such relationships could be improved.

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

(3) A description of the extent to which the capabilities of the United States Government to respond to or prevent cybersecurity threats (including cyber attacks, theft, or data breaches) directed against the United States private sector are degraded by a delay in the prompt notification by private entities of such threats or cyber attacks, theft, and breaches.

(4) An assessment of additional technologies or capabilities that would enhance the ability of the United States to prevent and to respond to cybersecu-

rity threats (including cyber attacks, theft, and data breaches).

(5) An assessment of any technologies or practices utilized by the private sector that could be rapidly fielded to assist the intelligence community in preventing and responding to cybersecurity threats.

(c) FORM OF REPORT.—The report required by subsection (a) shall be submitted in unclassified form, but may include a classified annex.

(d) PUBLIC AVAILABILITY OF REPORT.—The Director of National Intelligence shall make publicly available the unclassified portion of the report required by subsection (a).

(e) INTELLIGENCE COMMUNITY DEFINED.—In this section, the term ''intelligence community'' has the meaning given that term in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).

SEC. 9. CONSTRUCTION AND PREEMPTION.

(a) PROHIBITION OF SURVEILLANCE.—Nothing in this Act or the amendments made by this Act shall be construed to authorize the Department of Defense or the National Security Agency or any other element of the intelligence community to target a person for surveillance.

(b) OTHERWISE LAWFUL DISCLOSURES.—Nothing in this Act or the amendments made by this Act shall be construed to limit or prohibit—

(1) otherwise lawful disclosures of communications, records, or other information, including reporting of known or suspected criminal activity, by a non-Federal entity to any other non-Federal entity or the Federal Government; or

(2) any otherwise lawful use of such disclosures by any entity of the Federal government, without regard to whether such otherwise lawful disclosures duplicate or replicate disclosures made under this Act.

(c) WHISTLE BLOWER PROTECTIONS.—Nothing in this Act or the amendments made by this Act shall be construed to prohibit or limit the disclosure of information protected under section 2302(b)(8) of title 5, United States Code (governing disclosures of illegality, waste, fraud, abuse, or public health or safety threats), section 7211 of title 5, United States Code (governing disclosures to Congress), section 1034 of title 10, United States Code (governing disclosure to Congress by members of the military), or any similar provision of Federal or State law..

(d) PROTECTION OF SOURCES AND METHODS.—Nothing in this Act or the amendments made by this Act shall be construed—

(1) as creating any immunity against, or otherwise affecting, any action brought by the Federal Government, or any department or agency thereof, to

enforce any law, executive order, or procedure governing the appropriate handling, disclosure, or use of classified information;

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

(3) to modify the authority of the President or a department or agency of the Federal Government to protect and control the dissemination of classified information, intelligence sources and methods, and the national security of the United States.

(e) RELATIONSHIP TO OTHER LAWS.—Nothing in this Act or the amendments made by this Act shall be construed to affect any requirement under any other provision of law for a non-Federal entity to provide information to the Federal Government.

(f) INFORMATION SHARING RELATIONSHIPS.—Nothing in this Act or the amendments made by this Act shall be construed—

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

(2) to prohibit a new information-sharing relationship; or

(3) to require a new information-sharing relationship between any non-Federal entity and the Federal Government.

(g) PRESERVATION OF CONTRACTUAL OBLIGATIONS AND RIGHTS.—Nothing in this Act or the amendments made by this Act shall be construed—

(1) to amend, repeal, or supersede any current or future contractual agreement, terms of service agreement, or other contractual relationship between any non-Federal entities, or between any non-Federal entity and a Federal entity; or

(2) to abrogate trade secret or intellectual property rights of any non-Federal entity or Federal entity.

(h) ANTI-TASKING RESTRICTION.—Nothing in this Act or the amendments made by this Act shall be construed to permit the Federal Government—

(1) to require a non-Federal entity to provide information to the Federal Government;

(2) to condition the sharing of a cyber threat indicator with a non-Federal entity on such non-Federal entity's provision of a cyber threat indicator to the Federal Government; or

(3) to condition the award of any Federal grant, contract, or purchase on the provision of a cyber threat indicator to a Federal entity.

(i) NO LIABILITY FOR NON-PARTICIPATION.—Nothing in this Act or the amendments made by this Act shall be

construed to subject any non-Federal entity to liability for choosing not to engage in a voluntary activiy authorized in this Act and the amendments made by this Act.

(j) USE AND RETENTION OF INFORMATION.—Nothing in this Act or the amendments made by this Act shall be construed to authorize, or to modify any existing authority of, a department or agency of the Federal Government to retain or use any information shared under this Act or the amendments made by this Act for any use other than permitted in this Act or the amendments made by this Act.

(k) FEDERAL PREEMPTION.—

(1) IN GENERAL.—This Act and the amendments made by this Act supersede any statute or other provision of law of a State or political subdivision of a State that restricts or otherwise expressly regulates an activity authorized under this Act or the amendments made by this Act.

(2) STATE LAW ENFORCEMENT.—Nothing in this Act or the amendments made by this Act shall be construed to supersede any statute or other provision of law of a State or political subdivision of a State concerning the use of authorized law enforcement practices and procedures.

(l) REGULATORY AUTHORITY.—Nothing in this Act or the amendments made by this Act shall be construed—

(1) to authorize the promulgation of any regulations not specifically authorized by this Act or the amendments made by this Act;

(2) to establish any regulatory authority not specifically established under this Act or the amendments made by this Act; or

(3) to authorize regulatory actions that would duplicate or conflict with regulatory requirements, mandatory standards, or related processes under another provision of Federal law.

SEC. 10. 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 inserting after paragraph (9) the following:

"(10) information shared with or provided to the Federal Government pursuant to the Protecting Cyber Networks Act or the amendments made by such Act.".

SEC. 11. 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) 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 Department of the Treasury.

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

(3) CYBERSECURITY PURPOSE.—The term "cybersecurity purpose" means the purpose of protecting (including through the use of a defensive measure) an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability or identifying the source of a cybersecurity threat.

(4) CYBERSECURITY THREAT.—

(A) IN GENERAL.—Except as provided in subparagraph (B), the term "cybersecurity threat" means an action, not protected by the

first amendment to the Constitution of the United States, on or through an information system that may result in an unauthorized effort to adversely impact the security, confidentiality, integrity, or availability of an information system or information that is stored on, processed by, or transiting an information system.

(B) EXCLUSION.—The term "cybersecurity threat" does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement.

(5) CYBER THREAT INDICATOR.—The term "cyber threat indicator" means information or a physical object that is necessary to describe or 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 or security vulnerability;

(B) a method of defeating a security control or exploitation of a security vulnerability;

(C) a security vulnerability, including anomalous activity that appears to indicate the existence of 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 or exploitation of a security vulnerability;

(E) malicious cyber command and control;

(F) the actual or potential harm caused by an incident, including a description of the information exfiltrated as a result of a particular cybersecurity threat; or

(G) any other attribute of a cybersecurity threat, if disclosure of such attribute is not otherwise prohibited by law.

(6) DEFENSIVE MEASURE.—The term "defensive measure" means an action, device, procedure, technique, or other measure executed on an information system or information that is stored on, processed by, or transiting an information system that prevents or mitigates a known or suspected cybersecurity threat or security vulnerability.

(7) FEDERAL ENTITY.—The term "Federal entity" means a department or agency of the United States or any component of such department or agency.

(8) INFORMATION SYSTEM.—The term "information system"—

(A) has the meaning given the term in section 3502 of title 44, United States Code; and

(B) includes industrial control systems, such as supervisory control and data acquisition systems, distributed control systems, and programmable logic controllers.

(9) LOCAL GOVERNMENT.—The term "local government" means any borough, city, county, parish, town, township, village, or other political subdivision of a State.

(10) 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.

(11) 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.

(12) MONITOR.—The term "monitor" means to acquire, identify, scan, or otherwise possess information that is stored on, processed by, or transiting an information system.

(13) NON-FEDERAL ENTITY.—

(A) IN GENERAL.—Except as otherwise provided in this paragraph, the term "non-Federal entity" means any private entity, non-Federal government department or agency, or State, tribal, or local government (including a political subdivision, department, officer, employee, or agent thereof).

(B) INCLUSIONS.—The term "non-Federal entity" includes a government department or agency (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 "non-Federal entity" does not include a foreign power or known agent of a foreign power, as both terms are defined in section 101 of the Foreign Intel-

ligence Surveillance Act of 1978 (50 U.S.C. 1801).

(14) PRIVATE ENTITY.—

(A) IN GENERAL.—Except as otherwise provided in this paragraph, the term "private entity" means any person or private group, organization, proprietorship, partnership, trust, cooperative, corporation, or other commercial or nonprofit entity, including an officer, employee, or agent thereof.

(B) INCLUSION.—The term "private entity" includes a component of a State, tribal, or local government performing electric utility services.

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

(15) REAL TIME; REAL-TIME.—The terms "real time" and "real-time" mean a process by which an automated, machine-to-machine system processes cyber threat indicators such that the time in which the occurrence of an event and the reporting or recording of it are as simultaneous as technologically and operationally practicable.

(16) SECURITY CONTROL.—The term "security control" means the management, operational, and technical controls used to protect against an unauthorized effort to adversely impact the security, confidentiality, integrity, and availability of an information system or its information.

(17) SECURITY VULNERABILITY.—The term "security vulnerability" means any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control.

(18) 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).

Union Calendar No. 44

114TH CONGRESS
1ST SESSION

H. R. 1560

[Report No. 114–63]

A BILL

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

APRIL 13, 2015

Reported with an amendment, committed to the Committee of the Whole House on the State of the Union, and ordered to be printed